



Guía del usuario de

# AWS IAM Identity Center



# AWS IAM Identity Center: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

# Table of Contents

|                                                                                                                                 |    |
|---------------------------------------------------------------------------------------------------------------------------------|----|
| ¿Qué es IAM Identity Center? .....                                                                                              | 1  |
| ¿Por qué utilizar el IAM Identity Center? .....                                                                                 | 1  |
| Cambio de nombre de IAM Identity Center .....                                                                                   | 3  |
| Los espacios de nombres antiguos siguen siendo los mismos .....                                                                 | 3  |
| Introducción .....                                                                                                              | 4  |
| Requisitos previos y consideraciones sobre el IAM Identity Center .....                                                         | 6  |
| Elegir una Región de AWS .....                                                                                                  | 7  |
| Uso del IAM Identity Center únicamente para aplicaciones .....                                                                  | 14 |
| Roles de IAM creados por IAM Identity Center .....                                                                              | 15 |
| Centro de identidad de IAM y AWS Organizations .....                                                                            | 16 |
| Instancias de IAM Identity Center .....                                                                                         | 17 |
| Cuenta de AWS tipos que pueden habilitar el IAM Identity Center .....                                                           | 17 |
| Instancias de organización de IAM Identity Center .....                                                                         | 19 |
| Instancias de cuenta de IAM Identity Center .....                                                                               | 20 |
| Eliminación de la instancia de IAM Identity Center .....                                                                        | 25 |
| Activar IAM Identity Center .....                                                                                               | 28 |
| Para habilitar una instancia de cuenta de IAM Identity Center .....                                                             | 29 |
| Confirmación de orígenes de identidad .....                                                                                     | 32 |
| Actualización de firewalls y puertas de enlace .....                                                                            | 34 |
| Consideraciones a la hora de permitir la inclusión de dominios y puntos de conexión de URL .....                                | 36 |
| Tutoriales sobre orígenes de identidad .....                                                                                    | 38 |
| Active Directory .....                                                                                                          | 39 |
| CyberArk .....                                                                                                                  | 41 |
| Requisitos previos .....                                                                                                        | 42 |
| Consideraciones de SCIM .....                                                                                                   | 43 |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                              | 44 |
| Paso 2: configure el aprovisionamiento en CyberArk .....                                                                        | 45 |
| (Opcional) Paso 3: configure los atributos de usuario en CyberArk para el control de acceso (ABAC) en IAM Identity Center ..... | 46 |
| (Opcional) Paso de atributos para el control de acceso .....                                                                    | 46 |
| Google Workspace .....                                                                                                          | 47 |
| Consideraciones .....                                                                                                           | 48 |
| Paso 1 Google Workspace: Configurar la aplicación SAML .....                                                                    | 49 |

|                                                                                                                                                                                       |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Paso 2: IAM Identity Center y Google Workspace: cambio del origen de identidad de IAM Identity Center y configuración de Google Workspace como proveedor de identidades de SAML ..... | 50 |
| Paso 3: Google Workspace: habilitación de las aplicaciones .....                                                                                                                      | 51 |
| Paso 4: IAM Identity Center: configuración del aprovisionamiento automático de IAM Identity Center .....                                                                              | 52 |
| Paso 5: Google Workspace: configuración del aprovisionamiento automático .....                                                                                                        | 53 |
| Paso de atributos para el control de acceso: opcional .....                                                                                                                           | 55 |
| Asigne acceso a Cuentas de AWS .....                                                                                                                                                  | 55 |
| Siguientes pasos .....                                                                                                                                                                | 58 |
| Resolución de problemas .....                                                                                                                                                         | 58 |
| JumpCloud .....                                                                                                                                                                       | 59 |
| Requisitos previos .....                                                                                                                                                              | 60 |
| Consideraciones de SCIM .....                                                                                                                                                         | 61 |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                                                                                    | 61 |
| Paso 2: configure el aprovisionamiento en JumpCloud .....                                                                                                                             | 62 |
| (Opcional) Paso 3: configure los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center .....                                                             | 63 |
| (Opcional) Paso de atributos para el control de acceso .....                                                                                                                          | 64 |
| Microsoft Entra ID .....                                                                                                                                                              | 64 |
| Requisitos previos .....                                                                                                                                                              | 65 |
| Consideraciones .....                                                                                                                                                                 | 65 |
| Paso 1: preparación de su inquilino de Microsoft .....                                                                                                                                | 67 |
| Paso 2: Prepara tu AWS cuenta .....                                                                                                                                                   | 69 |
| Paso 3: configuración y prueba de la conexión SAML .....                                                                                                                              | 72 |
| Paso 4: configuración y comprobación de la sincronización de SCIM .....                                                                                                               | 76 |
| Paso 5: Configurar ABAC: opcional .....                                                                                                                                               | 80 |
| Asigne el acceso a Cuentas de AWS .....                                                                                                                                               | 82 |
| Microsoft Entra IDconfiguración para acceder a regiones adicionales .....                                                                                                             | 84 |
| Resolución de problemas .....                                                                                                                                                         | 85 |
| Okta .....                                                                                                                                                                            | 87 |
| Consideraciones .....                                                                                                                                                                 | 89 |
| Paso 1: Okta: obtención de los metadatos de SAML de su cuenta de Okta .....                                                                                                           | 90 |
| Paso 2: IAM Identity Center: configuración de Okta como origen de identidad para IAM Identity Center .....                                                                            | 90 |
| Paso 3: IAM Identity Center and Okta: aprovisionar usuarios de Okta .....                                                                                                             | 92 |



|                                                                                                                          |     |
|--------------------------------------------------------------------------------------------------------------------------|-----|
| Paso 4: Okta: sincronización de los usuarios desde Okta con IAM Identity Center .....                                    | 93  |
| Paso de atributos para el control de acceso: opcional .....                                                              | 95  |
| Asigne el acceso a Cuentas de AWS .....                                                                                  | 96  |
| Oktaconfiguración para acceder a regiones adicionales .....                                                              | 98  |
| Siguientes pasos .....                                                                                                   | 99  |
| Resolución de problemas .....                                                                                            | 99  |
| OneLogin .....                                                                                                           | 101 |
| Requisitos previos .....                                                                                                 | 103 |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                       | 103 |
| Paso 2: configure el aprovisionamiento en OneLogin .....                                                                 | 104 |
| (Opcional) Paso 3: configure los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center ..... | 105 |
| (Opcional) Paso de atributos para el control de acceso .....                                                             | 106 |
| Resolución de problemas .....                                                                                            | 107 |
| Ping Identity .....                                                                                                      | 108 |
| PingFederate .....                                                                                                       | 108 |
| PingOne .....                                                                                                            | 116 |
| Directorio de Identity Center .....                                                                                      | 123 |
| Tutoriales de vídeo .....                                                                                                | 129 |
| Configuración del personal .....                                                                                         | 130 |
| Usuarios, grupos y aprovisionamiento .....                                                                               | 130 |
| Exclusividad del nombre de usuario y de la dirección de correo electrónico .....                                         | 130 |
| Groups .....                                                                                                             | 131 |
| Aprovisionamiento de usuarios y grupos .....                                                                             | 131 |
| Desaprovisionamiento de usuarios y grupos .....                                                                          | 131 |
| Administración de su fuente de identidad .....                                                                           | 132 |
| Consideraciones para cambiar la fuente de identidad .....                                                                | 132 |
| Cambiar su fuente de identidad .....                                                                                     | 138 |
| Atributos de usuario y grupo en IAM Identity Center .....                                                                | 140 |
| Proveedores de identidades externos .....                                                                                | 142 |
| Directorio Microsoft AD .....                                                                                            | 161 |
| Administración de usuarios en el directorio de Identity Center .....                                                     | 183 |
| Aprovisionamiento cuando los usuarios están en IAM Identity Center .....                                                 | 183 |
| Cambio de su fuente de identidad .....                                                                                   | 183 |
| Agregar usuarios .....                                                                                                   | 184 |
| Cómo agregar grupos .....                                                                                                | 187 |

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Agregar usuarios a grupos .....                                                          | 188 |
| Eliminación de grupos .....                                                              | 189 |
| Eliminar usuarios .....                                                                  | 190 |
| Eliminar usuarios de los grupos .....                                                    | 192 |
| Edición de propiedades del usuario .....                                                 | 192 |
| Acceso del personal .....                                                                | 194 |
| Descripción de las sesiones de autenticación .....                                       | 194 |
| Tipos de sesiones de autenticación .....                                                 | 195 |
| Formas de finalizar las sesiones de usuario .....                                        | 196 |
| Qué sucede con el acceso de los usuarios al finalizar una sesión .....                   | 197 |
| Cierre de sesión único .....                                                             | 201 |
| Prácticas recomendadas para la administración de sesiones .....                          | 201 |
| Configuración de la duración de la sesión .....                                          | 201 |
| Sesiones interactivas de usuario .....                                                   | 202 |
| Sesiones de usuario en segundo plano .....                                               | 203 |
| Sesiones ampliadas para Kiro .....                                                       | 205 |
| Finalización de las sesiones activas de los usuarios del personal .....                  | 206 |
| Consideraciones sobre las fuentes de identidad, la AWS CLI y AWS SDKs .....              | 207 |
| Desactivación de los accesos de usuario .....                                            | 211 |
| Denegación de acceso a usuarios .....                                                    | 212 |
| Administración del acceso para usuarios en el directorio de Identity Center .....        | 213 |
| Administración de contraseñas .....                                                      | 214 |
| MFA .....                                                                                | 214 |
| Configuración de contraseñas de usuario .....                                            | 215 |
| Autenticación multifactor .....                                                          | 218 |
| Acceso de aplicaciones .....                                                             | 233 |
| AWS aplicaciones gestionadas .....                                                       | 234 |
| Control del acceso a las aplicaciones .....                                              | 234 |
| Compartición de información de identidad .....                                           | 235 |
| Restringir el uso de aplicaciones gestionadas AWS .....                                  | 236 |
| Aplicaciones que puede utilizar con IAM Identity Center .....                            | 237 |
| Configuración del IAM Identity Center para probar las aplicaciones gestionadas AWS ..... | 243 |
| Visualización y modificación de los detalles de la aplicación .....                      | 249 |
| Deshabilitar una aplicación AWS gestionada .....                                         | 250 |
| Activación de sesiones de consola con identidad mejorada .....                           | 251 |
| Aplicaciones administradas por el cliente .....                                          | 254 |

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Aplicaciones SAML 2.0 y 2.0 OAuth .....                                            | 255 |
| Configuración de aplicaciones de SAML 2.0 .....                                    | 261 |
| Propagación de identidades confiables .....                                        | 264 |
| Ventajas de la propagación de la identidad de confianza .....                      | 265 |
| Activación de la propagación de identidades de confianza .....                     | 265 |
| Cómo funciona la propagación de identidades de confianza .....                     | 266 |
| Requisitos y consideraciones previos .....                                         | 267 |
| Casos de uso .....                                                                 | 269 |
| Autorización de servicios .....                                                    | 297 |
| Cómo configurar tu propia aplicación OAuth 2.0 .....                               | 308 |
| Configuración de aplicaciones administradas por el cliente .....                   | 309 |
| Especificación de las aplicaciones de confianza .....                              | 313 |
| Emisor de tokens de confianza .....                                                | 314 |
| Rotación de certificados .....                                                     | 330 |
| Consideraciones antes de rotar un certificado .....                                | 330 |
| Rotación de un certificado de IAM Identity Center .....                            | 331 |
| Indicadores de estado de caducidad de certificados .....                           | 333 |
| Entender las propiedades de la aplicación .....                                    | 334 |
| URL de inicio de la aplicación .....                                               | 334 |
| Estado de retransmisión .....                                                      | 335 |
| Duración de la sesión .....                                                        | 336 |
| Asigne el acceso de los usuarios a las aplicaciones .....                          | 336 |
| Eliminar el acceso de los usuarios a aplicaciones .....                            | 337 |
| Asignación de atributos .....                                                      | 338 |
| Cuenta de AWS acceder .....                                                        | 339 |
| Cuenta de AWS tipos .....                                                          | 339 |
| Asignación Cuenta de AWS de acceso .....                                           | 342 |
| La experiencia del usuario final .....                                             | 342 |
| Aplicación y limitación del acceso .....                                           | 343 |
| Delegación y aplicación del acceso .....                                           | 344 |
| Límite de acceso al almacén de identidades desde las cuentas de los miembros ..... | 344 |
| Administración delegada .....                                                      | 345 |
| Prácticas recomendadas .....                                                       | 346 |
| Requisitos previos .....                                                           | 351 |
| Registro de una cuenta de miembro .....                                            | 351 |
| Anulación del registro de una cuenta de miembro .....                              | 353 |

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Consulte las cuentas de administrador delegado .....                                    | 354 |
| Acceso elevado temporal .....                                                           | 354 |
| Acceso mediante inicio de sesión único a Cuentas de AWS .....                           | 355 |
| Asigne el acceso de usuario o grupo a Cuentas de AWS .....                              | 356 |
| Elimina el acceso de usuarios y grupos a un Cuenta de AWS .....                         | 359 |
| Revocar una sesión de conjunto de permisos activa .....                                 | 360 |
| Delegue quién puede asignar el acceso de inicio de sesión único .....                   | 362 |
| Conjuntos de permisos .....                                                             | 363 |
| Creación de un conjunto de permisos que aplique los permisos de privilegio mínimo ..... | 364 |
| Permisos predefinidos .....                                                             | 366 |
| Permisos personalizados .....                                                           | 367 |
| Creación, administración y eliminación de conjuntos de permisos .....                   | 370 |
| Configure las propiedades del conjunto de permisos .....                                | 384 |
| Referencias de conjuntos de permisos .....                                              | 391 |
| Recomendaciones para evitar interrupciones en el acceso .....                           | 394 |
| Ejemplo de políticas de confianza personalizadas .....                                  | 394 |
| Control de acceso basado en atributos .....                                             | 396 |
| Ventajas .....                                                                          | 396 |
| Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS .....        | 397 |
| Atributos para controlar el acceso .....                                                | 400 |
| Roles vinculados a servicios .....                                                      | 407 |
| AWS portal de acceso .....                                                              | 409 |
| Cómo empezar a utilizar el portal de AWS acceso .....                                   | 409 |
| Configure el portal de AWS acceso .....                                                 | 410 |
| Qué puede configurar .....                                                              | 410 |
| Activar el portal de acceso AWS .....                                                   | 410 |
| Personalización de la URL del portal de AWS acceso .....                                | 411 |
| Confirme que los usuarios puedan iniciar sesión en el portal de AWS acceso .....        | 412 |
| Utilice el portal de acceso AWS .....                                                   | 414 |
| Cómo utilizar el portal de acceso AWS .....                                             | 414 |
| Iniciar sesión en el portal de AWS acceso .....                                         | 415 |
| Restablecimiento de la contraseña .....                                                 | 417 |
| AWS CLI y acceso al AWS SDK .....                                                       | 419 |
| Crear enlaces de acceso directo .....                                                   | 424 |
| Registro de un dispositivo para MFA .....                                               | 427 |
| Finalización de la sesión activa .....                                                  | 429 |

|                                                                                                             |     |
|-------------------------------------------------------------------------------------------------------------|-----|
| Uso del Centro de Identidad de IAM en varios Regiones de AWS .....                                          | 431 |
| Ventajas del soporte multirregional .....                                                                   | 431 |
| Requisitos y consideraciones previos .....                                                                  | 431 |
| Elegir una región adicional .....                                                                           | 432 |
| Replique el centro de identidad de IAM en una región adicional .....                                        | 433 |
| Paso 1: Crear una clave de réplica .....                                                                    | 433 |
| Paso 2: Añadir la región .....                                                                              | 434 |
| Paso 3: Actualizar la configuración del IdP externo .....                                                   | 435 |
| Paso 4: Confirme las listas de permisos del firewall y la puerta de enlace .....                            | 436 |
| Paso 5: Proporcione información a sus usuarios .....                                                        | 436 |
| La región cambia después de añadir la primera región .....                                                  | 436 |
| ¿Qué datos se replican? .....                                                                               | 436 |
| Acceso de la fuerza laboral a través de una región adicional .....                                          | 438 |
| Sesiones de usuario en varios Regiones de AWS .....                                                         | 438 |
| AWS acceda a los puntos finales del portal en el principal y en el adicional Regiones de AWS .....          | 439 |
| Los puntos finales ACS son el principal y el adicional Regiones de AWS .....                                | 440 |
| Uso de aplicaciones AWS gestionadas sin varios ACS URLs .....                                               | 442 |
| Conmutación por error a una región adicional para acceder Cuenta de AWS .....                               | 442 |
| Cuenta de AWS resiliencia de acceso sin varios ACS URLs .....                                               | 443 |
| Implementación y administración de aplicaciones en múltiples Regiones de AWS .....                          | 444 |
| Implementación y administración de aplicaciones AWS administradas en múltiples Regiones de AWS .....        | 444 |
| Implementación y administración de aplicaciones administradas por los clientes en varias AWS regiones ..... | 446 |
| Eliminar una región del centro de identidad de IAM .....                                                    | 447 |
| Paso 1: Actualizar la configuración del IdP externo .....                                                   | 447 |
| Paso 2: Eliminar la región .....                                                                            | 447 |
| Paso 3: Eliminar la clave de réplica .....                                                                  | 448 |
| El servicio es APIs compatible en versiones adicionales Regiones de AWS .....                               | 449 |
| CloudTrail eventos en la región principal y en las regiones adicionales .....                               | 449 |
| Casos de uso del IAM Identity Center en la región principal y en las regiones adicionales .....             | 450 |
| Diseño de resiliencia y comportamiento regional .....                                                       | 453 |
| Diseñado para la disponibilidad .....                                                                       | 454 |
| Configure el acceso de emergencia al Consola de administración de AWS .....                                 | 454 |
| Resumen de la configuración del acceso de emergencia .....                                                  | 456 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Cómo diseñar sus roles de operaciones críticas .....                              | 456 |
| Cómo planificar su modelo de acceso .....                                         | 457 |
| Cómo diseñar una asignación de roles, cuentas y grupos de emergencia .....        | 458 |
| Cómo crear la configuración de acceso de emergencia .....                         | 459 |
| Tareas de preparación de emergencias .....                                        | 460 |
| Proceso de conmutación por error de emergencia .....                              | 460 |
| Volver a las operaciones normales .....                                           | 461 |
| Configuración única de una aplicación de federación de IAM directa en Okta .....  | 461 |
| Configuración única de una aplicación de federación de IAM directa con ADFS ..... | 465 |
| Seguridad .....                                                                   | 472 |
| Administración de identidades y accesos para IAM Identity Center .....            | 473 |
| Autenticación .....                                                               | 473 |
| Control de acceso .....                                                           | 473 |
| Información general sobre la administración del acceso .....                      | 474 |
| Ejemplos de políticas basadas en identidades .....                                | 478 |
| Ejemplo de política basada en recursos .....                                      | 487 |
| AWS políticas gestionadas .....                                                   | 489 |
| Cómo utilizar roles vinculados a servicios .....                                  | 511 |
| Consola de IAM Identity Center y autorización de la API .....                     | 519 |
| Acciones de la API después de noviembre de 2023 .....                             | 520 |
| Acciones de la API después de octubre de 2020 .....                               | 521 |
| AWS STS claves de condición para el Centro de Identidad de IAM .....              | 523 |
| UserId .....                                                                      | 524 |
| IdentityStoreArn .....                                                            | 524 |
| ApplicationArn .....                                                              | 525 |
| CredentialId .....                                                                | 525 |
| InstanceArn .....                                                                 | 525 |
| Registro y supervisión .....                                                      | 526 |
| Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail .....   | 526 |
| Registro del IAM Identity Center SCIM con AWS CloudTrail .....                    | 568 |
| Amazon EventBridge .....                                                          | 575 |
| Registro de errores de sincronización de AD configurable .....                    | 575 |
| Validación de conformidad .....                                                   | 578 |
| Estándares de conformidad admitidos .....                                         | 579 |
| Resiliencia .....                                                                 | 581 |
| Seguridad de la infraestructura .....                                             | 582 |

|                                                                                                                                                          |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Protección de datos .....                                                                                                                                | 583 |
| Cifrado en tránsito .....                                                                                                                                | 583 |
| Privacidad de datos .....                                                                                                                                | 584 |
| Retención de datos .....                                                                                                                                 | 584 |
| Cifrado en reposo .....                                                                                                                                  | 584 |
| Contexto de cifrado de IAM Identity Center .....                                                                                                         | 586 |
| Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente .....                                                    | 587 |
| Supervisión de claves de cifrado para IAM Identity Center .....                                                                                          | 587 |
| AWS el almacenamiento, el cifrado y la eliminación de los atributos de identidad del IAM Identity Center por parte de las aplicaciones gestionadas ..... | 587 |
| Implementación de claves KMS administradas por el cliente .....                                                                                          | 588 |
| Instrucciones básicas de KMS y políticas de IAM .....                                                                                                    | 599 |
| Instrucciones de política de claves de KMS avanzadas .....                                                                                               | 621 |
| Etiquetado de recursos .....                                                                                                                             | 631 |
| Restricciones de las etiquetas .....                                                                                                                     | 632 |
| Administre las etiquetas con la consola .....                                                                                                            | 632 |
| AWS CLI ejemplos .....                                                                                                                                   | 633 |
| Asignación de etiquetas .....                                                                                                                            | 633 |
| Visualización de etiquetas .....                                                                                                                         | 634 |
| Eliminación de etiquetas .....                                                                                                                           | 634 |
| Cómo aplicar etiquetas al crear un conjunto de permisos .....                                                                                            | 635 |
| Acciones de API de .....                                                                                                                                 | 635 |
| Integración de AWS CLI con IAM Identity Center .....                                                                                                     | 636 |
| Cómo integrar AWS CLI con IAM Identity Center .....                                                                                                      | 636 |
| Consideraciones sobre acceso privado .....                                                                                                               | 637 |
| Cuotas .....                                                                                                                                             | 638 |
| Cuotas de aplicaciones .....                                                                                                                             | 638 |
| Cuenta de AWS cuotas .....                                                                                                                               | 639 |
| Cuotas de Active Directory .....                                                                                                                         | 640 |
| Cuotas de almacén de identidades de IAM Identity Center .....                                                                                            | 640 |
| Límites de solicitudes de IAM Identity Center .....                                                                                                      | 641 |
| Cuotas de solicitud de servicio de OIDC .....                                                                                                            | 642 |
| Cuotas adicionales .....                                                                                                                                 | 643 |
| Resolución de problemas .....                                                                                                                            | 645 |
| Problemas al crear una instancia de cuenta de IAM Identity Center .....                                                                                  | 645 |

|                                                                                                                                                |     |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Recibe un error al intentar ver la lista de aplicaciones en la nube que están preconfiguradas para funcionar con IAM Identity Center .....     | 645 |
| Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center .....                                    | 647 |
| Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo .....                                      | 647 |
| Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo .....                               | 649 |
| Los usuarios no pueden iniciar sesión cuando su nombre de usuario está en formato UPN .....                                                    | 650 |
| Al modificar un rol de IAM, aparece el error: “No se puede realizar la operación en el rol protegido”. .....                                   | 650 |
| Los usuarios del directorio no pueden restablecer su contraseña .....                                                                          | 651 |
| En un conjunto de permisos se hace referencia a mi usuario, pero no puede acceder a las cuentas o aplicaciones asignadas .....                 | 652 |
| No puedo configurar correctamente mi aplicación del catálogo de aplicaciones .....                                                             | 652 |
| Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo .....              | 653 |
| Error: “No se pudieron habilitar los atributos del control de acceso” .....                                                                    | 654 |
| El mensaje “El navegador no es compatible” aparece cuando intento registrar un dispositivo para MFA .....                                      | 654 |
| El grupo “Usuarios de dominio” de Active Directory no se sincroniza correctamente con IAM Identity Center .....                                | 654 |
| Error de credenciales de MFA no válidas .....                                                                                                  | 655 |
| El mensaje “Se ha producido un error inesperado” aparece cuando intento registrarme o iniciar sesión con una aplicación de autenticación ..... | 655 |
| Aparece el mensaje de error “No es usted, somos nosotros” cuando intento iniciar sesión en IAM Identity Center .....                           | 655 |
| Mis usuarios no reciben correos electrónicos de IAM Identity Center .....                                                                      | 656 |
| Error: no puedes delete/modify/remove/assign acceder a los conjuntos de permisos aprovisionados en la cuenta de administración .....           | 656 |
| Error: no se encontró el token de sesión o no es válido .....                                                                                  | 656 |
| Los miembros del grupo de dominios de confianza no se sincronizan con el Centro de Identidad de IAM .....                                      | 657 |
| Solucione los problemas de las claves administradas por el cliente en AWS IAM Identity Center .....                                            | 657 |
| Acceso denegado: problema con el permiso de descifrado de KMS .....                                                                            | 657 |



|                                                                                                                                                                                                         |          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| AWS errores de inicio de sesión en aplicaciones gestionadas con una clave KMS gestionada por el cliente habilitada en el IAM Identity Center .....                                                      | 658      |
| AWS Se produce un error en la asignación and/or de usuarios durante la instalación de aplicaciones gestionadas con una clave KMS gestionada por el cliente y habilitada en el IAM Identity Center ..... | 658      |
| Problema de permisos de KMS: configurar la clave administrada por el cliente con AWS IAM Identity Center .....                                                                                          | 659      |
| AWS errores de inicio de sesión en el portal de acceso con una clave KMS gestionada por el cliente y habilitada en el IAM Identity Center .....                                                         | 659      |
| Solucione los problemas de configuración multirregional en AWS IAM Identity Center .....                                                                                                                | 660      |
| La región en la que quiero replicar mi instancia de IAM Identity Center no está disponible en la consola de IAM Identity Center .....                                                                   | 660      |
| AWS errores de inicio de sesión en aplicaciones gestionadas en otra región .....                                                                                                                        | 660      |
| Historial de revisión .....                                                                                                                                                                             | 661      |
| AWS Glosario .....                                                                                                                                                                                      | 672      |
| .....                                                                                                                                                                                                   | dclxxiii |

# ¿Qué es IAM Identity Center?

AWS IAM Identity Center es la AWS solución para conectar a los usuarios de su fuerza laboral con aplicaciones AWS gestionadas, como Kiro y Amazon Quick, y otros AWS recursos. Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien crear y gestionar sus usuarios directamente en el IAM Identity Center. A continuación, puede utilizar el IAM Identity Center para una de las siguientes opciones o para ambas:

- Acceso de los usuarios a las aplicaciones
- Acceso de los usuarios a Cuentas de AWS

## ¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo actuales para utilizar el IAM Identity Center y acceder a las aplicaciones AWS gestionadas. Si utiliza la [federación con IAM](#) para el Cuenta de AWS acceso, sus usuarios pueden seguir Cuentas de AWS accediendo de la misma manera que siempre lo han hecho, y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

## ¿Por qué utilizar el IAM Identity Center?

IAM Identity Center optimiza y simplifica el acceso de los usuarios del personal a las aplicaciones Cuentas de AWS, o a ambas, mediante las siguientes funciones clave.

### Integración con aplicaciones gestionadas AWS

[AWS administró aplicaciones](#) como Kiro e Amazon Redshift integró con IAM Identity Center. El IAM Identity Center proporciona a las aplicaciones AWS gestionadas una visión común de los usuarios y grupos.

### Propagación de identidad de confianza en aplicaciones

Gracias a la propagación de identidades fiable, las aplicaciones AWS gestionadas, como Amazon Quick, pueden compartir de forma segura la identidad de un usuario con otras aplicaciones AWS gestionadas, por ejemplo, Amazon Redshift y autorizar el acceso a AWS los recursos en función de la identidad del usuario. Puede auditar más fácilmente la actividad de los usuarios porque CloudTrail los eventos se registran en función del usuario y de las acciones que este haya

iniciado. De ese modo, resulta más sencillo entender quién ha accedido a qué. Para obtener información sobre los casos de uso compatibles, incluida end-to-end la guía de configuración, consulte [Casos de uso de propagación de identidades de confianza](#).

## Un lugar para asignar permisos a varias Cuentas de AWS

Con los permisos de varias cuentas, el IAM Identity Center ofrece un único lugar para asignar permisos a grupos de usuarios de varias Cuentas de AWS. Puede crear permisos basados en funciones laborales habituales o definir permisos personalizados que se adapten a sus necesidades de seguridad. A continuación, puede asignar esos permisos a los usuarios de la fuerza laboral para controlar su acceso a determinados recursos Cuentas de AWS.

Esta característica opcional solo está disponible para las [instancias de organización](#) de IAM Identity Center.

## Un punto de federación para simplificar el acceso de los usuarios a AWS

Al proporcionar un punto de federación, IAM Identity Center reduce el esfuerzo administrativo necesario para utilizar varias aplicaciones AWS gestionadas y Cuentas de AWS. Con IAM Identity Center, solo se federa una vez y solo se tiene que gestionar un certificado cuando se utiliza un proveedor de identidades de [SAML 2.0](#). El IAM Identity Center proporciona a las aplicaciones AWS gestionadas una visión común de los usuarios y grupos para casos prácticos de propagación de identidades fiables o cuando los usuarios comparten el acceso a los AWS recursos con otras personas.

Para obtener información acerca de cómo configurar los proveedores de identidad de uso habitual para que funcionen con el IAM Identity Center, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#). Si no tiene un proveedor de identidad existente, puede [crear y gestionar usuarios directamente en el IAM Identity Center](#).

## Dos tipos de instancias

IAM Identity Center admite dos tipos de instancias: las instancias de organización y las instancias de cuenta. La práctica recomendada es usar una instancia de organización. Es la única instancia que le permite administrar el acceso a las aplicaciones Cuentas de AWS y se recomienda para todo uso de producción de las mismas. Se implementa una instancia de organización en la cuenta AWS Organizations de administración y proporciona un punto único desde el que gestionar el acceso de los usuarios AWS.

Las instancias de cuenta están vinculadas al lugar Cuenta de AWS en el que están habilitadas. Utilice las instancias de cuenta del IAM Identity Center únicamente para admitir despliegues

aislados de determinadas aplicaciones AWS gestionadas. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Portal web de fácil acceso para sus usuarios

El portal de AWS acceso es un portal web fácil de usar que proporciona a sus usuarios un acceso sin problemas a todas las aplicaciones asignadas Cuentas de AWS, o a ambas.

## Acceso y aplicaciones Cuentas de AWS multirregionales

Al replicar su instancia del IAM Identity Center en otras regiones, sus empleados pueden acceder a las aplicaciones Cuentas de AWS y a las que tienen asignadas a través de todas las regiones habilitadas, y pueden implementar aplicaciones AWS gestionadas en cada región habilitada.

# Cambio de nombre de IAM Identity Center

El 26 de julio de 2022, AWS Single Sign-On pasó a llamarse. AWS IAM Identity Center

## Los espacios de nombres antiguos siguen siendo los mismos

Los espacios de nombres de sso y identitystore API, junto con los siguientes espacios de nombres relacionados, permanecen sin cambios por motivos de compatibilidad con versiones anteriores.

- Comandos de la CLI
  - [aws configure sso](#)
  - [identitystore](#)
  - [sso](#)
  - [sso-admin](#)
  - [sso-oidc](#)
- [Políticas administradas](#) que contienen prefijos de AWSSSO y AWSIdentitySync
- [Puntos de conexión de servicio](#) que contienen sso e identitystore
- Recursos de [CloudFormation](#) contienen prefijos de AWS::SSO
- [Rol vinculado al servicio](#) que contiene AWSServiceRoleForSSO
- Consola URLs que contiene y sso singlessignon
- Documentación URLs que contiene singlessignon

# Introducción al IAM Identity Center

A continuación se describe cómo comenzar a utilizar IAM Identity Center.

## 1. Activar IAM Identity Center

Al [activar IAM Identity Center](#), puede elegir entre dos tipos de instancias de IAM Identity Center. Estos tipos son las [instancias de organización](#) (recomendadas) y las [instancias de cuentas](#). Para obtener más información sobre las distintas funciones de estos tipos de instancias, consulte [Organization and account instances of IAM Identity Center](#).

### Note

Una vez activado IAM Identity Center, puede iniciar sesión y abrir la [consola de IAM Identity Center](#) mediante una de las siguientes acciones:

- Instancia de organización: inicie sesión para AWS usar credenciales con permisos administrativos en la cuenta de administración.
- Instancia de cuenta: inicie sesión con AWS credenciales con permisos administrativos en la ubicación en la Cuenta de AWS que el Centro de Identidad de IAM esté activado.

## 2. Conectar su origen de identidad de IAM Identity Center

En la consola de IAM Identity Center, confirme el origen de identidad que desee utilizar. Consulte lo siguiente para ver los orígenes de identidad:

- Proveedor de identidad externo: si ya tiene un proveedor de identidades para administrar los usuarios de su personal, puede conectarlo a IAM Identity Center. Para obtener más información acerca de cómo configurar los proveedores de identidad de uso habitual para que funcionen con IAM Identity Center, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#).
- Active Directory: si utiliza Active Directory para administrar los usuarios de su personal, puede conectarlo a IAM Identity Center. Para obtener más información, consulte [Uso de Active Directory como origen de identidad](#).
- IAM Identity Center: también puede [crear y administrar usuarios y grupos directamente en IAM Identity Center](#).

 Note

Actualmente, debe utilizar un proveedor de identidad externo como fuente de identidad para aprovechar una configuración multirregional con su centro de identidad de IAM. Para obtener más información sobre las ventajas de esta configuración, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#)

### 3. Configure el acceso de los usuarios a Cuentas de AWS (solo a la instancia de la organización)

Si utiliza una instancia de organización del Centro de identidades de IAM, puede [asignar el acceso de un usuario o grupo a Cuentas de AWS](#), utilizando [conjuntos de permisos](#) para conceder a sus usuarios acceso a los recursos Cuentas de AWS y a los recursos.

### 4. Configuración del acceso del usuario a las aplicaciones

Con IAM Identity Center, puede conceder a los usuarios acceso a dos tipos de aplicaciones:

#### a. [AWS aplicaciones gestionadas](#)

- Puede utilizar IAM Identity Center con aplicaciones AWS gestionadas como Amazon Q Business y Amazon Redshift. AWS CLI Para obtener más información, consulte [AWS aplicaciones gestionadas](#) y [Integración de AWS CLI con IAM Identity Center](#).

#### b. [Aplicaciones administradas por el cliente](#)

- Puede integrar cualquiera de los siguientes tipos de aplicaciones administradas por el cliente con IAM Identity Center:
  - [Aplicaciones incluidas en el catálogo de IAM Identity Center](#)
  - [Sus aplicaciones personalizadas](#)
- Tras configurar la aplicación, puede [asignar a sus usuarios el acceso a la aplicación](#).

### 5. Proporcionar a sus usuarios las instrucciones de inicio de sesión para el portal de acceso de AWS

El portal de AWS acceso es un portal web que proporciona a sus usuarios un acceso sin problemas a todas las aplicaciones asignadas Cuentas de AWS, o a ambas. Los nuevos usuarios del Centro de Identidad de IAM deben activar sus credenciales de usuario antes de poder iniciar sesión en el portal de AWS acceso.

Para obtener información sobre cómo iniciar sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario. Para obtener más

información sobre el proceso de inicio de sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#).

## Requisitos previos y consideraciones sobre el IAM Identity Center

Puede utilizar IAM Identity Center para acceder únicamente a las aplicaciones AWS gestionadas, Cuentas de AWS únicamente o a ambas. Si utiliza la federación de IAM para gestionar el acceso Cuentas de AWS, puede seguir haciéndolo mientras utiliza el IAM Identity Center para acceder a las aplicaciones.

Antes de habilitar IAM Identity Center, considere lo siguiente:

- AWS Región

Primero debe habilitar el Centro de Identidad de IAM en una sola región [compatible](#) para cada instancia del Centro de Identidad de IAM. Si desea utilizar IAM Identity Center para acceder a las cuentas de AWS mediante un único inicio de sesión, todos los usuarios de su organización deben poder acceder a la región. Si piensa utilizar el Centro de identidad de IAM para acceder a las aplicaciones, tenga en cuenta que algunas aplicaciones AWS gestionadas, como Amazon SageMaker AI, solo pueden funcionar en las regiones que admiten. Además, la mayoría de las aplicaciones AWS administradas requieren que el Centro de Identidad de IAM esté disponible en la misma región que la aplicación. Esto puede lograrse ubicándolas en la misma región o, si es posible, replicando la instancia del IAM Identity Center en la región de despliegue deseada de una aplicación gestionada. AWS Para obtener más información, consulte [Consideraciones para elegir un Región de AWS](#).

- Acceso de aplicaciones

Puede usar el Centro de identidad de IAM solo para que los usuarios accedan a aplicaciones como Kiro, utilizando su proveedor de identidad actual. Para obtener más información, consulte [Uso del IAM Identity Center únicamente para el acceso de los usuarios a las aplicaciones](#).

 Note

El propietario de la aplicación administra de forma independiente el acceso a los recursos de la aplicación.

- Cuota de roles de IAM

IAM Identity Center crea roles de IAM para conceder a los usuarios permisos a los recursos de la cuenta. Para obtener más información, consulte [Roles de IAM creados por IAM Identity Center](#).

- Centro de identidad de IAM y AWS Organizations

AWS Organizations se recomienda, pero no es obligatorio, para su uso con el Centro de identidades de IAM. Si no ha configurado una organización, no tiene que hacerlo. Si ya ha configurado el Centro de Identidad de IAM AWS Organizations y lo va a añadir a su organización, asegúrese de que todas las AWS Organizations funciones estén habilitadas. Para obtener más información, consulte [Centro de identidad de IAM y AWS Organizations](#).

Las interfaces web del IAM Identity Center, incluidos el portal de acceso y la consola del IAM Identity Center, están pensadas para que las personas puedan acceder a ellas a través de navegadores web compatibles. Los navegadores compatibles incluyen las tres últimas versiones de Microsoft Edge, Mozilla Firefox, Google Chrome y Apple Safari. No se admite el acceso a estos puntos finales mediante rutas que no estén basadas en el navegador. Para el acceso programático a los servicios del Centro de Identidad de IAM, recomendamos utilizar la documentación APIs disponible en las guías de referencia del Centro de Identidad de IAM y la API de Identity Store.

## Consideraciones para elegir un Región de AWS

Puede activar el Centro de Identidad de IAM en una sola unidad, con el soporte Región de AWS que prefiera y que esté disponible para los usuarios de todo el mundo. Esta disponibilidad global le facilita la configuración del acceso de los usuarios a múltiples Cuentas de AWS aplicaciones. Las siguientes son consideraciones clave para elegir una Región de AWS.

- Ubicación geográfica de sus usuarios: si selecciona una región que esté geográficamente más cercana a la mayoría de sus usuarios finales, estos tendrán una latencia de acceso más baja al portal de AWS acceso y a las aplicaciones AWS gestionadas, como Amazon SageMaker AI.
- Regiones de suscripción voluntaria (regiones que están deshabilitadas de forma predeterminada): una región de suscripción voluntaria es aquella Región de AWS que está deshabilitada de forma predeterminada. Debe activar la región registrada para utilizarla. Para obtener más información, consulte [Managing IAM Identity Center in an opt-in Region](#).
- Replicación del centro de identidad de IAM en regiones adicionales: si planea replicar el centro de identidad de IAM en más regiones Regiones de AWS, debe elegir una región que esté habilitada de forma predeterminada. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).



- Selección de regiones de despliegue para las aplicaciones AWS gestionadas: las aplicaciones AWS gestionadas solo pueden funcionar en las regiones Regiones de AWS en las que estén disponibles. Muchas aplicaciones AWS gestionadas también pueden funcionar solo en una región en la que el Centro de Identidad de IAM esté activado o en la que esté replicado (región principal o adicional). Para confirmar si su instancia del IAM Identity Center admite la replicación en regiones adicionales, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#). Si la replicación no es una opción, considere habilitar el IAM Identity Center en la región en la que planea usar las aplicaciones AWS administradas.
- Soberanía digital: las normas de soberanía digital o las políticas de la empresa pueden exigir el uso de una determinada Región de AWS. Consulte con el departamento legal de su empresa.
- Fuente de identidad: si utiliza [AWS Managed Microsoft AD](#) su directorio autogestionado de [Active Directory \(AD\)](#) como fuente de identidad, su región de origen debe coincidir con la región Región de AWS en la que habilitó el IAM Identity Center.
- Correos electrónicos entre regiones con Amazon Simple Email Service: en algunas regiones, IAM Identity Center puede llamar a [Amazon Simple Email Service \(Amazon SES\)](#) de una región diferente para enviar correos electrónicos. En estas llamadas entre regiones, el IAM Identity Center envía determinados atributos de usuario a la otra región. Para obtener más información, consulte [Correos electrónicos entre regiones con Amazon SES](#).
- AWS Control Tower— Si habilitas una instancia de organización del IAM Identity Center desde AWS Control Tower, la instancia se creará en la misma región que la AWS Control Tower landing zone.

## Temas

- [Operaciones y almacenamiento de datos regionales de IAM Identity Center](#)
- [Conmutación Regiones de AWS](#)
- [Deshabilitar un Región de AWS lugar donde el Centro de identidad de IAM esté activado](#)

## Operaciones y almacenamiento de datos regionales de IAM Identity Center

Descubra cómo IAM Identity Center gestiona el almacenamiento de datos y las operaciones en todas las Regiones de AWS.

Comprenda cómo IAM Identity Center almacena los datos

Al activar el Centro de identidades de IAM, todos los datos que configure en el Centro de identidades de IAM se almacenan en la región en la que los haya activado. Estos datos incluyen configuraciones

de directorios, conjuntos de permisos, instancias de aplicaciones y asignaciones de usuarios a Cuenta de AWS las aplicaciones. Si utiliza el almacén de identidades de IAM Identity Center, todos los usuarios y grupos que cree en IAM Identity Center también se almacenan en la misma región. Si replica tu instancia del Centro de Identidad de IAM en otras regiones, el Centro de Identidad de IAM replica automáticamente los usuarios, los grupos, los conjuntos de permisos y sus asignaciones, así como otros metadatos y configuraciones en esas regiones.

## Correos electrónicos entre regiones con Amazon SES

IAM Identity Center utiliza [Amazon Simple Email Service \(Amazon SES\)](#) para enviar correos electrónicos a los usuarios finales cuando estos intentan iniciar sesión con una contraseña de un solo uso (OTP) como segundo factor de autenticación. Estos correos electrónicos también se envían para determinados eventos de administración de identidades y credenciales, como cuando se invita al usuario a configurar una contraseña inicial, verificar una dirección de correo electrónico y restablecer la contraseña. Amazon SES está disponible en un subconjunto de los Regiones de AWS que admite IAM Identity Center.

IAM Identity Center llama a los puntos de conexión locales de Amazon SES cuando Amazon SES está disponible localmente en una Región de AWS. Cuando Amazon SES no está disponible localmente, IAM Identity Center llama a los puntos de conexión de Amazon SES que se encuentren en una Región de AWS diferente, como se indica en la siguiente tabla.

| Código de región de IAM Identity Center | Nombre de región de IAM Identity Center | Código de región de Amazon SES | Nombre de región de Amazon SES |
|-----------------------------------------|-----------------------------------------|--------------------------------|--------------------------------|
| ap-east-1                               | Asia-Pacífico (Hong Kong)               | ap-northeast-2                 | Asia-Pacífico (Seúl)           |
| ap-east-2                               | Asia-Pacífico (Taipei)                  | ap-northeast-1                 | Asia-Pacífico (Tokio)          |
| ap-south-2                              | Asia-Pacífico (Hyderabad)               | ap-south-1                     | Asia-Pacífico (Mumbai)         |
| ap-southeast-4                          | Asia-Pacífico (Melbourne)               | ap-southeast-2                 | Asia-Pacífico (Sídney)         |
| ap-southeast-5                          | Asia-Pacífico (Malasia)                 | ap-southeast-1                 | Asia-Pacífico (Singapur)       |

| Código de región de IAM Identity Center | Nombre de región de IAM Identity Center | Código de región de Amazon SES | Nombre de región de Amazon SES      |
|-----------------------------------------|-----------------------------------------|--------------------------------|-------------------------------------|
| ap-southeast-6                          | Asia-Pacífico (Nueva Zelanda)           | ap-southeast-2                 | Asia-Pacífico (Sídney)              |
| ap-southeast-7                          | Asia-Pacífico (Tailandia)               | ap-northeast-3                 | Asia-Pacífico (Osaka)               |
| ca-west-1                               | Oeste de Canadá (Calgary)               | ca-central-1                   | Canadá (centro)                     |
| eu-south-2                              | Europa (España)                         | eu-west-3                      | Europa (París)                      |
| eu-central-2                            | Europa (Zúrich)                         | eu-central-1                   | Europa (Fráncfort)                  |
| mx-central-1                            | México (centro)                         | us-east-2                      | Este de EE. UU. (Ohio)              |
| me-central-1                            | Medio Oriente (EAU)                     | eu-central-1                   | Europa (Fráncfort)                  |
| us-gov-east-1                           | AWS GovCloud (Este de EE. UU.)          | us-gov-west-1                  | AWS GovCloud (Estados Unidos-Oeste) |

En estas llamadas entre regiones, IAM Identity Center puede enviar los siguientes atributos de usuario:

- Dirección de correo electrónico
- Nombre
- Apellido
- Cuenta en AWS Organizations
- AWS URL del portal de acceso
- Nombre de usuario
- ID de directorio
- ID de usuario

Administrar IAM Identity Center en una región de activación opcional (región que está deshabilitada de forma predeterminada)

La mayoría Regiones de AWS están habilitadas para funcionar en todos los AWS servicios de forma predeterminada, pero debe habilitar las siguientes [regiones de suscripción](#) si quiere utilizar el Centro de identidad de IAM:

- África (Ciudad del Cabo)
- Asia Pacific (Hong Kong)
- Asia-Pacífico (Taipéi)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Nueva Zelanda)
- Asia-Pacífico (Tailandia)
- Oeste de Canadá (Calgary)
- Europa (Milán)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- México (centro)
- Middle East (Bahrain)
- Medio Oriente (EAU)

Si implementa IAM Identity Center en una región de activación opcional, debe habilitar esta región en todas las cuentas para las que desee administrar el acceso a IAM Identity Center. Todas las cuentas necesitan esta configuración, independientemente de si va a crear recursos en esa región o no.

Puede habilitar una región para las cuentas actuales de su organización y debe repetir esta acción cuando agrega cuentas nuevas. Para obtener instrucciones, consulte [Enable or disable a Region in your organization](#) en la Guía del usuario de AWS Organizations . Para evitar repetir estos pasos adicionales, puede optar por implementar su IAM Identity Center en una [Región habilitada de forma predeterminada](#).

 Note

Su cuenta de AWS miembro debe estar habilitada en la misma región que la región en la que se encuentra su instancia del Centro de Identidad de IAM para que pueda acceder a la cuenta de AWS miembro desde el portal de acceso. AWS

## Metadatos almacenados en regiones de activación opcional

Al habilitar el Centro de Identidad de IAM para una cuenta de administración en una suscripción voluntaria Región de AWS, los siguientes metadatos del Centro de Identidad de IAM correspondientes a cualquier cuenta de miembro se almacenan en la región.

- ID de cuenta
- Nombre de cuenta
- Correo electrónico de la cuenta
- Nombres de recursos de Amazon (ARNs) de las funciones de IAM que el Centro de Identidad de IAM crea en la cuenta del miembro

## Regiones de AWS que están habilitados de forma predeterminada

Las siguientes regiones están habilitadas de forma predeterminada, y puede habilitar IAM Identity Center en estas regiones.

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- Oeste de EE. UU. (Norte de California)
- Europa (París)
- América del Sur (São Paulo)
- Asia-Pacífico (Mumbai)
- Europa (Estocolmo)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Tokio)
- Europa (Irlanda)

- Europa (Fráncfort)
- Europa (Londres)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Canadá (centro)
- Asia-Pacífico (Osaka)

## Conmutación Regiones de AWS

Le recomendamos que instale IAM Identity Center en una región que desee mantener disponible para los usuarios, no en una región que pueda tener que deshabilitar. Para obtener más información, consulte [Consideraciones para elegir un Región de AWS](#).

Para cambiar de región en IAM Identity Center, solo tiene que [eliminar la instancia actual de IAM Identity Center](#) y crear una nueva en otra región. Si ya ha activado una aplicación administrada por AWS con su instancia existente de IAM Identity Center, desactive la aplicación antes de eliminarla de IAM Identity Center. Para obtener instrucciones sobre cómo deshabilitar las aplicaciones AWS administradas, consulte [Deshabilitar una aplicación AWS gestionada](#).

### Note

Si está pensando en cambiar la región del centro de identidad de IAM para permitir el despliegue de una aplicación AWS gestionada en otra región, considere replicar la instancia del centro de identidad de IAM en esa región. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).

## Consideraciones de configuración en la nueva región

Debe volver a crear los usuarios, los grupos, los conjuntos de permisos, las aplicaciones y las asignaciones en la nueva instancia de IAM Identity Center. Puede utilizar la asignación de cuentas y aplicaciones del IAM Identity Center [APIs](#) para obtener una instantánea de la configuración y, a continuación, utilizarla para volver a crear la configuración en una nueva región. Al cambiar a otra región, también se cambia la URL del [portal de AWS acceso](#), lo que proporciona a los usuarios un acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones. Es posible que también necesite volver a crear parte de la configuración de IAM Identity Center a través de la consola de administración de la nueva instancia.

## Deshabilitar un Región de AWS lugar donde el Centro de identidad de IAM esté activado

Si deshabilita una Región de AWS en la que esté instalado el Centro de Identidad de IAM, el Centro de Identidad de IAM también estará deshabilitado. Una vez deshabilitado IAM Identity Center en una región, los usuarios de esa región no tendrán acceso mediante un inicio de sesión único a las Cuentas de AWS y sus aplicaciones.

Para volver a activar el Centro de Identidad de IAM de forma [opcional Regiones de AWS](#), debe volver a activar la región. IAM Identity Center debe volver a procesar todos los eventos pausados, por lo que volver a habilitarlo puede llevar algún tiempo.

### Note

El Centro de Identidad de IAM solo puede gestionar el acceso a aquellas Cuentas de AWS que estén habilitados para su uso en una Región de AWS. Para gestionar el acceso a todas las cuentas de su organización, active el Centro de identidad de IAM en la cuenta de gestión de forma Región de AWS que se active automáticamente para su uso con el Centro de identidades de IAM.

Para obtener más información sobre la activación y la desactivación Regiones de AWS, consulte [Gestión Regiones de AWS en la AWS referencia general](#).

## Uso del IAM Identity Center únicamente para el acceso de los usuarios a las aplicaciones

Puede utilizar el Centro de identidad de IAM para que los usuarios accedan a aplicaciones como Kiro o a Cuentas de AWS ambas. Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien [crear y gestionar usuarios directamente en el IAM Identity Center](#). Para obtener información sobre cómo conectar su proveedor de identidad actual al IAM Identity Center, consulte el [Tutoriales de orígenes de identidad de IAM Identity Center](#).

¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo actuales para utilizar el IAM Identity Center y acceder a las aplicaciones AWS gestionadas. Si utiliza la [federación con IAM](#) para el Cuenta de AWS acceso, sus usuarios pueden seguir Cuentas de AWS accediendo de

la misma manera que siempre lo han hecho, y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

## Roles de IAM creados por IAM Identity Center

Al asignar un usuario a una AWS cuenta, el Centro de Identidad de IAM crea funciones de IAM para conceder a los usuarios permisos de acceso a los recursos.

Cuando asigna un conjunto de permisos, el IAM Identity Center crea los roles de IAM controlados por el IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de Identidad de IAM administra la función y permite que los usuarios autorizados que haya definido la asuman mediante el portal de acceso o. AWS CLI A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia. La replicación de su instancia del IAM Identity Center en regiones adicionales no afecta a las funciones de IAM existentes ni crea nuevas funciones de IAM.

### Note

Los conjuntos de permisos no se utilizan para conceder permisos a aplicaciones.

Si ya has configurado funciones de IAM en tu cuenta Cuenta de AWS, te recomendamos que compruebes si tu cuenta se acerca a la cuota de funciones de IAM. La cuota predeterminada de roles de IAM por cuenta es de 1000 roles. Para obtener más información, consulte [Cuotas de objetos de IAM](#).

Si se acerca a la cuota, considere solicitar un aumento de la cuota. De lo contrario, es posible que tenga problemas con IAM Identity Center al aprovisionar conjuntos de permisos a cuentas que hayan superado la cuota de roles de IAM. Para obtener información sobre cómo solicitar un aumento de cuota, consulte [Solicitar un aumento de cuota](#) en la Guía del usuario de Service Quotas.

### Note

Si quiere revisar los roles de IAM en una cuenta que ya utiliza IAM Identity Center, es posible que observe que los nombres de rol comienzan por “AWSReservedSSO\_”. Se trata de los roles que el servicio de IAM Identity Center ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta.



## Centro de identidad de IAM y AWS Organizations

AWS Organizations se recomienda, pero no es obligatorio, para su uso con el Centro de identidades de IAM. Si no ha configurado una organización, no tiene que hacerlo. Al activar el Centro de Identidad de IAM, elegirá si desea habilitar el servicio con. AWS Organizations Al configurar una organización, la cuenta Cuenta de AWS que la configura se convierte en la cuenta de administración de la organización. El usuario raíz de la Cuenta de AWS es ahora el propietario de la cuenta de administración de la organización. Todas las Cuentas de AWS adicionales que invite a su organización son cuentas de miembro. La cuenta de administración crea los recursos, las unidades organizativas y las políticas de la organización que administran las cuentas de miembro. La cuenta de administración delega los permisos a las cuentas de miembro.

### Note

Le recomendamos que habilite el Centro de Identidad de IAM con AWS Organizations, lo que crea una instancia de organización del Centro de Identidad de IAM. Nuestra práctica recomendada es una instancia de organización, ya que es compatible con todas las características de IAM Identity Center y proporciona capacidades de administración centralizada. Para obtener más información, consulte [Instancias de organización de IAM Identity Center](#).

Si ya ha configurado el Centro de Identidad de IAM AWS Organizations y lo va a añadir a su organización, asegúrese de que todas las AWS Organizations funciones estén habilitadas. Al crear una organización, las características se habilitan de manera predeterminada. Para obtener más información, consulte [Habilitar todas las características en la organización](#) en la Guía del usuario de AWS Organizations .

Para habilitar una instancia de organización del Centro de identidades de IAM, debe iniciar sesión en su cuenta de AWS Organizations administración como usuario con credenciales administrativas o como usuario raíz (no se recomienda a menos que no existan otros usuarios administrativos). Consola de administración de AWS Para obtener más información, consulte [Creación y administración de una AWS organización](#) en la Guía del AWS Organizations usuario.

Si ha iniciado sesión con las credenciales administrativas de una cuenta de AWS Organizations miembro, puede habilitar una instancia de cuenta del IAM Identity Center. Las instancias de cuentas tienen capacidades limitadas y están vinculadas a una sola AWS cuenta.

# Instancias de organización y cuenta de IAM Identity Center

Una instancia es una implementación única de IAM Identity Center. Hay dos tipos de instancias disponibles para IAM Identity Center: las instancias de organización y las instancias de cuenta.

- Instancia de organización (recomendada)

Una instancia de IAM Identity Center que se habilita en la cuenta AWS Organizations de administración. Las instancias de organización son compatibles con todas las características de IAM Identity Center. Le recomendamos que implemente una instancia de organización en lugar de una instancia de cuenta para minimizar la cantidad de puntos de administración.

- Instancia de cuenta

Una instancia del IAM Identity Center que está vinculada a una única Cuenta de AWS instancia y que solo es visible en la Cuenta de AWS AWS región en la que está habilitada. Utilice una instancia de cuenta para situaciones más sencillas de una sola cuenta. Puede habilitar una instancia de cuenta a partir de cualquiera de las siguientes opciones:

- Y Cuenta de AWS eso no lo gestiona AWS Organizations
- Una cuenta de miembro en AWS Organizations

## Cuenta de AWS tipos que pueden habilitar el IAM Identity Center

Para habilitar el Centro de identidades de IAM, inicie sesión en Consola de administración de AWS el con una de las siguientes credenciales, en función del tipo de instancia que desee crear:

- Su cuenta AWS Organizations de administración (recomendada): necesaria para crear una [instancia organizativa](#) del IAM Identity Center. Utilice una instancia de organización para los permisos de varias cuentas y las asignaciones de aplicaciones en toda la organización.
- Su cuenta de AWS Organizations miembro: utilícela para crear una [instancia de cuenta](#) del IAM Identity Center para permitir la asignación de solicitudes dentro de esa cuenta de miembro. En una organización pueden existir una o más cuentas con una instancia de nivel de miembro.
- Una instancia independiente Cuenta de AWS: se utiliza para crear una instancia de [organización o una instancia de cuenta](#) del IAM Identity Center. La versión independiente Cuenta de AWS no está gestionada por. AWS Organizations Solo puede asociar una instancia del IAM Identity Center a una instancia independiente Cuenta de AWS y utilizarla para las asignaciones de aplicaciones dentro de esa instancia independiente. Cuenta de AWS

Use la siguiente tabla para comparar las capacidades que ofrece el tipo de instancia:

| Funcionalidad                                                                                     | Instancia en la cuenta de AWS Organizations administración (recomendado)               | Instancia en una cuenta de miembro                                                     | Instancia en una instancia independiente Cuenta de AWS                                   |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Administración de usuarios                                                                        |  Sí   |  Sí   |  Sí   |
| AWS portal de acceso para acceder con un solo inicio de sesión a sus aplicaciones gestionadas AWS |  Sí   |  Sí   |  Sí   |
| OAuth Aplicaciones 2.0 (OIDC) administradas por el cliente                                        |  Sí  |  Sí  |  Sí  |
| Permisos para varias cuentas                                                                      |  Sí |  No |  No |
| AWS portal de acceso para acceder con un solo inicio de sesión a su Cuentas de AWS                |  Sí |  No |  No |
| Aplicaciones de SAML 2.0 administradas por el cliente                                             |  Sí |  No |  No |
| El administrador delegado puede                                                                   |  Sí |  No |  No |

| Funcionalidad                                                        | Instancia en la cuenta de AWS Organizations administración (recomendado)            | Instancia en una cuenta de miembro                                                  | Instancia en una instancia independiente Cuenta de AWS                                 |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| administrar la instancia                                             |                                                                                     |                                                                                     |                                                                                        |
| Cifrado en reposo mediante una clave KMS administrada por el cliente |  S |  N |  No |
| Replicación del centro de identidad de IAM en regiones adicionales   |  S |  N |  No |

Para obtener más información sobre las aplicaciones AWS gestionadas y el Centro de identidad de IAM, consulte. [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#)

## Temas

- [Instancias de organización de IAM Identity Center](#)
- [Instancias de cuenta de IAM Identity Center](#)
- [Eliminación de la instancia de IAM Identity Center](#)

## Instancias de organización de IAM Identity Center

Al activar el Centro de Identidad de IAM junto con AWS Organizations, se crea una instancia organizativa del Centro de Identidad de IAM. La instancia de organización debe estar habilitada en su cuenta de administración y puede administrar de forma centralizada el acceso de los usuarios y grupos con una sola instancia de organización. Solo puede tener una instancia de organización para cada cuenta de administración de AWS Organizations.

Si habilitó IAM Identity Center antes del 15 de noviembre de 2023, tiene una instancia de organización de IAM Identity Center.

Para habilitar una instancia de organización del IAM Identity Center, consulte [Para habilitar una instancia de cuenta de IAM Identity Center](#).

## Cuándo usar una instancia de organización

Las instancias de organización son el método principal para activar IAM Identity Center y, con frecuencia, se recomienda usar una instancia de organización. Las instancias de organización ofrecen los siguientes beneficios:

- Support para todas las funciones de IAM Identity Center, incluida la administración de permisos para varios Cuentas de AWS miembros de su organización, la asignación del acceso a las aplicaciones administradas por el cliente y la replicación multirregional.
- Reducción de la cantidad de puntos de administración: una instancia de organización tiene un único punto de administración, que es la cuenta de administración. Le recomendamos que habilite una instancia de organización en lugar de una instancia de cuenta para reducir la cantidad de puntos de administración.
- Control centralizado de la creación de instancias de cuentas: puede controlar si las cuentas de los miembros de su organización pueden crear instancias de cuentas, siempre y cuando no haya implementado una instancia del Centro de Identidad de IAM en su organización en una región habilitada (Región de AWS esta opción está desactivada de forma predeterminada).

Para obtener instrucciones a fin de habilitar una instancia de organización de IAM Identity Center, consulte [Para habilitar una instancia de cuenta de IAM Identity Center](#).

## Instancias de cuenta de IAM Identity Center

Con una instancia de cuenta de IAM Identity Center, puede implementar aplicaciones AWS gestionadas compatibles y aplicaciones gestionadas por clientes basadas en el OIDC. Las instancias de cuentas permiten el despliegue aislado de aplicaciones en una sola aplicación Cuenta de AWS, aprovechando las funciones del portal de acceso e identidad de los empleados de IAM Identity Center.

Las instancias de cuenta están vinculadas a una sola cuenta Cuenta de AWS y se utilizan únicamente para gestionar el acceso de usuarios y grupos a las aplicaciones compatibles de la misma cuenta y. Región de AWS Está limitado a una instancia de cuenta por Cuenta de AWS. Puedes crear una instancia de cuenta a partir de una de las siguientes opciones: una cuenta de miembro AWS Organizations o una cuenta independiente Cuenta de AWS que no esté gestionada por AWS Organizations.

Para obtener instrucciones sobre cómo habilitar una instancia de cuenta de IAM Identity Center, consulte [Para habilitar una instancia de cuenta de IAM Identity Center](#) y seleccione la pestaña Cuenta.

## Cuándo usar la instancia de cuenta

En la mayoría de los casos, se recomienda usar una [instancia de organización](#). Use las instancias de cuenta solo si se da una de las siguientes situaciones:

- Desea ejecutar una prueba temporal de una aplicación AWS gestionada compatible para determinar si la aplicación se adapta a las necesidades de su empresa.
- No tiene previsto adoptar el IAM Identity Center en toda su organización, pero quiere dar soporte a una o más aplicaciones AWS gestionadas.
- Tiene una instancia de organización de IAM Identity Center, pero desea implementar una aplicación administrada por AWS compatible en un conjunto aislado de usuarios que son distintos de los usuarios de la instancia de organización.
- No controla la AWS organización en la que opera. Por ejemplo, un tercero controla la AWS organización que administra su Cuentas de AWS.

### Important

Si piensa utilizar IAM Identity Center para admitir aplicaciones en varias cuentas, cree una instancia de organización. Las instancias de cuentas no admiten este caso de uso.

## AWS aplicaciones administradas que admiten instancias de cuentas

Consulte [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#) para saber qué aplicaciones AWS gestionadas son compatibles con las instancias de cuentas de IAM Identity Center. Compruebe la disponibilidad de la creación de instancias de cuentas con su aplicación AWS gestionada.

## Restricciones de disponibilidad de las cuentas de los miembros

Para implementar instancias de cuentas del IAM Identity Center en las cuentas de AWS Organizations los miembros, debe cumplirse una de las siguientes condiciones:

- No hay ninguna instancia de organización del IAM Identity Center en su organización de .

- Hay una instancia de organización de IAM Identity Center en su organización y el administrador de la instancia permite la creación de instancias de cuentas de IAM Identity Center (para las instancias de la organización creadas después del 15 de noviembre de 2023).
- Hay una instancia de organización del IAM Identity Center en su organización y el administrador de la instancia ha habilitado manualmente la creación de instancias de cuentas por parte de las cuentas de los miembros de la organización (en el caso de las instancias de la organización creadas antes del 15 de noviembre de 2023). Para obtener instrucciones, consulte [Permiso para la creación de instancias de cuentas en las cuentas de miembros](#).

Cuando se cumpla una de las condiciones anteriores, todas las siguientes condiciones deben ser verdaderas:

- El administrador no ha creado ninguna [política de control de servicio](#) que impida a las cuentas de los miembros crear instancias de cuenta.
- Independientemente de la Región de AWS, no tiene una instancia de IAM Identity Center en esta misma cuenta.
- Trabaja en un Región de AWS lugar en el que el Centro de Identidad de IAM esté disponible. Para obtener información acerca de las regiones, consulte [Operaciones y almacenamiento de datos regionales de IAM Identity Center](#).

## Consideraciones sobre las instancias de cuenta

Una instancia de cuenta está diseñada para casos de uso especializados y ofrece un subconjunto de características disponibles para una instancia de organización. Tenga en cuenta lo siguiente antes de crear una instancia de cuenta:

- Las instancias de cuenta no admiten conjuntos de permisos y, por lo tanto, no admiten el acceso a Cuentas de AWS.
- No puede convertir ni fusionar una instancia de cuenta en una instancia de organización.
- Solo determinadas [aplicaciones administradas por AWS](#) admiten las instancias de cuenta.
- Utilice instancias de cuenta para usuarios aislados que utilizarán las aplicaciones en una sola cuenta y durante la vida útil de las aplicaciones utilizadas.
- Las aplicaciones que están asociadas a una instancia de cuenta deben permanecer asociadas a la instancia de cuenta hasta que elimine la aplicación y sus recursos.
- La instancia de una cuenta debe permanecer en el Cuenta de AWS lugar donde se creó.

## Permiso para la creación de instancias de cuentas en las cuentas de miembros

Si habilitó IAM Identity Center antes del 15 de noviembre de 2023, tiene una [instancia de organización](#) de IAM Identity Center y la posibilidad de que las cuentas de miembro creen instancias de cuenta está deshabilitada de forma predeterminada. Puede elegir si las cuentas de miembros pueden crear instancias de cuenta mediante la habilitación de la característica de instancias de cuenta en la consola del IAM Identity Center.

Para habilitar la creación de instancias de cuentas por parte de las cuentas de miembros de su organización

### Important

La habilitación de las instancias de cuenta de IAM Identity Center para las cuentas de los miembros es una operación de una sola vez. Esto significa que esta operación no se puede revertir. Una vez habilitada, puede limitar la creación de instancias de cuenta mediante la creación de una política de control de servicio (SCP). Para ver las instrucciones, consulte [Control de la creación de instancias de cuenta con políticas de control de servicio](#).

1. Abra la [consola de IAM Identity Center](#)
2. Seleccione Configuración y, a continuación, seleccione la pestaña Administración.
3. En la sección Instancias de cuenta de IAM Identity Center, seleccione Habilitar instancias de cuenta de IAM Identity Center.
4. En el cuadro de diálogo Habilitar instancias de cuenta de IAM Identity Center, confirme que desea permitir que las cuentas de miembros de su organización creen instancias de cuenta; para ello, seleccione Habilitar.

## Uso de las políticas de control de servicios para controlar la creación de instancias de cuentas

La capacidad de las cuentas de los miembros para crear instancias de cuentas depende de cuándo haya activado IAM Identity Center:

- Antes de noviembre de 2023: debe [permitir la creación de instancias de cuentas en las cuentas de los miembros](#), lo cual es una acción que no se puede revertir.



- Después del 15 de noviembre de 2023: las cuentas de los miembros pueden crear instancias de cuentas de forma predeterminada.

En cualquier caso, puedes usar las políticas de control de servicios (SCPs) para:

- Impedir que todas las cuentas de los miembros creen instancias de cuentas.
- Permitir que solo cuentas de miembros específicas creen instancias de cuentas.

### Cómo impedir las instancias de cuenta

Utilice el procedimiento siguiente para generar una SCP que impida a las cuentas de los miembros crear instancias de cuenta de IAM Identity Center.

1. Abra la [consola de IAM Identity Center](#)
2. En el panel de control, en la sección Administración central, seleccione el botón Impedir instancias de cuentas.
3. En el cuadro de diálogo Asociar una SCP para impedir la creación de nuevas instancias de cuenta, se le ofrecerá una SCP. Cópiela y pulse el botón Ir al panel de control de SCP. Se le indicará que vaya a la [AWS Organizations consola](#) para crear el SCP o adjuntarlo como una declaración a un SCP existente. SCPs son una característica de. AWS Organizations Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

### Límite a las instancias de cuenta

En lugar de impedir la creación de todas las instancias de cuentas, esta política deniega cualquier intento de crear una instancia de cuenta de IAM Identity Center a todas, Cuentas de AWS excepto a las que se indican explícitamente en el "**<ALLOWED-ACCOUNT-ID>**" marcador de posición.

Example: política de denegación que limita la creación de instancias de cuentas

JSON

```
{  
  
  "Version": "2012-10-17",  
  "Statement" : [  

```

```

    {
      "Sid": "DenyMemberAccountInstances",
      "Effect": "Deny",
      "Action": "sso:CreateInstance",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
        }
      }
    }
  ]
}

```

- Sustituya ["<ALLOWED-ACCOUNT-ID>"] por los Cuentas de AWS ID reales que desee permitir para crear una instancia de cuenta del IAM Identity Center.
- Puede enumerar varias cuentas permitidas IDs en el formato de matriz: ["111122223333", "444455556666"].
- Adjunte esta política a la SCP de su organización para aplicar un control centralizado sobre la creación de instancias de cuentas de IAM Identity Center.

Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

## Eliminación de la instancia de IAM Identity Center

Cuando se elimina una instancia de IAM Identity Center, se eliminan todos los datos de esa instancia y no se pueden recuperar. En la siguiente tabla se describen los datos que se eliminan en función del tipo de directorio que está configurado en IAM Identity Center.

| ¿Qué datos se eliminan?                                                               | Directorio conectado : AWS Managed Microsoft AD<br>AD Connector o proveedor de identidad externo | Almacén de identidades de IAM Identity Center                                        |    |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----|
| Todos los conjuntos de permisos para los que ha configurado Cuentas de AWS            |                 | S   | Sí |
| Todas las aplicaciones que ha configurado en IAM Identity Center                      |                 | S   | Sí |
| Todas las asignaciones de usuarios Cuentas de AWS y aplicaciones que haya configurado |                | S  | Sí |
| Todos los usuarios y grupos del directorio o almacén                                  | N/D                                                                                              |   | Sí |

Si ha replicado su instancia del IAM Identity Center en regiones adicionales, debe eliminar esas regiones antes de eliminar la instancia.

Utilice el siguiente procedimiento para eliminar su instancia de IAM Identity Center.

#### Cómo eliminar su instancia de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página Configuración, seleccione la pestaña Administración.

4. En la sección Eliminar la configuración de IAM Identity Center, seleccione Eliminar.
5. En el cuadro de diálogo Eliminar la configuración de IAM Identity Center, marque todas las casillas de verificación para confirmar que entiende que los datos se van a eliminar. Escriba su instancia de IAM Identity Center en el cuadro de texto y, a continuación, seleccione Confirmar.

# Activar IAM Identity Center

Cuando habilita el Centro de identidades de IAM, elige un tipo de AWS IAM Identity Center instancia para habilitarla. Una instancia de un servicio es una implementación única de un servicio en su AWS entorno. Hay dos tipos de instancias disponibles para IAM Identity Center: las instancias de organización y las instancias de cuenta. Los tipos de instancias que puede habilitar dependen del tipo de cuenta en la que haya iniciado sesión.

La siguiente lista identifica el tipo de instancias de IAM Identity Center que puede habilitar para cada tipo de Cuenta de AWS:

- Su cuenta AWS Organizations de administración (recomendada): necesaria para crear una [instancia organizativa](#) del IAM Identity Center. Utilice una instancia de organización para los permisos de varias cuentas y las asignaciones de aplicaciones en toda la organización. Puede replicar este tipo de instancia en otras regiones para mejorar la resiliencia del acceso a las cuentas y la flexibilidad a la hora de elegir las regiones de despliegue de AWS aplicaciones.
- Su cuenta de AWS Organizations miembro: utilícela para crear una [instancia de cuenta](#) del IAM Identity Center para permitir la asignación de solicitudes dentro de esa cuenta de miembro. En una organización pueden existir una o más cuentas con una instancia de nivel de miembro.
- Una instancia independiente Cuenta de AWS: se utiliza para crear una instancia de [organización o una instancia de cuenta](#) del IAM Identity Center. La versión independiente Cuenta de AWS no está gestionada por. AWS Organizations Solo puede asociar una instancia del IAM Identity Center a una instancia independiente Cuenta de AWS y utilizarla para las asignaciones de aplicaciones dentro de esa instancia independiente. Cuenta de AWS

## Important

La cuenta de administración de la organización puede controlar si [las cuentas de los miembros de la organización pueden crear instancias de cuentas de IAM Identity Center](#) mediante una política de control de servicios.

Si utiliza una cuenta de nivel gratuito, al crear una AWS organización, su cuenta se convierte automáticamente en un plan de pago con precios. pay-as-you-go Los créditos de la capa gratuita caducan inmediatamente. Para obtener más información, consulte [Capa gratuita de AWS FAQs](#).

Para comparar las distintas capacidades que proporcionan los distintos tipos de instancias, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Antes de activar IAM Identity Center, le recomendamos que revise [Requisitos previos y consideraciones sobre el IAM Identity Center](#).

## Para habilitar una instancia de cuenta de IAM Identity Center

Elija la pestaña correspondiente al tipo de instancia de IAM Identity Center que desee habilitar, ya sea una instancia de organización o de cuenta:

### Organization (recommended)

1. Realice una de estas operaciones para iniciar sesión en la Consola de administración de AWS.
  - Nuevo para AWS (usuario root): inicia sesión como propietario de la cuenta; para ello, selecciona Usuario root e introduce tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo AWS utilizas de forma independiente Cuenta de AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
  - Ya lo estás usando AWS Organizations (credenciales de IAM): inicia sesión con las credenciales de tu cuenta de administración.
2. Abra la [consola de IAM Identity Center](#).
3. (Opcional) Si desea utilizar una clave KMS gestionada por el cliente para el cifrado en reposo en lugar de la clave AWS gestionada predeterminada, configure la clave gestionada por el cliente en la sección Clave para cifrar los datos inactivos del IAM Identity Center. Para obtener más información, consulta [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).

#### Important

Realice este paso solo si ha configurado los permisos necesarios para usar la clave de KMS administrada por el cliente. Sin los permisos adecuados, este paso puede producir errores o interrumpir la administración y AWS las aplicaciones gestionadas del IAM Identity Center.

4. En Activar el IAM Identity Center, seleccione Activar.

5. En la página **Habilitar IAM Identity Center con AWS Organizations**, revise la información y, a continuación, seleccione **Habilitar** para completar el proceso.

 **Note**

AWS Organizations solo puede habilitar el Centro de identidad de IAM en una sola AWS región. Tras activar IAM Identity Center, si necesita cambiar la región en la que está habilitado IAM Identity Center, debe [eliminar](#) la instancia actual y crear una instancia en la otra región.

Después de habilitar la instancia de organización, se recomienda hacer lo siguiente para terminar de configurar el entorno:

- Confirme que utiliza el origen de identidad que eligió. Si ya tiene un origen de identidad, puede seguir utilizándolo. Para obtener más información, consulte [Confirme sus orígenes de identidad del IAM Identity Center](#).
- Registre una cuenta de miembro como administrador delegado. Para obtener más información, consulte [Administración delegada](#).
- El IAM Identity Center le proporciona un portal de acceso a los AWS recursos. Si filtra el acceso a AWS dominios o puntos de enlace URL específicos mediante una solución de filtrado de contenido web, como firewalls de última generación (NGFW) o Secure Web Gateways (SWG), consulte [Actualice los firewalls y las puertas de enlace para permitir el acceso a Portal de acceso a AWS](#)

## Account

1. Realice una de estas operaciones para iniciar sesión en la Consola de administración de AWS.
  - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione **Root user** e introduzca su dirección de correo electrónico. Cuenta de AWS En la siguiente página, escriba su contraseña.
  - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
  - Si ya las utiliza AWS Organizations (credenciales de IAM): inicie sesión con las credenciales administrativas de su cuenta de miembro.

2. Abra la [consola de IAM Identity Center](#).
3. Si es la primera vez que utiliza una cuenta independiente AWS o la tiene Cuenta de AWS, en Activar el centro de identidad de IAM, seleccione Activar.

Aparecerá la página Habilitar IAM Identity Center con AWS Organizations. Esto no es obligatorio pero sí recomendable.

Seleccione el enlace Habilitar una instancia de cuenta de IAM Identity Center.

4. Si es administrador de una cuenta de AWS Organizations miembro, en Habilitar una instancia de cuenta del IAM Identity Center, seleccione Habilitar una instancia de cuenta.
5. En la página Habilitar una instancia de cuenta de IAM Identity Center, revise la información y, si lo desea, añada las etiquetas que desee asociar a esta instancia de cuenta. A continuación, seleccione Habilitar para completar el proceso.

 Note

Si su AWS cuenta es miembro de una organización, es posible que haya restricciones a la hora de habilitar una instancia de cuenta del Centro de identidades de IAM.

- Si su organización habilitó IAM Identity Center antes del 15 de noviembre de 2023, la posibilidad de que las cuentas de miembro creen instancias de cuentas está deshabilitada de forma predeterminada y debe habilitarla la cuenta de administración de la organización.
- Si su organización habilitó IAM Identity Center después del 15 de noviembre de 2023, la posibilidad de que las cuentas de miembro creen instancias de cuentas está habilitada de forma predeterminada. Sin embargo, las políticas de control de servicio se pueden utilizar para impedir la creación de instancias de cuenta de IAM Identity Center dentro de una organización.

Para obtener más información, consulte [the section called “Permiso para la creación de instancias de cuentas en las cuentas de miembros”](#) y [the section called “SCPs para la creación de una instancia de cuenta”](#).



# Confirme sus orígenes de identidad del IAM Identity Center

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Después de habilitar IAM Identity Center, asegúrese de que utiliza el origen de identidad que eligió. Si ya tiene un origen de identidad, puede seguir utilizándolo.

Si ya administra usuarios y grupos en Active Directory o en un IdP externo, le recomendamos que considere la posibilidad de conectar este origen de identidad al habilitar IAM Identity Center y elegir su origen de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.

Si ya administra usuarios y grupos en una fuente de identidad en IAM Identity Center, cambiar a un origen de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del Centro de identidades de IAM, perderán el acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones. Para obtener más información, consulte [Consideraciones para cambiar la fuente de identidad](#).

Para confirmar su fuente de identidad

1. Abra la [consola de IAM Identity Center](#)
2. En la página del panel, debajo de la sección Pasos de configuración recomendados, seleccione Confirme su origen de identidad. Para acceder a esta página, también puede seleccionar Configuración y la pestaña Origen de identidad.
3. No tiene que realizar ninguna acción si desea conservar el origen de identidad asignado. Si prefiere cambiarlo, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.

Puede elegir una de las siguientes opciones como origen de identidad:

## Directorio de Identity Center

Cuando se activa IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como fuente de identidad predeterminada. Si aún no utilizas otro proveedor de identidad externo, puedes empezar a crear tus usuarios y grupos y asignar su nivel de acceso a tus aplicaciones Cuentas de AWS y a las tuyas. Para ver un tutorial sobre el uso de este origen de identidad, consulte [Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center](#).

## Active Directory

Si ya está gestionando los usuarios y grupos de su AWS Managed Microsoft AD directorio mediante Directory Service o de su directorio autogestionado Active Directory (AD), le recomendamos que conecte ese directorio al activar el Centro de identidades de IAM. No cree ningún usuario ni grupo en el directorio predeterminado de Identity Center. IAM Identity Center utiliza la conexión proporcionada por AWS Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades de IAM Identity Center. Para obtener más información, consulte [Directorio Microsoft AD](#).

### Note

El Centro de Identidad de IAM no SAMBA4 admite Simple AD como fuente de identidad.

## Proveedor de identidades externo

Para los proveedores de identidad externos (IdPs), como Okta o Microsoft Entra ID, puede utilizar el Centro de identidades de IAM para autenticar las identidades IdPs mediante el estándar del lenguaje de marcado de aserciones de seguridad (SAML) 2.0. El protocolo SAML no proporciona ninguna forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center. Puede realizar el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) v2.0 si su IdP admite SCIM. De lo contrario, puede aprovisionar manualmente los usuarios y grupos; para ello, ingrese manualmente los nombres de usuario, la dirección de correo electrónico y los grupos en IAM Identity Center.

Para obtener instrucciones detalladas sobre cómo configurar su fuente de identidad, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#).

### Note

Si tiene previsto utilizar un proveedor de identidades externo, tenga en cuenta que el IdP externo, no IAM Identity Center, administra la configuración de la autenticación multifactor (MFA). Los proveedores de identidad externos no admiten la MFA en el IAM Identity Center. Para obtener más información, consulte [Solicitar MFA a los usuarios](#).

 Note

Si planea replicar el Centro de identidades de IAM en otras regiones, tendrá que configurar un proveedor de identidad externo. Para obtener más información, incluidos los requisitos previos, consulte. [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#)

## Actualice los firewalls y las puertas de enlace para permitir el acceso a Portal de acceso a AWS

El portal de AWS acceso proporciona a los usuarios un acceso de inicio de sesión único a todas sus aplicaciones en la nube Cuentas de AWS y a las más utilizadas, como Office 365, Concur, Salesforce y muchas más. Para lanzar varias aplicaciones rápidamente, basta con elegir el icono Cuenta de AWS o la aplicación en el portal.

 Note

AWS las aplicaciones gestionadas se integran con el Centro de Identidad de IAM y lo utilizan para los servicios de autenticación y directorio, pero es posible que no utilicen el portal de AWS acceso para acceder a las aplicaciones.

Si filtra el acceso a AWS dominios o puntos de enlace de URL específicos mediante una solución de filtrado de contenido web, como firewalls de última generación (NGFW) o Secure Web Gateways (SWG), debe permitir incluir en la lista los dominios y puntos de enlace de URL asociados al portal de acceso. AWS

La siguiente lista proporciona los dominios IPv4 y puntos de enlace URL de doble pila que debe añadir a las listas de permitidos de su solución de filtrado de contenido web.

IPv4 lista de permitidos

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.com*
- \*.aws.dev
- \*.awsstatic.com
- \*.console.aws.a2z.com

- `oidc.[Region].amazonaws.com`
- `*.sso.amazonaws.com`
- `*.sso.[Region].amazonaws.com`
- `*.sso-portal.[Region].amazonaws.com`
- `[Region].prod.pr.panorama.console.api.aws/panoramamaroute`
- `[Region].signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`

#### Lista de permitidos de doble pila

- `[Identity Center instance ID].portal.[Region].app.aws`
- `*.aws.dev`
- `*.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.[Region].api.aws`
- `sso.[Region].api.aws`
- `portal.sso.[Region].api.aws`
- `[Region].sso.signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

#### Lista combinada de permitidos (IPv4 + pila doble con compatibilidad con versiones anteriores)

- `[Directory ID or alias].awsapps.com`

- `[Identity Center instance ID].[Region].portal.amazonaws.com`
- `[Identity Centers instance ID].portal.[Region].app.aws`
- `*.aws.dev`
- `*.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.[Region].amazonaws.com`
- `oidc.[Region].api.aws`
- `*.sso.amazonaws.com`
- `*.sso.[Region].amazonaws.com`
- `sso.[Region].api.aws`
- `*.sso-portal.[Region].amazonaws.com`
- `portal.sso.[Region].api.aws`
- `[Region].prod.pr.panorama.console.api.aws/panoramamaroute`
- `[Region].signin.aws`
- `[Region].sso.signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

## Consideraciones a la hora de permitir la inclusión de dominios y puntos de conexión de URL

Además de los requisitos de la lista de permitidos para el portal de AWS acceso, es posible que los demás servicios y aplicaciones que utilice exijan la inclusión de dominios en la lista de dominios permitidos.

- Para acceder a Cuentas de AWS la consola del Consola de administración de AWS IAM Identity Center y a ella desde su portal de AWS acceso, debe permitir incluir dominios adicionales en la

lista. Consulte [Solución de problemas](#) en la Guía de introducción para Consola de administración de AWS obtener una lista de Consola de administración de AWS dominios.

- Para acceder a las aplicaciones AWS gestionadas desde su portal de AWS acceso, debe permitir incluir sus dominios respectivos en una lista. Consulte la documentación de servicio correspondiente para obtener orientación.
- Si utilizas software externo, como el externo IdPs (por ejemplo, Okta y Microsoft Entra ID), tendrás que incluir sus dominios en tus listas de permisos.

# Tutoriales de orígenes de identidad de IAM Identity Center

Puede conectar su fuente de identidad existente en su cuenta AWS Organizations de administración a [una instancia de organización de IAM Identity Center](#). Si no tiene un proveedor de identidades existente, puede crear y gestionar los usuarios directamente en el directorio predeterminado de IAM Identity Center. Puede tener un origen de identidad por organización.

En los tutoriales de esta sección se describe cómo configurar una instancia de organización del Centro de Identidad de IAM con una fuente de identidad utilizada habitualmente, cómo crear un usuario administrativo y, si se utiliza el Centro de Identidad de IAM para gestionar el acceso Cuentas de AWS, cómo crear y configurar los conjuntos de permisos. Si utiliza el IAM Identity Center únicamente para acceder a las aplicaciones, no necesita utilizar conjuntos de permisos.

Estos tutoriales no describen cómo configurar instancias de cuenta del IAM Identity Center. Puede usar instancias de cuentas para asignar usuarios y grupos a las aplicaciones, pero no puede usar este tipo de instancia para administrar el acceso de los usuarios a Cuentas de AWS. Para obtener más información, consulte [Instancias de cuenta de IAM Identity Center](#).

## Note

Antes de iniciar cualquiera de estos tutoriales, habilite el IAM Identity Center. Para obtener más información, consulte [Activar IAM Identity Center](#).

## Temas

- [Uso de Active Directory como origen de identidad](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [Configuración de SAML y SCIM con Google Workspace e IAM Identity Center](#)
- [Uso de IAM Identity Center para conectarse a su plataforma de directorios de JumpCloud](#)
- [Configuración de SAML y SCIM con Microsoft Entra ID e IAM Identity Center](#)
- [Configuración de SAML y SCIM con Okta e IAM Identity Center](#)
- [Configuración del aprovisionamiento de SCIM entre OneLogin e IAM Identity Center](#)
- [Uso de productos de Ping Identity con IAM Identity Center](#)
- [Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center](#)
- [Tutoriales de vídeo](#)

# Uso de Active Directory como origen de identidad

Si administra los usuarios de su AWS Managed Microsoft AD directorio mediante Active Directory (AD) Directory Service o de su directorio autogestionado, puede cambiar la fuente de identidad del IAM Identity Center para que funcione con esos usuarios. Le recomendamos que considere la posibilidad de conectar este origen de identidad al habilitar IAM Identity Center y elegir el origen de identidad. Hacerlo antes de crear usuarios y grupos en el directorio predeterminado de Identity Center lo ayudará a evitar la configuración adicional que se requiere si cambia la fuente de identidad más adelante.

Para utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si lo está utilizando AWS Managed Microsoft AD, debe habilitar el Centro de identidades de IAM en el mismo Región de AWS lugar donde está configurado su AWS Managed Microsoft AD directorio. Centro de identidades de IAM almacena los datos de asignación en la misma región que el directorio. Para administrar Centro de identidades de IAM, es posible que deba cambiarse a la región en la que está configurado Centro de identidades de IAM. Además, tenga en cuenta que el portal de AWS acceso utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

Debe tener un AD Connector o AWS Managed Microsoft AD directorio existente configurado y debe residir en AWS Directory Service su cuenta AWS Organizations de administración. Solo puede conectar un directorio de conector de AD o un directorio en AWS Managed Microsoft AD a la vez. Si necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte lo siguiente:

- [Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- Utilice una instancia de Active Directory que resida en la cuenta de administrador delegado:

Si planea habilitar un administrador delegado del Centro de Identidad de IAM y usar Active Directory como fuente de identidad del Centro de Identidad de IAM, puede usar un AD Connector existente o un AWS Managed Microsoft AD directorio configurado en el AWS Directorio que resida en la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir en



(ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center, si existe alguna; de lo contrario, debe estar en la cuenta de administración.

En este tutorial se explica la configuración básica para usar Active Directory como origen de identidad de IAM Identity Center.

## Paso 1: conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio a IAM Identity Center.

### Note

Si planea conectar un AWS Managed Microsoft AD directorio o un directorio autogestionado en Active Directory y no va a utilizar RADIUS MFA AWS Directory Service con, active la MFA en IAM Identity Center.

### AWS Managed Microsoft AD

1. Revise la guía en [Directorio Microsoft AD](#).
2. Siga los pasos de [Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

### Directorio autogestionado en Active Directory

1. Revise la guía en [Directorio Microsoft AD](#).
2. Siga los pasos de [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Paso 2: sincronización de un usuario administrativo en IAM Identity Center

Tras conectar el directorio al Centro de identidades de IAM, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con el Centro de identidades de IAM.

1. Abra la [Consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, ingrese el nombre de usuario exacto y seleccione Agregar.
6. En Usuarios y grupos añadidos, haga lo siguiente:
  - a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
  - b. Seleccione la casilla de verificación situada a la izquierda del nombre de usuario.
  - c. Elija Enviar
7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar el usuario a ese conjunto de permisos. Para obtener más información, consulte [Crea un conjunto de permisos](#).

## Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios de CyberArk Directory Platform a IAM Identity Center. Este aprovisionamiento utiliza

el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

#### Note

CyberArk actualmente no admite el servicio de consumo de aserciones múltiples (ACS) de SAML URLs en la AWS IAM Identity Center aplicación. Esta función de SAML es necesaria para aprovechar al máximo el [soporte multirregional del IAM Identity Center](#). Si planea replicar el Centro de Identidad de IAM en otras regiones, tenga en cuenta que el uso de una sola URL de ACS puede afectar a la experiencia del usuario en esas regiones adicionales. Su región principal seguirá funcionando con normalidad. Le recomendamos que trabaje con su proveedor de IdP para habilitar esta función. Para obtener más información sobre la experiencia del usuario en otras regiones con una única URL de ACS, consulte [the section called “Uso de aplicaciones AWS gestionadas sin varios ACS URLs”](#) y [the section called “Cuenta de AWS resiliencia de acceso sin varios ACS URLs”](#).

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones de SCIM](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: configure el aprovisionamiento en CyberArk](#)
- [\(Opcional\) Paso 3: configure los atributos de usuario en CyberArk para el control de acceso \(ABAC\) en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Suscripción a CyberArk o prueba gratuita. Para suscribirse a una versión de prueba gratuita, vaya a [CyberArk](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde su cuenta de CyberArk a IAM Identity Center, tal y como se describe en la [documentación de IAM Identity Center CyberArk](#).
- Asocie el conector de IAM Identity Center a los roles, usuarios y organizaciones a los que desee permitir el acceso a las Cuentas de AWS.

## Consideraciones de SCIM

A continuación, se presentan las consideraciones a tener en cuenta al utilizar la federación de CyberArk para IAM Identity Center:

- Solo los roles asignados en la sección de aprovisionamiento de aplicaciones se sincronizarán con IAM Identity Center.
- El script de aprovisionamiento solo se admite en su estado predeterminado; una vez modificado, el aprovisionamiento de SCIM podría fallar.
  - Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Si se cambia la asignación de roles en la aplicación de IAM Identity Center CyberArk, se espera el siguiente comportamiento:
  - Si se cambian los nombres de los roles, no habrá cambios en los nombres de los grupos en IAM Identity Center.
  - Si se cambian los nombres de los grupos, se crearán nuevos grupos en IAM Identity Center y los grupos antiguos permanecerán sin miembros.
- El comportamiento de sincronización y desaprovisionamiento de los usuarios se puede configurar desde la aplicación de IAM Identity Center CyberArk. Asegúrese de configurar el comportamiento correcto para su organización. Estas son las opciones:
  - Sobrescriba (o no) a los usuarios del directorio de Identity Center con el mismo nombre principal.
  - Cancele el aprovisionamiento de usuarios de IAM Identity Center cuando se elimine al usuario del rol de CyberArk.
  - Cancele el aprovisionamiento de usuarios: deshabilite o elimine.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación IAM Identity Center de CyberArk. Estos pasos se explican en el procedimiento siguiente.

## Paso 2: configure el aprovisionamiento en CyberArk

Utilice el siguiente procedimiento en la aplicación IAM Identity Center CyberArk para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación IAM Identity Center CyberArk a la consola de administración de CyberArk en la sección Aplicaciones web. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

### Cómo configurar el aprovisionamiento en CyberArk

1. Abra la aplicación IAM Identity Center CyberArk que agregó como parte de la configuración de SAML CyberArk (Aplicaciones > Aplicación web). Consulte [Requisitos previos](#).
2. Elija la aplicación IAM Identity Center y vaya a la sección Aprovisionamiento.
3. Marque la casilla Habilitar el aprovisionamiento para esta aplicación y elija Live Mode.
4. En el procedimiento anterior, copió el valor del punto de conexión del SCIM de IAM Identity Center. Pegue ese valor en el campo URL del servicio SCIM, en la aplicación IAM Identity Center CyberArk, defina el tipo de autorización como encabezado de autorización.
5. Configure el tipo de encabezado como token al portador.
6. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token al portador de la aplicación IAM Identity Center CyberArk.
7. Haga clic en Verificar para probar y aplicar la configuración.
8. En Opciones de sincronización, elija el comportamiento correcto para el que desee que funcione el aprovisionamiento saliente de CyberArk. Puede optar por sobrescribir (o no) a los usuarios actuales de IAM Identity Center con un nombre principal y un comportamiento de desaprovisionamiento similares.
9. En Asignación de roles, adapte el mapeo de los roles desde CyberArk, en el campo Nombre al grupo de IAM Identity Center, en Grupo de destino.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de CyberArk aparecerán en la página Usuarios. Estos usuarios ya pueden asignarse a cuentas y conectarse dentro de IAM Identity Center.

## (Opcional) Paso 3: configure los atributos de usuario en CyberArk para el control de acceso (ABAC) en IAM Identity Center

Se trata de un procedimiento opcional si CyberArk decide configurar los atributos del Centro de Identidad de IAM para gestionar el acceso a sus recursos. AWS Los atributos que defina en CyberArk se transfieren en una aserción de SAML al IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde CyberArk.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Cómo configurar atributos de usuario utilizados en CyberArk para el control de acceso en IAM Identity Center

1. Abra la aplicación IAM Identity Center CyberArk que instaló como parte de la configuración de SAML para CyberArk (Aplicaciones > Aplicaciones web).
2. Vaya a la opción Respuesta SAML.
3. En Atributos, añada los atributos relevantes a la tabla siguiendo la siguiente lógica:
  - a. El Nombre del atributo es el nombre del atributo original de CyberArk.
  - b. El Valor del atributo es el nombre del atributo que se envía en la aserción SAML a IAM Identity Center.
4. Seleccione Save.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Configuración de SAML y SCIM con Google Workspace e IAM Identity Center

Si su organización Google Workspace lo utiliza, puede integrar a sus usuarios Google Workspace en el Centro de identidades de IAM para darles acceso a AWS los recursos. Puede lograr esta integración al cambiar la fuente de identidad del IAM Identity Center de la fuente de identidad predeterminada del IAM Identity Center a Google Workspace.

### Note

Google Workspace actualmente no admite el servicio de consumo de múltiples aserciones (ACS) de SAML URLs en la aplicación. AWS IAM Identity Center Esta función de SAML es necesaria para aprovechar al máximo el [soporte multirregional del IAM Identity Center](#). Si planea replicar el Centro de Identidad de IAM en otras regiones, tenga en cuenta que el uso de una sola URL de ACS puede afectar a la experiencia del usuario en esas regiones adicionales. Su región principal seguirá funcionando con normalidad. Le recomendamos que trabaje con su proveedor de IdP para habilitar esta función. Para obtener más información sobre la experiencia del usuario en otras regiones con una única URL de ACS, consulte [the section called “Uso de aplicaciones AWS gestionadas sin varios ACS URLs”](#) y [the section called “Cuenta de AWS resiliencia de acceso sin varios ACS URLs”](#).

La información de los usuarios de Google Workspace se sincroniza con IAM Identity Center mediante el [protocolo del sistema de administración de identidades entre dominios \(SCIM\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).



Esta conexión se configura en Google Workspace mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Google Workspace con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y Google Workspace. Para ello, debe configurar Google Workspace como proveedor de identidades de IAM y conectarse con su IAM Identity Center.

## Objetivo

Los pasos de este tutorial le ayudarán a establecer la conexión SAML entre Google Workspace y AWS. Más adelante, sincronizará a los usuarios de Google Workspace mediante SCIM. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Google Workspace usuario y verificará el acceso a los AWS recursos. Tenga en cuenta que este tutorial se basa en un entorno de prueba con un directorio de Google Workspace pequeño. No se incluyen en este tutorial las estructuras de directorios, como los grupos y las unidades organizativas. Tras completar este tutorial, sus usuarios podrán acceder al portal de AWS acceso con sus Google Workspace credenciales.

### Note

Para suscribirse a una versión de prueba gratuita de Google Workspace, vaya a [Google Workspace](#) en el sitio web de Google's.

Si aún no ha habilitado IAM Identity Center, consulte [Activar IAM Identity Center](#).

## Consideraciones

- Antes de configurar el aprovisionamiento de SCIM entre Google Workspace e IAM Identity Center, le recomendamos revisar primero [Consideraciones para utilizar el aprovisionamiento automático](#).
- La sincronización automática de SCIM desde Google Workspace actualmente está limitada al aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. Los grupos se pueden crear manualmente con el comando [create-group](#) de AWS CLI Identity Store o la API AWS Identity and Access Management (IAM). [CreateGroup](#) Como alternativa, puede utilizar [ssosync](#) para sincronizar los usuarios de Google Workspace y los grupos en el IAM Identity Center.
- Todos los usuarios de Google Workspace deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.

- Cada usuario de Google Workspace tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán. Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es “teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.
- Los atributos siguen sincronizados si el usuario está deshabilitado en IAM Identity Center, pero sigue activo en Google Workspace.
- Si existe un usuario en el directorio de Identity Center con el mismo nombre de usuario y correo electrónico, el usuario se sobrescribirá y sincronizará mediante SCIM desde Google Workspace.
- Hay algunas consideraciones adicionales a la hora de cambiar la fuente de identidad. Para obtener más información, consulte [the section called “Cómo cambiar de IAM Identity Center a un IdP externo”](#).

## Paso 1 Google Workspace: Configurar la aplicación SAML

1. Inicie sesión en la consola de administración de Google con una cuenta con privilegios de superadministrador.
2. En el panel de navegación izquierdo de la consola de administración de Google, elija Apps y seleccione Apps web y móviles.
3. En la lista desplegable Agregar aplicación, seleccione Buscar aplicaciones.
4. En el cuadro de búsqueda, ingrese Amazon Web Services y, a continuación, seleccione la aplicación Amazon Web Services (SAML) de la lista.
5. En la página Detalles del proveedor de identidad de Google: Amazon Web Services, puede realizar una de las siguientes acciones:
  - a. Descargar los metadatos del IdP.
  - b. Copie la URL del SSO, la URL del ID de la entidad y la información del certificado.

Necesitará el archivo XML o la información de la URL en el paso 2.

6. Antes de continuar con el siguiente paso en la consola de administración de Google, deje esta página abierta y vaya a la consola del IAM Identity Center.

## Paso 2: IAM Identity Center y Google Workspace: cambio del origen de identidad de IAM Identity Center y configuración de Google Workspace como proveedor de identidades de SAML

1. Inicie sesión en la [consola de IAM Identity Center](#) con un rol con permisos administrativos.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.
  - Si no ha habilitado el IAM Identity Center,, consulte [Activar IAM Identity Center](#) para obtener más información. Tras activar y acceder al IAM Identity Center por primera vez, accederá al panel, donde podrá seleccionar la fuente de identidad.
4. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
5. Se abre la página Configurar un proveedor de identidad externo. Para completar esta página y la página de Google Workspace del paso 1, deberá completar lo siguiente:
  - En la sección metadatos del proveedor de identidad de la consola de IAM Identity Center, deberá realizar una de las siguientes acciones:
    - i. Cargue los metadatos de SAML Google como metadatos de SAML del IdP en la consola del IAM Identity Center.
    - ii. Copie y pegue la URL del SSO de Google en el campo URL de inicio de sesión del IdP, la URL del emisor de Google en el campo URL del emisor del IdP y cargue el certificado de Google como certificado de IdP.
6. Tras introducir los metadatos de Google en la sección de metadatos del proveedor de identidades de la consola del IAM Identity Center, copie la URL del IAM Identity Assertion Consumer Service (ACS) y la URL del emisor del IAM Identity Center. En el siguiente paso, tendrás que proporcionarlos URLs en la consola de Google administración.
7. Deje la página de la consola de IAM Identity Center y vuelva a la consola de administración de Google. Debería estar en la página de Amazon Web Services: detalles del proveedor de servicios. Seleccione Continuar.
8. En la página Service provider details, ingrese los valores de ACS URL y Entity ID. Ha copiado estos valores en el paso anterior y se encuentran en la consola de IAM Identity Center.

- Pegue la URL del IAM Identity Center Assertion Consumer Service (ACS) en el campo URL de ACS.
  - Pegue la URL del emisor del IAM Identity Center en el campo ID de entidad.
9. En la página Detalles del proveedor del servicio, rellene los campos que aparecen debajo de ID de nombre de la siguiente manera:
- En Name ID format, seleccione EMAIL.
  - En Name ID, seleccione Basic Information > Primary email.
10. Elija Continuar.
11. En la página Attribute Mapping, en Attributes, seleccione ADD MAPPING y, a continuación, configure estos campos en GoogleGoogle Directory attribute:
- Para el atributo de la aplicación **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**, seleccione el campo Información básica, correo electrónico principal entre los atributos de Google Directory.
  - Para el atributo de la aplicación `https://aws.amazon.com/SAML/Attributes/Role`, seleccione cualquier atributo de Google Directory. Un atributo del directorio de Google podría ser Departamento.
12. Seleccione Finish.
13. Vuelva a la consola de IAM Identity Center y seleccione Siguiente. En la página Revisar y confirmar, revise la información y, a continuación, ingrese ACEPTAR en el espacio correspondiente. Elija Cambiar fuente de identidad.

Ya está listo para habilitar la aplicación de Amazon Web Services en Google Workspace para poder aprovisionar a los usuarios en IAM Identity Center.

### Paso 3: Google Workspace: habilitación de las aplicaciones

1. Vuelve a la Consola de Google administración y a tu AWS IAM Identity Center aplicación, que encontrarás en Aplicaciones y Aplicaciones web y móviles.
2. En el panel User access, junto a User access, seleccione la flecha hacia abajo para expandir User access para mostrar el panel Service status.
3. En el panel Service status, seleccione ON for everyone y, a continuación, seleccione SAVE.

 Note

Para ayudar a mantener el principio de privilegios mínimos, le recomendamos que, después de completar este tutorial, cambie Service status a OFF for everyone. Solo los usuarios que necesiten acceder a AWS deben tener el servicio habilitado. Puede usar grupos o unidades organizativas de Google Workspace para dar acceso a los usuarios a un subconjunto concreto de usuarios.

## Paso 4: IAM Identity Center: configuración del aprovisionamiento automático de IAM Identity Center

1. Vuelva a la consola de IAM Identity Center.
2. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
3. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. En el paso 5 de este tutorial, introducirá estos valores para configurar el aprovisionamiento automático en Google Workspace.
  - a. Punto final SCIM: por ejemplo,
    - IPv4https://  
scim.**Region**.amazonaws.com/**1111111111-2222-3333-4444-555555555555**/scim/v2
    - Pila doble https://  
scim.**Region**.api.aws/**1111111111-2222-3333-4444-555555555555**/scim/v2
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar.

#### 4. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, en el siguiente paso configurará el aprovisionamiento automático en Google Workspace.

## Paso 5: Google Workspace: configuración del aprovisionamiento automático

1. Vuelva a la consola de administración de Google y a su aplicación de AWS IAM Identity Center, que se encuentran en Apps y Apps web y móviles. En la sección Aprovisionamiento automático, elija Configurar aprovisionamiento automático.
2. En el procedimiento anterior, copió el valor del token de acceso en la consola de IAM Identity Center. Pegue ese valor en el campo Token de acceso y seleccione Continuar. Además, en el procedimiento anterior, copió el valor del punto de conexión de SCIM en la consola del IAM Identity Center. Pegue ese valor en el campo URL del punto de conexión y elija Continuar.
3. Compruebe que todos los atributos obligatorios de IAM Identity Center (los marcados con un asterisco) estén asignados a los atributos de Google Cloud Directory. Si no es así, haga clic en la flecha hacia abajo y asigne el atributo correspondiente. Elija Continuar.
4. En la sección Provisioning scope, puede seleccionar un grupo con su directorio de Google Workspace para proporcionar acceso a la aplicación de Amazon Web Services. Omita este paso y seleccione Continue.
5. En la sección Deprovisioning, puede elegir cómo responder a los diferentes eventos que impiden el acceso de un usuario. Para cada situación, puede especificar el tiempo que debe transcurrir antes de que comience el desaprovisionamiento:
  - en menos de 24 horas
  - después de un día
  - después de siete días
  - después de 30 días

Cada situación tiene una configuración de tiempo para cuándo suspender el acceso a una cuenta y cuándo eliminarla.

 Tip

Configure siempre más tiempo antes de eliminar la cuenta de un usuario que para suspenderla.

6. Seleccione Finalizar. Volverá a la página de la aplicación de Amazon Web Services.
7. En la sección Autoaprovisionamiento, active el conmutador para cambiarlo de Inactivo a Activo.

 Note

El control deslizante de activación está deshabilitado si IAM Identity Center no está activado para los usuarios. Seleccione Acceso de usuario y active la aplicación para activar el control deslizante.

8. En el cuadro de diálogo de confirmación, elija Activar.
9. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. En la página Users se muestran los usuarios de su directorio de Google Workspace que creó SCIM. Si los usuarios aún no aparecen en la lista, es posible que el aprovisionamiento aún esté en proceso. El aprovisionamiento puede tardar hasta 24 horas, aunque en la mayoría de los casos se completa en cuestión de minutos. Asegúrese de actualizar la ventana del navegador cada pocos minutos.

Seleccione un usuario y consulte sus detalles. La información debe coincidir con la información del directorio de Google Workspace.

 ¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Google Workspace AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

## Paso de atributos para el control de acceso: opcional

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Asigne acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las solicitudes.

### Note

Para completar este paso, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Paso 1: IAM Identity Center: conceder a los usuarios de Google Workspace acceso a las cuentas

1. Vuelva a la consola de IAM Identity Center. En el panel de navegación del IAM Identity Center, en **Permisos para varias cuentas**, seleccione **Cuentas de AWS**.



2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado **AdministratorAccess** con una duración de sesión establecida en una hora.
    - iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.
    - iv. En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.
    - v. En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de **AdministratorAccess** permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.
  - c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el *AdministratorAccess* rol.

 Note

La sincronización automática de SCIM de Google Workspace solo permite el aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. No puede crear grupos para los usuarios de Google Workspace mediante la Consola de administración de AWS. Tras aprovisionar a los usuarios, puede crear grupos mediante el comando [create-group](#) de AWS CLI Identity Store o la API de IAM. [CreateGroup](#)

## Paso 2 Google Workspace: Confirme Google Workspace el acceso de los usuarios a los recursos AWS

1. Inicie sesión en Google con una cuenta de usuario de prueba. Para obtener información sobre cómo agregar usuarios a Google Workspace, consulte la [documentación de Google Workspace](#).
2. Seleccione el icono del lanzador de Google apps (símbolo).
3. Desplácese a la parte inferior de la lista de aplicaciones donde se encuentran las aplicaciones personalizadas de Google Workspace. Aparece la aplicación de Amazon Web Services.
4. Seleccione la aplicación Amazon Web Services. Ha iniciado sesión en el portal de AWS acceso y puede ver el Cuenta de AWS icono. Amplíe ese icono para ver la lista a la Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.
5. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.
6. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Cuando creó el conjunto de permisos, especificó que se habilitó el acceso mediante programación y con la Consola de administración, por lo que esas dos opciones están

presentes. Seleccione Consola de administración para abrir la Consola de administración de AWS.

7. El usuario ha iniciado sesión en la consola.

## Siguientes pasos

Ahora que ha configurado Google Workspace como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Utilice el comando [create-group de AWS CLI](#) Identity Store o la API de IAM [CreateGroup](#) para crear grupos para sus usuarios.

Los grupos son útiles a la hora de asignar acceso a aplicaciones y aplicaciones. Cuentas de AWS En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.

- Para configurar los permisos en función de los cargos en el trabajo; consulte [Create a permission set](#).

Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario.

### Note

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados. Asegúrese de revisar cómo [administrar los certificados de SAML](#) para Google Workspace.

## Resolución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con Google Workspace, consulte las secciones siguientes:

- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para solucionar problemas en Google Workspace, consulte la [documentación de Google Workspace](#).

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con: AWS

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Uso de IAM Identity Center para conectarse a su plataforma de directorios de JumpCloud

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde la plataforma de directorios de JumpCloud a IAM Identity Center. Este aprovisionamiento utiliza el protocolo de [Lenguaje de marcado de seguridad \(SAML\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en JumpCloud mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en JumpCloud con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y JumpCloud.

Esta guía está basada en JumpCloud a fecha de junio de 2021. Los pasos para las versiones más recientes pueden variar. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos de JumpCloud a IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones de SCIM](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: configure el aprovisionamiento en JumpCloud](#)
- [\(Opcional\) Paso 3: configure los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Suscripción a JumpCloud o prueba gratuita. Para suscribirse a una versión de prueba gratuita, vaya a [JumpCloud](#).
- Una cuenta habilitada para el IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde su cuenta de JumpCloud a IAM Identity Center, tal y como se describe en la [documentación de IAM Identity Center JumpCloud](#).
- Si ha replicado el Centro de Identidad de IAM en otras regiones, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones AWS gestionadas y Cuentas de AWS desde esas regiones. Para obtener más información, consulte [the section called “Paso 3: Actualizar la configuración del IdP externo”](#). Consulte la JumpCloud documentación para obtener más información.
- Asocie el conector de IAM Identity Center a los grupos a los que desee permitir el acceso a las cuentas de AWS .

## Consideraciones de SCIM

A continuación, se presentan las consideraciones a tener en cuenta al utilizar la federación de JumpCloud para IAM Identity Center.

- Solo los grupos asociados al conector de inicio de sesión AWS único se JumpCloud sincronizarán con el SCIM.
- Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Los usuarios del directorio de JumpCloud deben tener su nombre y apellidos configurados para poder sincronizarse con IAM Identity Center mediante SCIM.
- Los atributos siguen sincronizados si el usuario está deshabilitado en IAM Identity Center, pero sigue activo en JumpCloud.
- Si desea activar la sincronización con SCIM únicamente para la información del usuario, desmarque la opción “Habilitar la administración de grupos de usuarios y la pertenencia a grupos” en el conector.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`

- b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación IAM Identity Center de JumpCloud. Estos pasos se explican en el procedimiento siguiente.

## Paso 2: configure el aprovisionamiento en JumpCloud

Utilice el siguiente procedimiento en el conector IAM Identity Center JumpCloud para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación JumpCloud de IAM Identity Center a la consola de JumpCloud administración del portal. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

### Cómo configurar el aprovisionamiento en JumpCloud

1. Abra el conector IAM Identity Center JumpCloud que instaló como parte de la configuración SAML para JumpCloud (Autenticación de usuario > IAM Identity Center). Consulte [Requisitos previos](#).
2. Seleccione el conector IAM Identity Center y, a continuación, elija la tercera pestaña Gestión de identidades.
3. Marque la casilla Habilitar la administración de grupos de usuarios y la pertenencia a grupos en esta aplicación si desea que los grupos se sincronicen con SCIM.
4. Haga clic en Configurar.
5. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base en el conector IAM Identity Center JumpCloud.

6. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Clave de token en el conector IAM Identity Center JumpCloud.
7. Haga clic en Activar para aplicar la configuración.
8. Asegúrese de tener activado un indicador verde junto a Inicio de sesión único activado.
9. Vaya a la cuarta pestaña Grupos de usuarios y marque los grupos que desee aprovisionar con SCIM.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de JumpCloud aparecerán en la página de Usuarios. Estos usuarios ya pueden asignarse a cuentas en IAM Identity Center.

## (Opcional) Paso 3: configure los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional si JumpCloud decide configurar los atributos del Centro de Identidad de IAM para gestionar el acceso a sus recursos. AWS Los atributos que defina en JumpCloud se transfieren en una aserción de SAML al IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde JumpCloud.

Antes de iniciar este procedimiento, habilite primero la característica [Atributos para el control de acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

### Cómo configurar atributos de usuario utilizados en JumpCloud para el control de acceso en IAM Identity Center

1. Abra el conector IAM Identity Center JumpCloud que instaló como parte de la configuración SAML para JumpCloud (Autenticación de usuario > IAM Identity Center).
2. Elija el conector de IAM Identity Center. A continuación, seleccione la segunda pestaña: IAM Identity Center.
3. En la parte inferior de esta pestaña está la asignación de atributos de usuario. Elija Añadir nuevo atributo y, a continuación siga estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.



- a. En el campo Nombre del atributo proporcionado por el servicio, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl: AttributeName`. Reemplace **AttributeName** con el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl: Email`.
  - b. En el campo Nombre del atributo de JumpCloud, elija los atributos de usuario de su directorio de JumpCloud. Por ejemplo, Correo electrónico (trabajo).
4. Seleccione Save.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo Name configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl: {TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Configuración de SAML y SCIM con Microsoft Entra ID e IAM Identity Center

AWS IAM Identity Center admite la integración con el [lenguaje de marcado de aserciones de seguridad \(SAML\) 2.0](#), así como el [aprovisionamiento automático](#) (sincronización) de la información

de usuarios y grupos desde Microsoft Entra ID (antes conocida como Azure Active Directory o Azure AD) al IAM Identity Center mediante el protocolo [System for Cross-domain Identity Management](#) (SCIM) 2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

## Objetivo

En este tutorial, configurará un laboratorio de pruebas y configurará una conexión SAML y el aprovisionamiento de SCIM entre Microsoft Entra ID e IAM Identity Center. Durante los pasos iniciales de preparación, creará un usuario de prueba (Nikki Wolf) tanto en Microsoft Entra ID como en IAM Identity Center que utilizará para probar la conexión SAML en ambas direcciones. Más adelante, como parte de los pasos de SCIM, creará un usuario de prueba diferente (Richard Roe) para comprobar que los nuevos atributos de Microsoft Entra ID se sincronizan con IAM Identity Center según lo previsto.

## Requisitos previos

Antes de empezar con este tutorial, primero tendrá que definir lo siguiente:

- Un inquilino de Microsoft Entra ID. Para obtener más información, consulte [Quickstart: Configurar un inquilino](#) en la documentación de Microsoft.
- Una cuenta habilitada para los usuarios. AWS IAM Identity Center Para más información, consulte [Activar IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

## Consideraciones

Las siguientes son consideraciones importantes sobre Microsoft Entra ID que pueden afectar a la forma en que planea implementar el [aprovisionamiento automático](#) con IAM Identity Center en su entorno de producción mediante el protocolo SCIM v2.

### Aprovisionamiento automático

Antes de comenzar a implementar SCIM, le recomendamos revisar primero las [Consideraciones para utilizar el aprovisionamiento automático](#).

### Atributos para controlar el acceso

Los atributos para el control de acceso se utilizan en las políticas de permisos que determinan quién de su fuente de identidad puede acceder a sus AWS recursos. Si se elimina un atributo de un usuario en Microsoft Entra ID, ese atributo no se elimina del usuario correspondiente en IAM Identity

Center. Se trata de una limitación de Microsoft Entra ID conocida. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincroniza con IAM Identity Center.

### Agrupación anidada

El servicio de aprovisionamiento de usuarios de Microsoft Entra ID no puede leer ni aprovisionar usuarios en grupos anidados. Solo se puede leer y aprovisionar los usuarios que sean miembros inmediatos de un grupo asignado explícitamente. Microsoft Entra ID no desglosa de forma recursiva las pertenencias a grupos de usuarios o grupos asignados indirectamente (usuarios o grupos que son miembros de un grupo asignado directamente). Para obtener más información, consulte [Ámbito basado en asignaciones](#) en la documentación de Microsoft. Como alternativa, puede utilizar la [sincronización de AD de IAM Identity Center](#) para integrar grupos de Active Directory con IAM Identity Center.

### Grupos dinámicos

El servicio de aprovisionamiento de usuarios de Microsoft Entra ID puede leer y aprovisionar usuarios en [grupos dinámicos](#). Consulte a continuación un ejemplo que muestra la estructura de usuarios y grupos al utilizar grupos dinámicos y cómo se muestran en IAM Identity Center. Estos usuarios y grupos se aprovisionaron de Microsoft Entra ID a IAM Identity Center mediante SCIM

Por ejemplo, si la estructura de los grupos dinámicos de Microsoft Entra ID es la siguiente:

1. Grupo A con los miembros ua1, ua2
2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con una regla para incluir a los miembros de los grupos A, B, C
5. Grupo K con una regla para incluir a los miembros de los grupos A, B, C

Una vez que la información del usuario y el grupo se aprovisiona de Microsoft Entra ID a IAM Identity Center a través de SCIM, la estructura será la siguiente:

1. Grupo A con los miembros ua1, ua2
2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con miembros ua1, ua2, ub1, uc1
5. Grupo L con miembros ub1, uc1

Cuando configure el aprovisionamiento automático mediante grupos dinámicos, tenga en cuenta las siguientes consideraciones.

- Un grupo dinámico puede incluir un grupo anidado. Sin embargo, el servicio de aprovisionamiento de Microsoft Entra ID no aplanar los grupos anidados. Por ejemplo, si tiene la siguiente estructura de Microsoft Entra ID para grupos dinámicos,
  - El grupo A es un elemento principal del grupo B.
  - El grupo A tiene a ua1 como miembro.
  - El grupo B tiene a ub1 como miembro.

El grupo dinámico que incluye al grupo A solo incluirá a los miembros directos del grupo A (es decir, ua1). No incluirá de forma recursiva a los miembros del grupo B.

- Los grupos dinámicos no pueden contener otros grupos dinámicos. Para obtener más información, consulte [Limitaciones de vista previa](#) en la documentación de Microsoft.

## Paso 1: preparación de su inquilino de Microsoft

En este paso, explicará cómo instalar y configurar su aplicación AWS IAM Identity Center empresarial y cómo asignar el acceso a un usuario de Microsoft Entra ID prueba recién creado.

### Step 1.1 >

#### Paso 1.1: Configurar la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID

En este procedimiento, se instala la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID. Necesitará esta aplicación más adelante para configurar su conexión SAML con AWS.

1. Inicie sesión en el [Centro de administración de Microsoft Entra](#) como mínimo como administrador de aplicaciones en la nube.
2. Vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione New application.
3. En la página Browse Microsoft Entra Gallery, ingrese **AWS IAM Identity Center** en el cuadro de búsqueda.
4. Seleccione AWS IAM Identity Center de los resultados.
5. Seleccione Crear.

## Step 1.2 >

### Paso 1.2: creación de un usuario de prueba en Microsoft Entra ID

Nikki Wolf es el nombre del usuario de prueba de Microsoft Entra ID que creará en este procedimiento.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **NikkiWolf** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, NikkiWolf@*example.org*.
4. En Display name, ingrese **NikkiWolf**.
5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, en Name, ingrese **Nikki**. En Last name, ingrese **Wolf**.
7. Elija Review + create y, a continuación, seleccione Create.

## Step 1.3

### Paso 1.3: Pon a prueba la experiencia de Nikki antes de asignar sus permisos a AWS IAM Identity Center

En este procedimiento, verificará que Nikki puede iniciar sesión correctamente en el [portal Mi cuenta](#) de Microsoft.

1. En el mismo navegador, abra una pestaña nueva, vaya a la página de inicio de sesión del [portal Mi cuenta](#) e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, NikkiWolf@*example.org*
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in. Si se trata de una contraseña generada automáticamente, se le solicitará que la cambie.
3. En la página Action Required, seleccione Ask later para omitir la solicitud de métodos de seguridad adicionales.
4. En la página Mi cuenta, en el menú de navegación izquierdo, seleccione Mis aplicaciones. Tenga en cuenta que, además de los complementos, no se muestra ninguna aplicación en

este momento. Agregaré una aplicación de AWS IAM Identity Center que aparecerá aquí en un paso posterior.

## Step 1.4

### Paso 1.4: asignación de permisos a Nikki en Microsoft Entra ID

Ahora que ha comprobado que Nikki puede acceder correctamente al portal Mi cuenta, utilice este procedimiento para asignar su usuario a la aplicación de AWS IAM Identity Center.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center en la lista.
2. A la izquierda, seleccione Users and groups.
3. Elija Agregar usuario o grupo. Puede ignorar el mensaje que indica que los grupos no están disponibles para su asignación. En este tutorial no se utilizan grupos para las asignaciones.
4. En la página Add Assignment, en Users, seleccione None Selected.
5. Seleccione y NikkiWolf, a continuación, elija Seleccionar.
6. En la página Añadir tarea, elija Asignar. NikkiWolf ahora aparece en la lista de usuarios que están asignados a la AWS IAM Identity Center aplicación.

## Paso 2: Prepara tu AWS cuenta

En este paso, seguirá las indicaciones para usar IAM Identity Center a fin de configurar los permisos de acceso (mediante un conjunto de permisos), crear manualmente el usuario correspondiente de Nikki Wolf y asignarle los permisos necesarios para administrar los recursos en AWS.

### Step 2.1 >

#### Paso 2.1: Crea un conjunto de RegionalAdmin permisos en IAM Identity Center

Este conjunto de permisos se utilizará para conceder a Nikki los permisos de AWS cuenta necesarios para gestionar las regiones desde la página de la cuenta del Consola de administración de AWS. De forma predeterminada, todos los demás permisos para ver o administrar cualquier otra información de la cuenta de Nikki están denegados.

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.

3. Elija Crear conjunto de permisos.
4. En la página Seleccionar el tipo de conjunto de permisos, seleccione Conjunto de permisos personalizado y seleccione Siguiente.
5. Seleccione Política insertada para ampliarla y, a continuación, siga estos pasos para crear una política para el conjunto de permisos:
  - a. Seleccione Agregar nueva instrucción para crear una instrucción de política.
  - b. En Editar instrucción, seleccione Cuenta de la lista y, a continuación, seleccione las siguientes casillas de verificación.
    - **ListRegions**
    - **GetRegionOptStatus**
    - **DisableRegion**
    - **EnableRegion**
  - c. Junto a Agregar un recurso, elija Agregar.
  - d. En la página Agregar recurso, en Tipo de recurso, seleccione Todos los recursos y, a continuación, seleccione Agregar recurso. Compruebe que la política sea similar a la siguiente:

```
{
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "account:ListRegions",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetRegionOptStatus"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Elija Siguiente.

7. En la página Especificar los detalles del conjunto de permisos, en Nombre de conjunto de permisos, escriba **RegionalAdmin** y, a continuación, seleccione Siguiente.
8. En la página Review and create (Revisar y crear), elija Create (Crear). Debería RegionalAdmin aparecer en la lista de conjuntos de permisos.

## Step 2.2 >

### Paso 2.2: Cree el NikkiWolf usuario correspondiente en IAM Identity Center

Como el protocolo SAML no proporciona un mecanismo para consultar el IdP (Microsoft Entra ID) y crear usuarios automáticamente aquí en IAM Identity Center, utilice el siguiente procedimiento para crear manualmente un usuario de IAM Identity Center que refleje los atributos principales del usuario Nikki Wolf en Microsoft Entra ID.

1. Abra la [consola de IAM Identity Center](#)
2. Seleccione Usuarios, Agregar usuario y, a continuación, proporcione la siguiente información:
  - a. Tanto para el nombre de usuario como para la dirección de correo electrónico: introduce la misma **NikkiWolf@yourcompanydomain.extension** que utilizaste al crear tu Microsoft Entra ID usuario. Por ejemplo, NikkiWolf@example.org.
  - b. Confirmar dirección de correo electrónico: vuelva a ingresar la dirección de correo electrónico del paso anterior
  - c. Nombre: ingrese **Nikki**.
  - d. Apellidos: ingrese **Wolf**.
  - e. Nombre de visualización: ingrese **Nikki Wolf**.
3. Seleccione Siguiente dos veces, y a continuación, seleccione Agregar usuario.
4. Seleccione Close (Cerrar).

## Step 2.3

### Paso 2.3: Asigne a Nikki el conjunto de RegionalAdmin permisos en IAM Identity Center

Aquí encontrará el lugar Cuenta de AWS en el que Nikki administrará las regiones y, a continuación, asignará los permisos necesarios para que pueda acceder correctamente al portal de AWS acceso.

1. Abra la [consola de IAM Identity Center](#)



2. En Permisos para varias cuentas, elija Cuentas de AWS.
3. Seleccione la casilla de verificación situada junto al nombre de la cuenta (por ejemplo *Sandbox*) a la que quiere conceder a Nikki el acceso para gestionar las regiones y, a continuación, seleccione Asignar usuarios y grupos.
4. En la página Asignar usuarios y grupos, seleccione la pestaña Usuarios, busque y marque la casilla situada junto a Nikki y, a continuación, seleccione Siguiente.

5.  
Example

<caption>On the Seleccionar conjuntos de permisos page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Next.</caption>

6. En la página Revisar y enviar, revise la selección y, a continuación, elija Enviar.

## Paso 3: configuración y prueba de la conexión SAML

En este paso, configura la conexión SAML mediante la aplicación AWS IAM Identity Center empresarial Microsoft Entra ID junto con la configuración del IdP externo en el Centro de identidad de IAM.

### Step 3.1 >

Paso 3.1: recopilación de los metadatos del proveedor de servicios necesarios de IAM Identity Center

En este paso, iniciará el asistente para cambiar la fuente de identidad desde la consola del IAM Identity Center y recuperará el archivo de metadatos y la URL de inicio de sesión AWS específica que deberá introducir al configurar la conexión en el siguiente paso. Microsoft Entra ID

1. En la [consola de IAM Identity Center](#), elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
3. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
4. En la página Configurar un proveedor de identidad externo, en Metadatos del proveedor de servicios, selecciona Predeterminado IPv4 o Dual-stack. Puede descargar el archivo de metadatos del proveedor de servicios después de completar el cambio de fuente de identidad.

5. En la misma sección, busque el valor de URL de inicio de sesión del portal de acceso de AWS y cópielo. Deberá ingresar este valor en el siguiente paso cuando se le pida.
6. Deje esta página abierta y continúe con el siguiente paso (**Step 3.2**) para configurar la aplicación AWS IAM Identity Center empresarialMicrosoft Entra ID. Más adelante, volverá a esta página para completar el proceso.

## Step 3.2 >

### Paso 3.2: Configure la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID

Este procedimiento establece la mitad de la conexión SAML en Microsoft mediante los valores del archivo de metadatos y la URL de inicio de sesión que obtuvo en el último paso.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. En el panel de la izquierda, elija 2. Configure el inicio de sesión único.
3. En la página Configurar el inicio de sesión único con SAML, seleccione SAML. Luego, seleccione Subir archivo de metadatos, seleccione el icono de la carpeta, seleccione el archivo de metadatos del proveedor de servicios que descargó en el paso anterior y, a continuación, seleccione Agregar.
4. En la página de configuración básica de SAML, compruebe que los valores del identificador y de la URL de respuesta (URL del servicio de atención al consumidor de afirmaciones) apuntan ahora a los puntos finales. AWS
  - Identificador: es la URL del emisor del IAM Identity Center. El mismo valor se aplica independientemente de si utiliza puntos finales de pila IPv4 única o de doble pila.
  - URL de respuesta (URL de Assertion Consumer Service): los valores aquí incluidos incluyen los puntos de enlace de doble pila y los IPv4 de doble pila de todas las regiones habilitadas de su centro de identidad de IAM. Puede usar la URL ACS de la región principal como predeterminada para que los usuarios sean redirigidos a la región principal cuando lancen la aplicación Amazon Web Services desde ellaMicrosoft Entra ID. Para obtener más información sobre ACS URLs, consulte [Los puntos finales ACS son el principal y el adicional Regiones de AWS](#).
  - (Opcional) Si ha replicado el Centro de Identidad de IAM en otras regiones, también puede crear una aplicación de marcadores Microsoft Entra ID para el portal de AWS acceso de

cada región adicional. Esto permite a sus usuarios acceder al portal de AWS acceso en otras regiones desde. Microsoft Entra ID Asegúrese de conceder a sus usuarios permisos para acceder a las aplicaciones de marcadores. Microsoft Entra ID Consulta [Microsoft Entra ID la documentación](#) para obtener más información. Si planea replicar el Centro de identidades de IAM en otras regiones más adelante, visite [Microsoft Entra ID configuración para acceder a regiones adicionales](#) para obtener información sobre cómo habilitar el acceso a las regiones adicionales después de esta configuración inicial.

5. En Sign on URL (Optional), pegue el valor de la URL de inicio de sesión del portal de acceso de AWS que copió en el paso anterior (**Step 3.1**), seleccione Save y, a continuación, seleccione X para cerrar la ventana.
6. Si se te pide que pruebes el inicio de sesión único con AWS IAM Identity Center, selecciona No, lo probaré más tarde. Realizará esta verificación en un paso posterior.
7. En la página Set up Single Sign-On with SAML, en la sección SAML Certificates, junto a Federation Metadata XML, seleccione Download para guardar el archivo de metadatos en el sistema. Deberá cargar este archivo en el siguiente paso cuando se le pida.

### Step 3.3 >

#### Paso 3.3: configuración del IdP externo de Microsoft Entra ID en AWS IAM Identity Center

Aquí volverá al asistente Cambiar el origen de identidad de la consola de IAM Identity Center para completar la segunda mitad de la conexión SAML en AWS.

1. Vuelva a la sesión del navegador que dejó abierta en **Step 3.1** en la consola de IAM Identity Center.
2. En la página Configurar un proveedor de identidad externo, en la sección Metadatos del proveedor de identidad, en Metadatos SAML del IdP, pulse el botón Elegir archivo, seleccione el archivo de metadatos del proveedor de identidades que descargó de Microsoft Entra ID en el paso anterior y, a continuación, seleccione Abrir.
3. Elija Siguiente.
4. Cuando haya leído el aviso legal y tenga todo listo para continuar, ingrese **ACCEPT**.
5. Seleccione Cambiar el origen de identidad para aplicar los cambios.

### Step 3.4 >

#### Paso 3.4: comprobación de que Nikki se redirige al portal de acceso de AWS

En este procedimiento, probará la conexión SAML; para ello, iniciará sesión en el portal Mi cuenta de Microsoft con las credenciales de Nikki. Una vez autenticado, seleccionará la AWS IAM Identity Center aplicación que redirigirá a Nikki al portal de acceso. AWS

1. Vaya a la página de inicio de sesión del [portal Mi cuenta](#) e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, **NikkiWolf** @ *example.org*
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in.
3. En la página Mi cuenta, en el menú de navegación izquierdo, seleccione Mis aplicaciones.
4. En la página My Apps, seleccione la aplicación denominada AWS IAM Identity Center. Esto debería solicitarle una autenticación adicional.
5. En la página de inicio de sesión de Microsoft, elige tus NikkiWolf credenciales. Si se te solicita la autenticación por segunda vez, vuelve a elegir tus NikkiWolf credenciales. Esto debería redirigirlo automáticamente al portal de AWS acceso.

 Tip

Si no se le redirige correctamente, compruebe que el valor de URL de inicio de sesión del portal de acceso de AWS que ha ingresado en **Step 3.2** coincide con el valor que ha copiado en **Step 3.1**.

6. Compruebe que su Cuentas de AWS pantalla.

 Tip

Si la página está vacía y no se Cuentas de AWS muestra, confirme que Nikki se ha asignado correctamente al conjunto de RegionalAdminpermisos (consulte **Step 2.3**).

## Step 3.5

Paso 3.5: comprobación del nivel de acceso de Nikki para administrar su Cuenta de AWS

En este paso, comprobará el nivel de acceso de Nikki para administrar la configuración regional de su Cuenta de AWS. Nikki solo debe tener los privilegios de administrador suficientes para administrar las regiones desde la página Cuentas.

1. En el portal de AWS acceso, seleccione la pestaña Cuentas para ver la lista de cuentas. Aparecen los nombres de las cuentas IDs, las cuentas y las direcciones de correo electrónico asociadas a las cuentas en las que haya definido conjuntos de permisos.
2. Elija el nombre de la cuenta (por ejemplo *Sandbox*) en la que aplicó el conjunto de permisos (consulte **Step 2.3**). Esto ampliará la lista de conjuntos de permisos entre los que Nikki puede elegir para administrar su cuenta.
3. Luego, RegionalAdmin elija la consola de administración para asumir la función que definió en el conjunto de RegionalAdmin permisos. Esto le redirige a la página de inicio de la Consola de administración de AWS .
4. En la esquina superior derecha de la consola, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta. El enlace le dirigirá a la página Cuenta. Observe que en todas las demás secciones de esta página aparece un mensaje en el que se indica que no tiene los permisos necesarios para ver ni modificar esos ajustes.
5. En la página Cuenta, desplácese hacia abajo hasta la sección Regiones de AWS . Seleccione la casilla de verificación de cualquier región disponible en la tabla. Tenga en cuenta que Nikki tiene los permisos necesarios para habilitar o deshabilitar la lista de regiones de su cuenta, tal y como estaba previsto.

#### ¡Bien hecho!

Los pasos del 1 al 3 lo ayudaron a implementar y probar correctamente la conexión SAML. Ahora, para completar el tutorial, le recomendamos que continúe con el paso 4 para implementar el aprovisionamiento automático.

## Paso 4: configuración y comprobación de la sincronización de SCIM

En este paso, configurará el [aprovisionamiento automático](#) (sincronización) de la información del usuario desde Microsoft Entra ID a IAM Identity Center mediante el protocolo SCIM v2.0. Esta conexión se configura en Microsoft Entra ID, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center.

Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Microsoft Entra ID con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y Microsoft Entra ID.

En los siguientes pasos se explica cómo habilitar el aprovisionamiento automático de usuarios que se encuentran principalmente en Microsoft Entra ID a IAM Identity Center mediante la aplicación de IAM Identity Center en Microsoft Entra ID.

## Step 4.1 >

### Paso 4.1: creación de un segundo usuario de prueba en Microsoft Entra ID

Con fines de prueba, creará un nuevo usuario (Richard Roe) en Microsoft Entra ID. Más adelante, después de configurar la sincronización con SCIM, comprobará que este usuario y todos los atributos pertinentes se han sincronizado correctamente con IAM Identity Center.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **RichRoe** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, RichRoe@*example.org*.
4. En Display name, ingrese **RichRoe**.
5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, a continuación, facilite los siguientes valores:
  - First name: ingrese **Richard**.
  - Last name: ingrese **Roe**.
  - Job title: ingrese **Marketing Lead**.
  - Department: ingrese **Sales**.
  - Employee ID: ingrese **12345**.
7. Elija Review + create y, a continuación, seleccione Create.

## Step 4.2 >

### Paso 4.2: habilitación del aprovisionamiento automático en IAM Identity Center

En este procedimiento, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático a IAM Identity Center de los usuarios y grupos que proceden de Microsoft Entra ID.

1. Abra la [consola de IAM Identity Center](#) y seleccione Configuración en el panel izquierdo de navegación.
2. En la página Configuración, en la pestaña Origen de identidad, observe que Método de aprovisionamiento está establecido en Manual.
3. Busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. Deberá pegar estos valores en el siguiente paso cuando configure el aprovisionamiento en Microsoft Entra ID.
  - a. Punto final SCIM: por ejemplo,
    - IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-5555555555/scim/v2`
    - Pila doble: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-5555555555/scim/v2`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar.

5. Seleccione Cerrar.
6. En la pestaña Origen de identidad, observe que Método de aprovisionamiento ahora está establecido en SCIM.

### Step 4.3 >

#### Paso 4.3: configuración del aprovisionamiento automático en Microsoft Entra ID

Ahora que ha establecido su usuario de RichRoe prueba y ha activado el SCIM en el Centro de Identidad de IAM, puede proceder a configurar los ajustes de sincronización del SCIM en Microsoft Entra ID

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Seleccione Provisioning y, en Manage, vuelva a seleccionar Provisioning.
3. En Provisioning Mode, seleccione Automatic.
4. En Admin Credentials, en Tenant URL, pegue el valor de la URL de Punto de conexión de SCIM que copió anteriormente en **Step 4.2**. En Secret Token, pegue el valor de Access token.
5. Elija Test Connection. Debería ver un mensaje que indica que las credenciales probadas se autorizaron correctamente para habilitar el aprovisionamiento.
6. Seleccione Save.
7. En Manage, seleccione Users and groups y, a continuación, seleccione Add user/group.
8. En la página Add Assignment, en Users, seleccione None Selected.
9. Seleccione y, a continuación RichRoe, elija Seleccionar.
10. En la página Agregar asignación, elija Asignar.
11. Seleccione Overview y, a continuación, seleccione Start provisioning.

## Step 4.4

Paso 4.4: comprobación de que se ha producido la sincronización

En esta sección, verificará que el usuario de Richard se aprovisionó correctamente y que todos los atributos se muestran en IAM Identity Center.

1. En la [consola de IAM Identity Center](#), seleccione Usuarios.
2. En la página de usuarios, debería aparecer su RichRoeusuario. Observe que, en la columna Creado por, el valor está establecido en SCIM.
3. Seleccione RichRoe, en Perfil, comprobar que se copiaron los siguientes atributos de Microsoft Entra ID.
  - Nombre: **Richard**.
  - Apellido: **Roe**.



- Departamento: **Sales**.
- Título: **Marketing Lead**.
- Número de empleado: **12345**.

Ahora que el usuario de Richard se ha creado en IAM Identity Center, puede asignarlo a cualquier conjunto de permisos para controlar el nivel de acceso que tiene a sus recursos de AWS. Por ejemplo, puede asignar RichRoeal conjunto de **RegionalAdmin** permisos que utilizó anteriormente para conceder a Nikki los permisos para administrar regiones (consulte **Step 2.3**) y, a continuación, probar su nivel de acceso utilizando **Step 3.5**.

 ¡Enhorabuena!

Has configurado correctamente una conexión SAML entre Microsoft AWS y has comprobado que el aprovisionamiento automático funciona para mantener todo sincronizado. Ahora puede aplicar lo aprendido para configurar su entorno de producción de forma más fluida.

## Paso 5: Configurar ABAC: opcional

Ahora que se ha configurado SAML y SCIM, puede optar por configurar el control de acceso basado en atributos (ABAC). El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos.

Con Microsoft Entra ID, puede utilizar uno de los dos métodos siguientes para configurar ABAC para su uso con IAM Identity Center.

Configure user attributes in ID de Microsoft Entra for access control in IAM Identity Center

Configuración de atributos de usuario en Microsoft Entra ID para el control de acceso en IAM Identity Center

En el siguiente procedimiento, determinará qué atributos Microsoft Entra ID debe utilizar el Centro de identidades de IAM para administrar el acceso a sus recursos. AWS Una vez definidos, Microsoft Entra ID envía estos atributos a IAM Identity Center mediante aserciones de SAML. A continuación, tendrá que [Crea un conjunto de permisos](#) en IAM Identity Center para gestionar el acceso en función de los atributos que transfirió desde Microsoft Entra ID.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Elija Single sign-on (Inicio de sesión único).
3. En la sección Attributes & Claims, elija Edit.
4. En la página Attributes & Claims, haga lo siguiente:
  - a. Elija Añadir nueva reclamación.
  - b. En Nombre, escriba `AccessControl:AttributeAttributeName`. Sustituya *AttributeName* por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `AccessControl:Department`.
  - c. En Espacio de nombres, escriba `https://aws.amazon.com/SAML/Attributes`.
  - d. En Source (Origen), elija Attribute (Atributo).
  - e. En Atributo de origen, utilice la lista desplegable para elegir los atributos del usuario de Microsoft Entra ID. Por ejemplo, `user.department`.
5. Repita el paso anterior para cada atributo que necesite enviar a IAM Identity Center en la aserción SAML.
6. Seleccione Save.

## Configure ABAC using IAM Identity Center

### Configuración de ABAC con IAM Identity Center

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un conjunto de Attribute con el atributo Name configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento AttributeValue que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `Department=billing`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Asigne el acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las solicitudes.

### Note

Para completar este paso, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Paso 1: IAM Identity Center: conceder a los usuarios de Microsoft Entra ID acceso a las cuentas

1. Vuelva a la consola de IAM Identity Center. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.

- b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
  - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
    - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
    - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.

Elija Siguiente.

- ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado *AdministratorAccess* con una duración de sesión establecida en una hora.

- iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.
  - iv. En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.
  - v. En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.
- c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el *AdministratorAccess* rol.

## Paso 2 Microsoft Entra ID: Confirme el acceso de Microsoft Entra ID los usuarios a AWS los recursos

1. Vuelva a la consola de Microsoft Entra ID y diríjase a la aplicación de inicio de sesión basada en SAML de IAM Identity Center.
2. Seleccione Usuarios y grupos y, a continuación, seleccione Añadir usuarios o grupos. Añadirá el usuario que creó en este tutorial en el paso 4 a la aplicación de Microsoft Entra ID. Al añadir el usuario, le permitirá iniciar sesión en AWS. Busque el usuario que creó en el paso 4. Si siguió este paso, sería **RichardRoe**.
  - Para ver una demostración, consulte [Federate your existing IAM Identity Center instance with Microsoft Entra ID](#)

## Microsoft Entra ID configuración para acceder a regiones adicionales del centro de identidad de IAM (opcional)

Si ha replicado el Centro de Identidad de IAM en otras regiones, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones AWS gestionadas y a Cuentas de AWS través de las regiones adicionales. Los pasos que se indican a continuación le guiarán a lo largo del procedimiento. Para obtener más información sobre este tema, incluidos los requisitos previos, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).

1. Recupere el ACS URLs de las regiones adicionales desde la consola del IAM Identity Center, tal y como se describe en. [Los puntos finales ACS son el principal y el adicional Regiones de AWS](#)
2. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
3. En el panel de la izquierda, elija 2. Configure el inicio de sesión único.
4. En la página de configuración básica de SAML, en la sección URL de respuesta (URL del servicio al consumidor de aserciones), seleccione Añadir URL de respuesta para cada URL ACS adicional de una región. Puedes mantener la URL ACS de la región principal como la predeterminada para que los usuarios sigan siendo redirigidos a la región principal cuando inicien la aplicación desde ella. AWS IAM Identity Center Microsoft Entra ID
5. Cuando termine de agregar el ACS URLs, guarde la AWS IAM Identity Center aplicación.
6. Puede crear una aplicación de marcadores Microsoft Entra ID para el portal de AWS acceso en cada región adicional. Esto permite a sus usuarios acceder al portal de AWS acceso en

otras regiones desde Microsoft Entra ID. Asegúrese de conceder a sus usuarios permisos para acceder a las aplicaciones de marcadores. Microsoft Entra ID Consulta [Microsoft Entra ID la documentación](#) para obtener más información.

7. Compruebe que puede iniciar sesión en el portal de AWS acceso de cada región adicional. Navegue hasta el [portal de AWS acceso URLs](#) o inicie las aplicaciones desde Microsoft Entra ID las que se marcan como favoritas.

## Resolución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con Microsoft Entra ID, consulte las secciones siguientes:

- [Problemas de sincronización con Microsoft Entra ID e IAM Identity Center](#)
- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- [Recursos adicionales](#)

### Problemas de sincronización con Microsoft Entra ID e IAM Identity Center

Si tiene problemas con usuarios de Microsoft Entra ID que no se sincronizan con IAM Identity Center, es posible que se deba a un problema de sintaxis que IAM Identity Center ha detectado al agregar un nuevo usuario a IAM Identity Center. Para confirmarlo, consulte los registros de auditoría de Microsoft Entra ID para ver si hay eventos con errores, como 'Export'. El motivo del estado de este evento indicará:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

También puedes comprobar AWS CloudTrail el evento fallido. Para ello, busque en la consola del historial de eventos o CloudTrail utilice el siguiente filtro:

```
"eventName": "CreateUser"
```

El error del CloudTrail evento indicará lo siguiente:

```
"errorCode": "ValidationException",  
  "errorMessage": "Currently list attributes only allow single item"
```

En última instancia, esta excepción significa que uno de los valores transferidos desde Microsoft Entra ID contenía más valores de los previstos. La solución consiste en revisar los atributos del usuario de Microsoft Entra ID, asegurándose de que ninguno contenga valores duplicados. Un ejemplo habitual de valores duplicados es la presencia de varios valores en los números de contacto, como el número de móvil, del trabajo y el fax. Aunque son valores independientes, todos se transfieren al IAM Identity Center con el atributo principal `phoneNumbers`.

Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas](#).

## Sincronización de cuentas de invitado de Microsoft Entra ID

Si desea sincronizar sus usuarios invitados de Microsoft Entra ID con el IAM Identity Center, consulte el siguiente procedimiento.

El correo electrónico de los usuarios invitados de Microsoft Entra ID es diferente al de los usuarios de Microsoft Entra ID. Esta diferencia provoca problemas a la hora de sincronizar usuarios invitados de Microsoft Entra ID con IAM Identity Center. Por ejemplo, consulte la siguiente dirección de correo electrónico para un usuario invitado:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com`.

El Centro de Identidad de IAM no espera que la dirección de correo electrónico contenga este `#EXT#@domain` formato.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Diríjase a la pestaña Inicio de sesión único en el panel izquierdo.
3. Seleccione Editar, que aparece junto a Atributos y notificaciones del usuario.
4. Seleccione un Identificador de usuario único (ID de nombre) después de las Notificaciones obligatorias.
5. Creará dos condiciones de notificación para sus usuarios de Microsoft Entra ID y para los usuarios invitados:

- a. Para los usuarios de Microsoft Entra ID, cree un tipo de usuario para los miembros con el atributo de origen establecido en `user.userprincipalname`.
- b. Para los usuarios invitados de Microsoft Entra ID, cree un tipo de usuario para los invitados externos con el atributo de origen establecido en `user.mail`.
- c. Seleccione Guardar y vuelva a intentar iniciar sesión como usuario invitado de Microsoft Entra ID.

## Recursos adicionales

- Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas de IAM Identity Center](#).
- Para solucionar problemas de Microsoft Entra ID, consulte la [documentación de Microsoft](#).
- Para obtener más información sobre la federación entre varias Cuentas de AWS, consulte [Proteger Cuentas de AWS con Azure Active Directory Federation](#).

Los siguientes recursos pueden ayudarle a solucionar problemas a medida que trabaja con AWS:

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Configuración de SAML y SCIM con Okta e IAM Identity Center

Puede aprovisionar o sincronizar la información de usuarios y grupos desde Okta a IAM Identity Center de forma automática mediante el protocolo del [sistema de administración de identidades entre dominios \(SCIM\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en Okta, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Okta con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y su cuenta de Okta.

Okta admite las siguientes características de aprovisionamiento cuando se conecta al IAM Identity Center a través de SCIM:



- Crear usuarios: los usuarios asignados a la aplicación IAM Identity Center Okta se aprovisionan en IAM Identity Center.
- Actualizar los atributos de usuario: los cambios en los atributos de los usuarios que están asignados a la aplicación IAM Identity Center Okta se actualizan en IAM Identity Center.
- Desactivar usuarios: los usuarios que no están asignados en la aplicación IAM Identity Center Okta están deshabilitados en IAM Identity Center.
- Transferencia de grupos: los grupos (y sus miembros) de Okta se sincronizan con IAM Identity Center.

#### Note

Para minimizar la sobrecarga administrativa tanto en Okta como en IAM Identity Center, le recomendamos que asigne y transfiera grupos en lugar de usuarios individuales.

- Importar usuarios: los usuarios se pueden importar desde el Centro de identidad de IAM aOkta.

## Objetivo

En este tutorial, seguirá las indicaciones para configurar una conexión SAML con IAM Identity Center en Okta. Más adelante, sincronizará los usuarios desde Okta mediante SCIM. En este escenario, administrará todos los usuarios y grupos en Okta. Los usuarios inician sesión a través del portal de Okta. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Okta usuario y verificará el acceso a AWS los recursos.

Al conectarse al Centro de Identidad de IAM Okta a través de SAML, se admiten las siguientes funciones:

- Inicio de sesión SAML iniciado por el IdP: los usuarios inician sesión a través del Okta portal y obtienen acceso al Centro de identidades de IAM.
- Inicio de sesión con SAML iniciado por SP: los usuarios acceden al portal de acceso, que los redirige para iniciar sesión AWS a través del portal. Okta

#### Note

Puede registrarse para obtener una cuenta de Okta ([prueba gratuita](#)) que tenga instalada la [aplicación IAM Identity Center](#) de Okta. En el caso de los productos de pago de Okta, es posible que deba confirmar que su licencia de Okta admite la administración del ciclo de vida

o capacidades similares que permitan el aprovisionamiento saliente. Estas características pueden ser necesarias para configurar SCIM desde Okta a IAM Identity Center. Si aún no ha habilitado IAM Identity Center, consulte [Activar IAM Identity Center](#).

## Consideraciones

- Antes de configurar el aprovisionamiento de SCIM entre Okta e IAM Identity Center, le recomendamos revisar primero [Consideraciones para utilizar el aprovisionamiento automático](#).
- Todos los usuarios de Okta deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.
- Cada usuario de Okta tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán. Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es “teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.
- Cuando se utiliza Okta con IAM Identity Center, este se configura generalmente como una aplicación en Okta. Esto le permite configurar varias instancias de IAM Identity Center como múltiples aplicaciones, lo que permite el acceso a varias organizaciones de AWS , dentro de una sola instancia de Okta.
- Los derechos y los atributos de rol no son compatibles y no se pueden sincronizar con IAM Identity Center.
- Actualmente, no es posible usar el mismo grupo de Okta para la transferencia de tareas y grupos. Para mantener una pertenencia uniforme a los grupos entre Okta e IAM Identity Center, cree un grupo independiente y configúrelo para enviar grupos a IAM Identity Center.
- Si ha replicado el Centro de identidades de IAM en otras regiones, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones gestionadas y a través de otras regiones. AWS Cuentas de AWS Para obtener más información, incluidos los requisitos previos, consulte. [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#) Los pasos específicos de Okta se describen en [Oktaconfiguración para acceder a regiones adicionales](#)

## Paso 1: Okta: obtención de los metadatos de SAML de su cuenta de Okta

1. Inicie sesión en el Okta admin dashboard, expanda Applications y, a continuación, seleccione Applications.
2. En la página Applications, elija Browse App Catalog (Examinar catálogo de aplicaciones).
3. En el cuadro de búsqueda AWS IAM Identity Center, escriba y seleccione la aplicación para añadir la aplicación IAM Identity Center.
4. Seleccione la pestaña Sign On.
5. En SAML Signing Certificates, seleccione Actions y, a continuación, View IdP Metadata. Se abre una nueva pestaña del navegador en la que se muestra el árbol de documentos de un archivo XML. Seleccione todo el XML de `<md:EntityDescriptor>` a `</md:EntityDescriptor>` y cópielo en un archivo de texto.
6. Guarde el archivo de texto como `metadata.xml`.

Deje el Okta admin dashboard abierto; seguirá usando esta consola en los pasos posteriores.

## Paso 2: IAM Identity Center: configuración de Okta como origen de identidad para IAM Identity Center

1. Abra la [consola de IAM Identity Center](#) como usuario con privilegios administrativos.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:
  - a. En Metadatos del proveedor de servicios, copie los siguientes elementos en un archivo de texto para acceder fácilmente a ellos:
    - URL del Servicio de Consumer Service (ACS) de IAM Identity Center: puede elegir entre ACS de pila IPv4 única o de doble pila. URLs Además, si su instancia del IAM Identity Center está habilitada en varias regiones, cada región adicional tiene su propio IPv4 ACS exclusivo y de doble pila. URLs Para obtener más información sobre ACS URLs, consulte. [Los puntos finales ACS son el principal y el adicional Regiones de AWS](#)

- URL del emisor de IAM Identity Center

Necesitará estos valores más adelante en este tutorial.

- b. En Metadatos del proveedor de identidad, en Metadatos SAML del IdP, seleccione Elegir archivo y, a continuación, seleccione el archivo metadata.xml que creó en el paso anterior.
  - c. Elija Siguiente.
6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.
  7. Elija Cambiar fuente de identidad.

Deje la AWS consola abierta y seguirá utilizándola en el siguiente paso.

8. Vuelva a la pestaña Iniciar sesión de la AWS IAM Identity Center aplicación Okta admin dashboard y, a continuación, seleccione Editar.
9. En Advanced Sign-on Settings, ingrese lo siguiente:
  - En el caso de la URL de ACS, introduzca los valores que ha copiado para la URL de IAM Identity Center Assertion Consumer Service (ACS). Puede usar la URL ACS de la región principal como predeterminada para que los usuarios sean redirigidos a la región principal cuando lancen la aplicación Amazon Web Services desde ellaOkta.
  - (Opcional) Si ha replicado el Centro de Identidad de IAM en otras regiones, también puede crear una aplicación de marcadores Okta para el portal de AWS acceso de cada región adicional. Esto permite a sus usuarios acceder al portal de AWS acceso en otras regiones desde. Okta Asegúrese de conceder a sus usuarios permisos para acceder a las aplicaciones de marcadores en Okta las que aparecen. Consulta [Okta documentación](#) para obtener más información. Si planea replicar el Centro de identidades de IAM en otras regiones más adelante, visite [Okta configuración para acceder a regiones adicionales](#) para obtener información sobre cómo habilitar el acceso a las regiones adicionales después de esta configuración inicial.
  - En Issuer URL, ingrese el valor que ha copiado de URL del emisor de IAM Identity Center.
  - En Application username format, seleccione una de las opciones del menú.

Asegúrese de que el valor que elija sea único para cada usuario. Para este tutorial, seleccione Okta username.

10. Seleccione Save.

Ya tiene todo listo para aprovisionar a usuarios desde Okta a IAM Identity Center. Deje el Okta admin dashboard abierto y vuelva a la consola de IAM Identity Center para continuar con el siguiente paso.

### Paso 3: IAM Identity Center and Okta: aprovisionar usuarios de Okta

1. En la consola de IAM Identity Center, en la página Configuración, busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión de SCIM y el token de acceso.
2. En el cuadro de diálogo Aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones:
  - a. Punto final SCIM: el formato del punto final depende de la configuración:
    - IPv4: `https://scim.us-east-2.amazonaws.com/ /scim/v2`  
`1111111111-2222-3333-4444-5555555555`
    - Pila doble: `https://scim.us-east-2.api.aws/ /scim/v2`  
`1111111111-2222-3333-4444-5555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

#### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en Okta más adelante en este tutorial.

3. Seleccione Cerrar.
4. Vuelva al Okta admin dashboard y acceda a la aplicación IAM Identity Center.
5. En la página de la aplicación IAM Identity Center, seleccione la pestaña Aprovisionamiento y, a continuación, en el menú de navegación de la izquierda, en Configuración, seleccione Integración.
6. Seleccione Edit y, a continuación, active la casilla de verificación situada junto a Enable API integration para habilitar el aprovisionamiento automático.
7. Configure Okta con los valores de aprovisionamiento de SCIM que copió anteriormente en este paso: AWS IAM Identity Center

- a. En el campo Base URL, ingrese el valor de Punto de conexión de SCIM.
  - b. En el campo API Token, ingrese el valor de Token de acceso.
8. Elija Verificar credenciales de API para comprobar que las credenciales introducidas son válidas.  
  
Aparecerá el mensaje AWS IAM Identity Center was verified successfully!.
9. Seleccione Save. Pasará a la sección de Configuración, con Integración seleccionada.
10. En Configuración, seleccione A la aplicación y, a continuación, active la casilla Habilitar para cada una de las características de Aprovisionar a la aplicación que desee habilitar. Para este tutorial, seleccione todas las opciones.
11. Seleccione Save.

Ya tiene todo listo para sincronizar los usuarios desde Okta con IAM Identity Center.

## Paso 4: Okta: sincronización de los usuarios desde Okta con IAM Identity Center

De forma predeterminada, no hay ningún usuario o grupo asignado a su aplicación IAM Identity Center de Okta. Los grupos de aprovisionamiento aprovisionan a los usuarios que sean miembros del grupo. Complete los siguientes pasos para sincronizar grupos y usuarios con AWS IAM Identity Center.

1. En la página de la aplicación IAM Identity Center de Okta, seleccione la pestaña Tareas. Puede asignar personas y grupos a la aplicación IAM Identity Center.
  - a. Para asignar personas:
    - En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to people.
    - Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento de los usuarios en IAM Identity Center.

- b. Para asignar grupos:

- En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to groups.
- Seleccione los grupos de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento del usuario o los usuarios en IAM Identity Center.

 Note

Es posible que deba especificar más atributos para el grupo si no están presentes en todos los registros de usuario. Los atributos especificados para el grupo anularán cualquier valor de atributo individual.

2. Seleccione la pestaña Transferir grupos. Elija el grupo de Okta que desee sincronizar con IAM Identity Center. Seleccione Save.

El estado del grupo cambia a Active después de que el grupo y sus miembros se hayan transferido a IAM Identity Center.

3. Vuelva a la pestaña Assignments.
4. Para agregar usuarios individuales de Okta a IAM Identity Center, realice los siguientes pasos:
  - a. En la página de tareas, seleccione Asignar y, a continuación, seleccione Asignar a personas.
  - b. Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento de los usuarios individuales en IAM Identity Center.

 Note

También puede asignar usuarios y grupos a la AWS IAM Identity Center aplicación, desde la página Aplicaciones del Okta admin dashboard. Para ello, seleccione el

icono Settings, seleccione Assign to Users o Assign to Groups y, a continuación, especifique el usuario o el grupo.

5. Vuelva a la consola de IAM Identity Center. En el menú de navegación de la izquierda, seleccione Users. Debería ver la lista de usuarios rellena por sus usuarios de Okta.

#### ¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Okta AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

## Paso de atributos para el control de acceso: opcional

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.



## Asigne el acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las solicitudes.

### Note

Para completar este paso, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Paso 1: IAM Identity Center: conceder a los usuarios de Okta acceso a las cuentas

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado *AdministratorAccess* con una duración de sesión establecida en una hora.

- iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

- c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el rol.

*AdministratorAccess*

## Paso 2Okta: Confirme el acceso de Okta los usuarios a los recursos AWS

1. Inicie sesión con una cuenta de prueba a Okta dashboard.
2. En Mis aplicaciones, seleccione el icono de AWS IAM Identity Center.
3. Deberías ver el Cuenta de AWS icono. Amplíe ese icono para ver la lista a la Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.
4. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.

5. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Al crear el conjunto de permisos, especificó el acceso tanto al acceso como al Consola de administración de AWS acceso programático. Seleccione Consola de administración para abrir la Consola de administración de AWS.
6. El usuario ha iniciado sesión en la Consola de administración de AWS.

También puede utilizar el portal de AWS acceso. Esto le redirige a iniciar sesión a través del Okta portal antes de ir al portal de AWS acceso. Esta ruta sigue el flujo de inicio de sesión SAML iniciado por el SP.

## Oktaconfiguración para acceder a regiones adicionales del Centro de Identidad de IAM (opcional)

Si ha replicado el Centro de Identidad de IAM en otras regiones, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones AWS gestionadas y a Cuentas de AWS través de las regiones adicionales. Los pasos que se indican a continuación le guiarán a lo largo del procedimiento. Para obtener más información sobre este tema, incluidos los requisitos previos, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).

1. Recupere el ACS URLs de las regiones adicionales desde la consola del IAM Identity Center, tal y como se describe en. [Los puntos finales ACS son el principal y el adicional Regiones de AWS](#)
2. En el panel de navegación del panel de Okta administración, seleccione Aplicaciones y, a continuación, vuelva a seleccionar Aplicaciones en la lista ampliada.
3. Elija la aplicación de AWS IAM Identity Center.
4. Elija la pestaña Sign On (Iniciar sesión).
5. En Configuración avanzada de inicio de sesión y otros SSO solicitables URLs, selecciona Añadir otro para cada URL de ACS adicional de la región y pega la URL de ACS en el campo de texto.
6. Cuando termine de añadir el ACS URLs, guarda la aplicación. AWS IAM Identity Center
7. Puede crear una aplicación de marcadores Okta para el portal de AWS acceso en cada región adicional. Esto permite a sus usuarios acceder al portal de AWS acceso en otras regiones desde Okta. Asegúrese de conceder a sus usuarios permisos para acceder a las aplicaciones de marcadores en Okta las que aparecen. Consulta [Okta documentación](#) para obtener más información.

8. Compruebe que puede iniciar sesión en el portal de AWS acceso de cada región adicional. Navegue hasta el [portal de AWS acceso URLs](#) o inicie las aplicaciones desde Okta las que se marcan como favoritas.

## Siguientes pasos

Ahora que ha configurado Okta como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Conceda acceso a Cuentas de AWS, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).
- Para conceder acceso a las aplicaciones en la nube, consulte [Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center](#).
- Para configurar los permisos en función de los cargos en el trabajo; consulte [Crear un conjunto de permisos](#).

## Resolución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con Okta, consulte las secciones siguientes:

- [Reaprovisionamiento de usuarios y grupos eliminados de IAM Identity Center](#)
- [Error de aprovisionamiento automático en Okta](#)
- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- [Recursos adicionales](#)

## Reaprovisionamiento de usuarios y grupos eliminados de IAM Identity Center

- Puede recibir el siguiente mensaje de error en la consola de Okta si intenta cambiar un usuario o un grupo en Okta que alguna vez se sincronizó y luego se eliminó del IAM Identity Center:

- No se AWS IAM Identity Center pudo enviar automáticamente el perfil del usuario *Jane Doe* a la aplicación: se produjo un error al intentar enviar la actualización del perfil de *jane\_doe@example.com*: No se devolvió ningún usuario para el usuario `xxxxx-xxxxxx-xxxxx-xxxxxx`
- Falta el grupo vinculado en AWS IAM Identity Center. Cambia el grupo vinculado para volver a aumentar las membresías del grupo.
- También puede recibir el siguiente mensaje de error en los registros del sistema de Okta para los usuarios o grupos del IAM Identity Center sincronizados o eliminados:
  - Error de Okta: Eventfailed application.provision.user.push\_profile: No se ha devuelto ningún usuario como usuario `xxxxx-xxxxxx-xxxxx-xxxxxx`
  - Error de Okta: application.provision.group\_push.mapping.update.or.delete.failed.with.error: falta un grupo vinculado en. AWS IAM Identity Center Cambia el grupo vinculado para volver a aumentar las membresías del grupo.

#### Warning

Si ha sincronizado Okta e IAM Identity Center mediante SCIM, debe eliminar los usuarios y los grupos de Okta en lugar del IAM Identity Center.

## Resolución de problemas de usuarios eliminados de IAM Identity Center

Para solucionar este problema con los usuarios eliminados del IAM Identity Center, los usuarios deben eliminarse de Okta. Si fuera necesario, también habría que volver a crear estos usuarios en Okta. Cuando se vuelva a crear el usuario en Okta, también se volverá a aprovisionar en el IAM Identity Center a través de SCIM. Para obtener más información sobre eliminar un usuario, consulte la [documentación de Okta](#).

#### Note

Si necesita eliminar el acceso de un usuario de Okta al IAM Identity Center, primero debe eliminarlo de su Group Push y, después, de su grupo de tareas en Okta. De este modo, se garantiza que el usuario deje de pertenecer a su grupo asociado en el IAM Identity Center. Para obtener más información sobre la resolución de problemas de Group Push, consulte la [documentación de Okta](#).

## Resolución de problemas de grupos eliminados de IAM Identity Center

Para solucionar este problema con los IAM Identity Center eliminados, el grupo debe eliminarse de Okta. Si fuera necesario, estos grupos también deberían volver a crearse en Okta mediante Group Push. Cuando se vuelva a crear el usuario en Okta, también se volverá a aprovisionar en el IAM Identity Center a través de SCIM. Para obtener más información sobre la eliminación de un grupo, consulte la [documentación de Okta](#).

## Error de aprovisionamiento automático en Okta

Si recibe un error en Okta:

Falló el aprovisionamiento automático del usuario Jane Doe a la aplicación: no se encontró el usuario coincidente AWS IAM Identity Center

Consulte la [documentación de la Okta](#) para obtener más información.

## Recursos adicionales

- Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas de IAM Identity Center](#).

Los siguientes recursos pueden ayudarle a solucionar problemas a medida que trabaja con: AWS

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Configuración del aprovisionamiento de SCIM entre OneLogin e IAM Identity Center

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde OneLogin a IAM Identity Center mediante el protocolo Sistema de administración de identidades entre dominios (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

### Note

OneLogin actualmente no admite el servicio de consumo de aserciones múltiples (ACS) de SAML URLs en la AWS IAM Identity Center aplicación. Esta función de SAML es necesaria

para aprovechar al máximo el [soporte multirregional del IAM Identity Center](#). Si planea replicar el Centro de Identidad de IAM en otras regiones, tenga en cuenta que el uso de una sola URL de ACS puede afectar a la experiencia del usuario en esas regiones adicionales. Su región principal seguirá funcionando con normalidad. Le recomendamos que trabaje con su proveedor de IdP para habilitar esta función. Para obtener más información sobre la experiencia del usuario en otras regiones con una única URL de ACS, consulte [the section called “Uso de aplicaciones AWS gestionadas sin varios ACS URLs”](#) y [the section called “Cuenta de AWS resiliencia de acceso sin varios ACS URLs”](#).

Esta conexión se configura en OneLogin mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en OneLogin con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y OneLogin.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos de OneLogin a IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#).

## Temas

- [Requisitos previos](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: configure el aprovisionamiento en OneLogin](#)
- [\(Opcional\) Paso 3: configure los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Resolución de problemas](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Una cuenta de OneLogin. Si no tiene una cuenta existente, es posible que pueda obtener una cuenta de prueba gratuita o una cuenta de desarrollador en el [sitio web OneLogin](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde su cuenta de OneLogin a IAM Identity Center. Para obtener más información, consulte [Enabling Single Sign-On Between OneLogin and AWS](#) en el Partner Network Blog de AWS .

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.



 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

## 5. Seleccione Cerrar.

Ha configurado el aprovisionamiento en la consola de IAM Identity Center. Ahora debe realizar las tareas restantes mediante la interfaz de usuario de OneLogin, tal y como se describe en los siguientes procedimientos.

## Paso 2: configure el aprovisionamiento en OneLogin

Utilice el siguiente procedimiento en el portal de administración de OneLogin para habilitar la integración entre IAM Identity Center y la aplicación IAM Identity Center. Este procedimiento supone que ya ha configurado la aplicación de inicio de sesión único para la autenticación SAML AWS . OneLogin Si aún no ha creado esta conexión SAML, hágalo antes de continuar y, a continuación, vuelva aquí para completar el proceso de aprovisionamiento del SCIM. Para obtener más información para configurar SAML con OneLogin, consulte [Enabling Single Sign-On Between OneLogin and AWS](#) en el Partner Network Blog de AWS .

### Cómo configurar el aprovisionamiento en OneLogin

1. Inicie sesión en OneLogin y vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. Selecciónela y, luego, seleccione Configuración en el panel de navegación.
3. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base de SCIM en OneLogin. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Tokens portadores de SCIM en OneLogin.
4. Junto a Conexión API, haga clic en Habilitar y, a continuación, en Guardar para completar la configuración.

5. En el panel de navegación, seleccione Provisioning (Aprovisionamiento).
6. Seleccione las casillas de verificación Habilitar el aprovisionamiento, Crear usuario, Eliminar usuario y Actualizar usuario y, a continuación, seleccione Guardar.
7. En el panel de navegación, seleccione Usuarios.
8. Haga clic en Más acciones y seleccione Sincronizar inicios de sesión. Deberías recibir el mensaje Sincronizar usuarios con single sign-On de AWS .
9. Vuelva a hacer clic en Más acciones y, a continuación, seleccione Volver a aplicar las asignaciones de derechos. Debería recibir el mensaje Se están reaplicando las asignaciones.
10. En este punto, debería comenzar el proceso de aprovisionamiento. Para confirmarlo, vaya a Actividad > Eventos y supervise el progreso. Los eventos de aprovisionamiento correctos, así como los errores, deberían aparecer en la secuencia de eventos.
11. Para comprobar que todos sus usuarios y grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de OneLogin aparecerán en la página de Usuarios. También puede ver sus grupos sincronizados en la página Grupos.
12. Para sincronizar automáticamente los cambios de los usuarios con el Centro de identidades de IAM, vaya a la página de aprovisionamiento, busque la sección Requerir la aprobación del administrador antes de realizar esta acción, anule la selección de Crear usuario, Eliminar usuario, Actualizar usuario y haga clic en Guardar. and/or

## (Opcional) Paso 3: configure los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional OneLogin si decide configurar los atributos que utilizará en el Centro de identidades de IAM para gestionar el acceso a sus recursos. AWS Los atributos que defina en OneLogin se transfieren en una aserción de SAML a IAM Identity Center. A continuación, deberá crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde OneLogin.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

## Cómo configurar atributos de usuario utilizados en OneLogin para el control de acceso en IAM Identity Center

1. Inicie sesión en OneLogin y vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. Selecciónela y, luego, en el panel de navegación, seleccione Parámetros.
3. En la sección Parámetros obligatorios, haga lo siguiente para cada atributo que desee utilizar en IAM Identity Center:
  - a. Elija +.
  - b. En Nombre del campo, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName` y sustituya **AttributeName** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
  - c. En Banderas, marque la casilla situada junto a Incluir en la afirmación de SAML y seleccione Guardar.
  - d. En el campo Valor, usa la lista desplegable para elegir los atributos del usuario de OneLogin. Por ejemplo, Departamento.
4. Seleccione Save.

### (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento Attribute con el atributo Name configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento AttributeValue que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
```

```
</saml:Attribute>  
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Resolución de problemas

La siguiente información puede ayudarle a solucionar algunos problemas comunes que puede encontrarse a la hora de configurar o utilizar la consola de OneLogin.

### Los grupos no se aprovisionan en IAM Identity Center

De forma predeterminada, los grupos no se pueden aprovisionar desde OneLogin a IAM Identity Center. Asegúrese de haber activado el aprovisionamiento de grupos para su aplicación de IAM Identity Center en OneLogin. Para ello, inicie sesión en la consola de administración de OneLogin y compruebe que la opción Incluir en el aprovisionamiento de usuarios esté seleccionada en las propiedades de la aplicación IAM Identity Center (Aplicación IAM Identity Center > Parámetros > Grupos). Para obtener más información sobre cómo crear grupos en OneLogin, incluida la forma de sincronizar los roles de OneLogin como grupos en SCIM, consulte el [sitio web de OneLogin](#).

No se sincroniza nada desde OneLogin a IAM Identity Center, a pesar de que todos los ajustes son correctos

Además de la nota anterior sobre la aprobación del administrador, tendrá que volver a aplicar las asignaciones de derechos para que se apliquen muchos cambios de configuración. Esto se encuentra en Aplicaciones > Aplicaciones > Aplicación IAM Identity Center > Más acciones. Puede ver los detalles y los registros de la mayoría de las acciones en OneLogin, incluidos los eventos de sincronización, en Actividad > Eventos.

He eliminado o desactivado un grupo en OneLogin, pero sigue apareciendo en IAM Identity Center

Actualmente, OneLogin no admite la operación SCIM DELETE para grupos, lo que significa que el grupo sigue existiendo en IAM Identity Center. Por lo tanto, deberá eliminar el grupo directamente de IAM Identity Center para asegurarse de que se eliminen todos los permisos correspondientes en IAM Identity Center para ese grupo.

He eliminado un grupo del Centro de Identidad de IAM sin eliminarlo primero OneLogin y ahora tengo problemas user/group de sincronización

Para solucionar esta situación, primero asegúrese de no tener ninguna regla o configuración de aprovisionamiento de grupos redundante en OneLogin. Por ejemplo, un grupo asignado directamente a una aplicación junto con una regla que se publica en el mismo grupo. A continuación, elimine los grupos no deseados de IAM Identity Center. Por último, en OneLogin, actualice los derechos (aplicación IAM Identity Center > Aprovisionamiento > Derechos) y, a continuación, vuelva a aplicar las asignaciones de derechos (aplicación IAM Identity Center > Más acciones). Para evitar este problema en el futuro, primero realice el cambio para dejar de aprovisionar el grupo en OneLogin y, a continuación, elimine el grupo de IAM Identity Center.

## Uso de productos de Ping Identity con IAM Identity Center

Los siguientes productos de Ping Identity se han probado con IAM Identity Center.

### Temas

- [PingFederate](#)
- [PingOne](#)

## PingFederate

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde PingFederate por parte de Ping Identity (de ahora en adelante “Ping”) a IAM Identity Center. Este aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en PingFederate mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en PingFederate con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y PingFederate.

Esta guía se basa en la versión 10.2 de PingFederate. Los pasos para las versiones más recientes pueden variar. Póngase en contacto con Ping para obtener más información sobre cómo configurar el aprovisionamiento en IAM Identity Center para otras versiones de PingFederate.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos de PingFederate a IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: configure el aprovisionamiento en PingFederate](#)
- [\(Opcional\) Paso 3: Configurar los atributos de usuario en erate para el control de acceso en PingFed el IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Resolución de problemas](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Un servidor de PingFederate que funcione. Si no tiene una cuenta existente en el server de PingFederate, es posible que pueda obtener una cuenta de prueba gratuita o una cuenta de desarrollador en el sitio web de [Ping Identity](#). La versión de prueba incluye licencias y descargas de software y la documentación asociada.
- Una copia del software IAM Identity Center Connector de PingFederate instalado en su servidor de PingFederate. Para obtener más información sobre cómo obtener este software, consulte [IAM Identity Center Connector](#) en el sitio web de Ping Identity.
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde su instancia de PingFederate al IAM Identity Center. Para obtener instrucciones sobre cómo configurar esta conexión, consulte la documentación de PingFederate. En resumen, la ruta recomendada es utilizar el conector de IAM Identity Center para configurar el “SSO del navegador” en PingFederate y utilizar las características de “descarga” e “importación”

de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingFederate y IAM Identity Center.

- Si ha replicado el Centro de identidades de IAM en regiones adicionales, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones AWS gestionadas y Cuentas de AWS desde esas regiones. Para obtener más información, consulte [the section called “Paso 3: Actualizar la configuración del IdP externo”](#). Consulte la PingFederate documentación para obtener más información.

## Consideraciones

Las siguientes son consideraciones importantes sobre PingFederate que pueden afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- Si se elimina un atributo de un usuario en PingFederate, ese atributo no se eliminará del usuario correspondiente en IAM Identity Center. Se trata de una limitación conocida en la implementación del aprovisionador de PingFederate's. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincroniza con IAM Identity Center.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`

- b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante la consola administrativa de PingFederate. Los pasos se describen en el siguiente procedimiento.

## Paso 2: configure el aprovisionamiento en PingFederate

Utilice el siguiente procedimiento en el portal de administración de PingFederate para habilitar la integración entre IAM Identity Center y la aplicación IAM Identity Center. En este procedimiento, se presupone que ya ha instalado el software del conector de IAM Identity Center. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

 Important

Si su servidor de PingFederate no se ha configurado previamente para el aprovisionamiento de SCIM saliente, es posible que deba realizar un cambio en el archivo de configuración para habilitar el aprovisionamiento. Para obtener más información, consulte la documentación de Ping. En resumen, debe modificar la configuración de `pf.provisioner.mode` del archivo `pingfederate-<version>/pingfederate/bin/run.properties` a un valor distinto a OFF (que es el predeterminado) y reiniciar el servidor si se está ejecutando actualmente. Por ejemplo, puede utilizar STANDALONE si actualmente no tiene una configuración de alta disponibilidad con PingFederate.



## Cómo configurar el aprovisionamiento en PingFederate

1. Inicie sesión en la consola administrativa de PingFederate.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. Debería ver que el SSO del navegador ya estaba seleccionado en su configuración anterior de SAML. Si no es así, primero debe completar esos pasos antes de continuar.
5. Seleccione la casilla de verificación Aprovisionamiento saliente, elija IAM Identity Center Cloud Connector como tipo y haga clic en Guardar. Si IAM Identity Center Cloud Connector no aparece como opción, asegúrese de haber instalado IAM Identity Center Cloud Connector y de haber reiniciado el servidor de PingFederate.
6. Haga clic en Siguiente varias veces hasta llegar a la página Aprovisionamiento saliente y, a continuación, haga clic en el botón Configurar aprovisionamiento.
7. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM en la consola de PingFederate. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token de acceso en la consola de PingFederate. Haga clic en Guardar.
8. En la página Configuración del canal (Configurar canal), haga clic en Crear.
9. Introduzca un nombre del canal para este nuevo canal de aprovisionamiento (por ejemplo **AWSIAMIdentityCenterchannel**) y haga clic en Siguiente.
10. En la página Origen, elija el almacén de datos activo que desee utilizar para la conexión al IAM Identity Center y haga clic en Siguiente.

### Note

Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la documentación del producto de Ping para obtener información sobre cómo elegir y configurar un origen de datos en PingFederate.

11. En la página Configuración de origen, confirme que todos los valores son correctos para la instalación y, a continuación, haga clic en Siguiente.

12. En la página Ubicación de origen, introduzca la configuración adecuada para su origen de datos y, a continuación, haga clic en Siguiente. Por ejemplo, si utiliza Active Directory como directorio LDAP:
  - a. Introduzca el DN base de su bosque de AD (por ejemplo, **DC=myforest,DC=mydomain,DC=com**).
  - b. En Usuarios > DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. Si no existe ese grupo único, créelo en AD, vuelva a esta configuración y, a continuación, introduzca el DN correspondiente.
  - c. Especifique si desea buscar subgrupos (Búsqueda anidada) y cualquier filtro LDAP necesario.
  - d. En Usuarios > DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. En muchos casos, puede ser el mismo DN que especificó en la sección Usuarios. Introduzca los valores búsqueda anidada y filtro según sea necesario.
13. En la página Asignación de atributos, asegúrese de lo siguiente y, a continuación, haga clic en Siguiente:
  - a. El campo userName debe asignarse a un atributo con formato de correo electrónico (user@domain.com). También debe coincidir con el valor que el usuario utilizará para iniciar sesión en Ping. Este valor, a su vez, se rellena en la notificación del nameId de SAML durante la autenticación federada y se utiliza para hacer coincidir con el usuario de IAM Identity Center. Por ejemplo, cuando utilice Active Directory, puede optar por especificar el UserPrincipalName como userName.
  - b. Los demás campos con un sufijo \* deben asignarse a atributos que no sean nulos para los usuarios.
14. En la página Activación y resumen, defina el estado del canal como Activo para que la sincronización comience inmediatamente después de guardar la configuración.
15. Confirme que todos los valores de configuración de la página son correctos y haga clic en Listo.
16. En la página Administrar canales, haga clic en Guardar.
17. En este punto, comienza el aprovisionamiento. Para confirmar la actividad, puede ver el archivo provisioner.log, que se encuentra de forma predeterminada en el directorio pingfederate-  
<version>/pingfederate/log de su servidor de PingFederate.
18. Para comprobar que los usuarios y los grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios

sincronizados de PingFederate aparecerán en la página de Usuarios. También puede ver sus grupos sincronizados en la página Grupos.

### (Opcional) Paso 3: Configurar los atributos de usuario en erate para el control de acceso en PingFed el IAM Identity Center

Se trata de un procedimiento opcional PingFederate si decide configurar los atributos que utilizará en el Centro de identidades de IAM para gestionar el acceso a sus recursos. AWS Los atributos que defina en PingFederate se transfieren en una aserción de SAML a IAM Identity Center. A continuación, deberá crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde PingFederate.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Cómo configurar atributos de usuario utilizados en PingFederate para el control de acceso en IAM Identity Center

1. Inicie sesión en la consola administrativa de PingFederate.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. A continuación, haga clic en Configurar el SSO del navegador.
5. En la página Configurar el SSO del navegador, seleccione Creación de aserciones y, a continuación, haga clic en Configurar creación de aserciones.
6. En la página Configurar la creación de aserciones, elija Contrato de atributos.
7. En la página Contrato de atributos, en la sección Ampliar el contrato, añada un nuevo atributo siguiendo estos pasos:
  - a. En el cuadro de texto, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, sustituya **AttributeName** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.

- b. En Formato de nombre de atributo, elija urn:oasis:names:tc:SAML:2.0:attrname-format:uri.
  - c. Elija Añadir, y a continuación, elija Siguiente.
8. En la página de asignación de fuentes de autenticación, elija la instancia de adaptador configurada con su aplicación.
9. En la página Cumplimiento del contrato de atributo, elija el origen (almacén de datos) y el valor (atributo del almacén de datos) para el contrato de atributo `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.

 Note

Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la documentación del producto de Ping para obtener información sobre cómo elegir y configurar un origen de datos en PingFederate.

10. Haga clic en Siguiente varias veces hasta llegar a la página de activación y resumen y, a continuación, haga clic en Guardar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Resolución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con PingFederate, consulte las secciones siguientes:

- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para obtener más información acerca de PingFederate, consulte la [documentación de PingFederate](#).

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con: AWS

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## PingOne

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde PingOne por parte de Ping Identity (de ahora en adelante “Ping”) a IAM Identity Center. Este aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Esta conexión se configura en PingOne mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en PingOne con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y PingOne.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios de PingOne a IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: configure el aprovisionamiento en PingOne](#)
- [\(Opcional\) Paso 3: configure los atributos de usuario en PingOne para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Resolución de problemas](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Una suscripción o una prueba gratuita de PingOne, con funciones de autenticación federada y aprovisionamiento. Para obtener más información acerca de cómo obtener una prueba gratuita, consulte el sitio web de [Ping Identity](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- La aplicación IAM Identity Center PingOne se agregó a su portal de administración de PingOne. Puede obtener la aplicación IAM Identity Center PingOne en el catálogo de aplicaciones de PingOne. Para obtener información general, consulte [Add an application from the Application Catalog](#) del sitio web de Ping Identity.
- Una conexión SAML desde su instancia de PingOne a IAM Identity Center. Una vez que la aplicación IAM Identity Center de PingOne se haya agregado a su portal de administración de PingOne, debe usarla para configurar una conexión SAML desde su instancia de PingOne a IAM Identity Center. Utilice las características de “descarga” e “importación” de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingOne y IAM Identity Center.

Para obtener instrucciones sobre cómo configurar esta conexión, consulte la documentación de PingOne.

- Si ha replicado el Centro de Identidad de IAM en otras regiones, debe actualizar la configuración de su proveedor de identidad para permitir el acceso a las aplicaciones AWS gestionadas y Cuentas de AWS desde esas regiones. Para obtener más información, consulte [the section called “Paso 3: Actualizar la configuración del IdP externo”](#). Consulte la PingOne documentación para obtener más información.

## Consideraciones

Las siguientes son consideraciones importantes sobre PingOne que pueden afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- PingOne no admite el aprovisionamiento de grupos a través de SCIM. Póngase en contacto con Ping para obtener la información más reciente sobre el apoyo grupal en SCIM para PingOne.
- Los usuarios pueden seguir aprovisionándose desde PingOne después de deshabilitar el aprovisionamiento en el portal de administración de PingOne. Si necesita finalizar el aprovisionamiento inmediatamente, elimine el token portador de SCIM correspondiente y and/or desactívelo [Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM](#) en el Centro de Identidad de IAM.
- Si se elimina un atributo de un usuario en PingOne, ese atributo no se eliminará del usuario correspondiente en IAM Identity Center. Se trata de una limitación conocida en la implementación del aprovisionador de PingOne's. Si se modifica un atributo, el cambio se sincronizará con IAM Identity Center.
- Las siguientes son notas importantes sobre la configuración de SAML en PingOne:
  - IAM Identity Center solo es compatible con emailaddress como formato de NameId. Esto significa que debe elegir un atributo de usuario que sea único en su directorioPingOne, que no sea nulo y que tenga el formato de email/UPN (por ejemplo, user@domain.com) para su mapeo de SAML\_SUBJECT. PingOne El correo electrónico (trabajo) es un valor razonable para probar las configuraciones con el directorio integrado de PingOne.
  - Es posible que los usuarios de PingOne con una dirección de correo electrónico que contenga un carácter + no puedan iniciar sesión en IAM Identity Center debido a errores como 'SAML\_215' o 'Invalid input'. Para solucionar este problema, en PingOne, seleccione la opción Avanzada para la asignación de SAML\_SUBJECT en las asignaciones de atributos. A continuación, defina el formato de ID de nombre para enviarlo a SP: para urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress en el menú desplegable.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación IAM Identity Center de PingOne. Estos pasos se explican en el procedimiento siguiente.



## Paso 2: configure el aprovisionamiento en PingOne

Utilice el siguiente procedimiento en la aplicación IAM Identity Center PingOne para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación PingOne de IAM Identity Center a la consola de administración del portal de PingOne. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

### Cómo configurar el aprovisionamiento en PingOne

1. Abra la aplicación IAM Identity Center PingOne que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones). Consulte [Requisitos previos](#).
2. Desplácese hasta el final de la página. En Aprovisionamiento de usuarios, elija el enlace completo para acceder a la configuración de aprovisionamiento de usuarios de su conexión.
3. En la página de instrucciones de aprovisionamiento, seleccione Continuar con el siguiente paso.
4. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM de la aplicación PingOne de IAM Identity Center. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo ACCESS\_TOKEN en la aplicación de PingOne de IAM Identity Center.
5. Para REMOVE\_ACTION, elija Desactivada o Eliminada (consulte el texto de descripción de la página para obtener más información).
6. En la página de asignación de atributos, elija un valor para usarlo en la afirmación SAML\_SUBJECT (NameId), siguiendo las instrucciones de [Consideraciones](#) que aparecen anteriormente en esta página. A continuación elija Continuar con el paso siguiente.
7. En la página Personalización de la aplicación IAM Identity Center PingOne, realice los cambios de personalización que desee (opcional) y haga clic en Continuar con el siguiente paso.
8. En la página Acceso grupal, seleccione los grupos que contienen los usuarios que desea habilitar para el aprovisionamiento y el inicio de sesión único en IAM Identity Center. Elija Continuar con el paso siguiente.
9. Desplácese hasta el final de la página y seleccione Finalizar para iniciar el aprovisionamiento.
10. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de PingOne aparecerán en la página Usuarios. Estos usuarios ahora pueden asignarse a cuentas en IAM Identity Center.

Recuerde que PingOne no admite el aprovisionamiento de grupos o la pertenencia a grupos a través de SCIM. Póngase en contacto con la asistencia de Ping para obtener más información.

## (Opcional) Paso 3: configure los atributos de usuario en PingOne para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional PingOne si decide configurar los atributos del Centro de Identidad de IAM para gestionar el acceso a sus recursos. AWS Los atributos que defina en PingOne se transfieren en una aserción de SAML a IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde PingOne.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

### Cómo configurar atributos de usuario utilizados en PingOne para el control de acceso en IAM Identity Center

1. Abra la aplicación IAM Identity Center PingOne que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones).
2. Elija Editar y, a continuación, elija Continuar con el siguiente paso hasta llegar a la página Asignaciones de atributos.
3. En la página Asignaciones de atributos, elija Añadir nuevo atributo. A continuación, siga estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.
  - a. En el campo Atributo de la aplicación, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`. Sustituya **Attribute**Name**** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
  - b. En el campo del atributo o valor lineal del puente de identidades, elija los atributos de usuario de su directorio de PingOne. Por ejemplo, Correo electrónico (trabajo).
4. Elija Siguiente y, a continuación, haga clic en Terminar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Resolución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con PingOne, consulte las secciones siguientes:

- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para obtener más información acerca de PingOne, consulte la [documentación de PingOne](#).

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con: AWS

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

# Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center

Cuando se habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado, por lo que no tiene que seleccionar uno. Si su organización utiliza otro proveedor de identidades, como Microsoft Active Directory, Microsoft Entra ID o Okta, considere la posibilidad de integrar ese origen de identidad con IAM Identity Center en lugar de utilizar la configuración predeterminada.

## Objetivo

En este tutorial, utilizará el directorio predeterminado como origen de identidad y una instancia de organización de IAM Identity Center para configurar y probar un usuario administrativo. Este usuario administrativo crea y administra usuarios y grupos y concede el AWS acceso con conjuntos de permisos. En los siguientes pasos, creará lo siguiente:

- Un usuario administrativo llamado *Nikki Wolf*
- Un grupo llamado *Admin team*
- Un conjunto de permisos denominado *AdminAccess*

Para comprobar que todo se creó correctamente, deberá iniciar sesión y establecer la contraseña del usuario administrativo. Tras completar este tutorial, puede utilizar el usuario administrativo para agregar más usuarios a IAM Identity Center, crear conjuntos de permisos adicionales y configurar el acceso organizativo a las aplicaciones. Como alternativa, si desea conceder a los usuarios el acceso a la aplicación, puede seguir el [paso 1](#) de este procedimiento y [configurar el acceso a la aplicación](#).

## Requisitos previos

Para completar este tutorial, necesita los siguientes requisitos previos:

- [Activar IAM Identity Center](#) y tener una [instancia de organización de IAM Identity Center](#).
  - Si tiene una [instancia de cuenta](#) de IAM Identity Center, puede crear usuarios y grupos, así como concederles acceso a las aplicaciones. Para obtener más información, consulte [Application access](#).
- Inicie sesión en la consola del IAM Identity Center Consola de administración de AWS y acceda a ella de la siguiente manera:

- Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta seleccionando el usuario Cuenta de AWS root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
- Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
- [Para obtener más ayuda para iniciar sesión en Consola de administración de AWS, consulte AWS Sign-In la Guía.](#)
- Puede configurar la autenticación multifactor para los usuarios de IAM Identity Center. Para obtener más información, consulte [Configuración de la MFA en IAM Identity Center](#).

## Paso 1: adición de un usuario

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación de IAM Identity Center, seleccione Usuarios y, a continuación, seleccione Agregar usuario.
3. En la página Especificar los detalles del usuario, rellene la siguiente información:

- Nombre de usuario: para este tutorial, introduzca *nikkiw*.

Al crear los usuarios, seleccione nombres de usuario que sean fáciles de recordar. Sus usuarios deben recordar el nombre de usuario para iniciar sesión en el portal de AWS acceso y no pueden cambiarlo más adelante.

- Contraseña: seleccione Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña (recomendado).

Esta opción envía al usuario un correo electrónico de Amazon Web Services, con el asunto Invitación para unirse a IAM Identity Center. El correo electrónico proviene de `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Agregue estas direcciones de correo electrónico a su lista de remitentes aprobados.

- Dirección de correo electrónico: ingrese una dirección de correo electrónico del usuario en la que pueda recibir el correo electrónico. A continuación, vuelva a escribirla para confirmarla. Cada usuario debe tener una dirección de correo electrónico única.
- En Nombre, ingrese el nombre del usuario. En este tutorial, escriba *Nikki*.
- En Apellido, ingrese el apellido del usuario. En este tutorial, escriba *Wolf*.

- Nombre de visualización: el valor predeterminado es el nombre y apellido del usuario. Si desea cambiar el nombre de visualización, puede ingresar otro nombre. El nombre de visualización está visible en el portal de inicio de sesión y en la lista de usuarios.
  - Complete la información opcional si lo desea. No se usa durante este tutorial y puede cambiarla más adelante.
4. Elija Siguiente. Aparece la página Agregar usuario a grupos. Vamos a crear un grupo al que asignarle permisos administrativos en lugar de dárselos directamente *Nikki*.

Seleccione Crear grupo.

Se abre una nueva pestaña del navegador para mostrar la página Crear grupo.

- a. En Detalles del grupo, en Nombre del grupo, ingrese un nombre para el grupo. Recomendamos un nombre de grupo que identifique el rol del grupo. En este tutorial, escriba *Admin team*.
  - b. Seleccione Crear grupo.
  - c. Cierre la pestaña Grupos del navegador para volver a la pestaña Agregar usuario del navegador.
5. En el área Grupos, seleccione el botón Actualizar. El *Admin team* grupo aparece en la lista.

Seleccione la casilla de verificación situada junto a *Admin team*, a continuación, elija Siguiente.

6. En la página Revisar y agregar usuario, confirme lo siguiente:
- La información principal aparece tal y como quería.
  - En Grupos se muestra el usuario agregado al grupo que ha creado

Si desea realizar cambios, seleccione Editar. Cuando todos los detalles sean correctos, seleccione Agregar usuario.

Un mensaje de notificación le informará de que se ha agregado el usuario.

A continuación, añadirá permisos administrativos para que el *Admin team* grupo *Nikki* tenga acceso a los recursos.

## Paso 2: adición de permisos administrativos

### Important

Siga estos pasos solo si ha activado una [instancia de organización de IAM Identity Center](#).

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la organización con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. Para el paso 1: Seleccione los usuarios y los grupos, elija el **Admin team** grupo que ha creado. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado **AdministratorAccess** con una duración de sesión establecida en una hora. Puede cambiar el nombre del conjunto de permisos al introducir un nombre nuevo en el campo Nombre del conjunto de permisos.
    - iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

- c. En la página Paso 3: Revisar y enviar las tareas, confirme que el *Admin team* grupo y el conjunto de *AdministratorAccess* permisos están seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado.

 ¡Enhorabuena!

Ha configurado correctamente su primer usuario, grupo y conjunto de permisos.

En la siguiente parte de este tutorial, probará el *Nikki's* acceso iniciando sesión en el portal de AWS acceso con sus credenciales administrativas y configurando su contraseña. Cierre la sesión de la consola.

### Paso 3: Probar el acceso de los usuarios

Ahora que *Nikki Wolf* es un usuario de su organización, puede iniciar sesión y acceder a los recursos para los que tiene permiso de acuerdo con su conjunto de permisos. Para comprobar que el usuario está configurado correctamente, en el siguiente paso utilizarás *Nikki's* las credenciales para iniciar sesión y configurar su contraseña. Cuando agregaste el usuario *Nikki Wolf* en el paso 1, elegiste *Nikki* recibir un correo electrónico con las instrucciones para configurar la contraseña. Es hora de abrir el correo electrónico y hacer lo siguiente:

1. En el correo electrónico, seleccione el enlace Aceptar la invitación para aceptar la invitación.



 Note

El correo electrónico también incluye el nombre de *Nikki 's* usuario y la URL del portal de AWS acceso que utilizarán para iniciar sesión en la organización. Registre esta información para usarla más adelante.

Accederá a la página de registro de nuevos usuarios, donde podrá establecer la *Nikki 's* contraseña y [registrar su dispositivo MFA](#).

2. Tras configurar la *Nikki 's* contraseña, accederá a la página de inicio de sesión. Ingresa *nikkiw* y selecciona Siguiente, luego ingresa la *Nikki 's* contraseña y selecciona Iniciar sesión.
3. Se abre el portal de AWS acceso y muestra la organización y las aplicaciones a las que puede acceder.

Seleccione la organización para ampliarla en una lista y, a Cuentas de AWS continuación, seleccione la cuenta para ver las funciones que puede utilizar para acceder a los recursos de la cuenta.

Cada conjunto de permisos tiene dos métodos de administración que puede utilizar: rol o claves de acceso.

- Rol, por ejemplo *AdministratorAccess*: abre el AWS Console Home.
  - Claves de acceso: proporcionan credenciales que puede usar con el AWS CLI o y el AWS SDK. Incluye la información para usar credenciales de corta duración que se actualizan automáticamente o claves de acceso de corta duración. Para obtener más información, consulte [Obtener las credenciales de usuario del IAM Identity Center para o AWS CLI AWS SDKs](#).
4. Elija el enlace del rol para iniciar sesión en AWS Console Home.

Has iniciado sesión y has accedido a la AWS Console Home página. Explore la consola y confirme que tiene el acceso que esperaba.

## Siguientes pasos

Ahora que ha creado un usuario administrativo en IAM Identity Center, puede hacer lo siguiente:

- [Asignar aplicaciones](#)
- [Agregar otros usuarios](#)
- [Asignar usuarios a las cuentas](#)
- [Configurar conjuntos de permisos adicionales](#)

 Note

Puede asignar varios conjuntos de permisos al mismo usuario. Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo al mismo usuario. De esta forma, podrá acceder a la suya únicamente Cuenta de AWS con los permisos que necesite, en lugar de con permisos administrativos.

Una vez que los usuarios [acepten la invitación](#) para activar su cuenta e inicien sesión en el portal de AWS acceso, los únicos elementos que aparecen en el Cuentas de AWS portal son los roles y las aplicaciones a los que están asignados.

## Tutoriales de vídeo

Como recurso adicional, puede utilizar estos tutoriales en video para obtener más información sobre la configuración de proveedores de identidad externos:

- [Migración entre proveedores de identidad externos en AWS IAM Identity Center](#)
- [Federar su instancia existente con AWS IAM Identity CenterMicrosoft Entra ID](#)

# Configuración del personal en IAM Identity Center

IAM Identity Center es la AWS solución para conectar a los usuarios de su fuerza laboral con aplicaciones AWS gestionadas, como Kiro y Amazon Quick, y otros AWS recursos. Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien crear y gestionar sus usuarios directamente en el IAM Identity Center.

¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo actuales para utilizar el IAM Identity Center y acceder a las aplicaciones AWS gestionadas. Si utiliza la [federación con IAM](#) para el Cuenta de AWS acceso, sus usuarios pueden seguir Cuentas de AWS accediendo de la misma manera que siempre lo han hecho, y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

Elija el enfoque que mejor se adapte a la estrategia de gestión de identidades de su organización y a la infraestructura existente.

Temas

- [Usuarios, grupos y aprovisionamiento en IAM Identity Center](#)
- [Administración de su fuente de identidad](#)
- [Administración de usuarios en el directorio de Identity Center](#)

## Usuarios, grupos y aprovisionamiento en IAM Identity Center

IAM Identity Center le permite controlar quién puede iniciar sesión y a qué recursos puede acceder. Se debe aprovisionar a un usuario para iniciar sesión. A continuación, puede asignar el acceso solo a los usuarios o grupos aprovisionados. Obtenga información sobre usuarios, grupos y aprovisionamiento en IAM Identity Center.

## Exclusividad del nombre de usuario y de la dirección de correo electrónico

IAM Identity Center requiere que cada usuario tenga un nombre de usuario único. El nombre de usuario es el identificador principal del usuario. El nombre de usuario no tiene que coincidir con la dirección de correo electrónico del usuario. IAM Identity Center exige que todos los nombres de usuario y direcciones de correo electrónico de sus usuarios sean únicos y no sean nulos.

## Groups

Los grupos son una combinación lógica de usuarios que usted define. Puede crear grupos y añadir usuarios a los grupos. IAM Identity Center no admite grupos anidados (un grupo dentro de otro grupo). Los grupos son útiles a la hora de asignar acceso a aplicaciones Cuentas de AWS y aplicaciones. En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.

## Aprovisionamiento de usuarios y grupos

El aprovisionamiento es el proceso de hacer que la información de usuarios y grupos esté disponible para su uso en el Centro de Identidad de IAM y en las aplicaciones AWS gestionadas o administradas por el cliente. Puede crear usuarios y grupos directamente en IAM Identity Center o conectar su origen de identidades a IAM Identity Center. Con IAM Identity Center, puede asignar a los usuarios y grupos el acceso a las aplicaciones conectadas y Cuentas de AWS.

El aprovisionamiento en IAM Identity Center varía en función de la fuente de identidades que utilice. Para obtener más información, consulte [Administración de su fuente de identidad](#).

## Desaprovisionamiento de usuarios y grupos

El desaprovisionamiento es el proceso de eliminar la información de usuarios y grupos de IAM Identity Center.

Si utiliza Active Directory o un proveedor de identidades externo con IAM Identity Center, debe eliminar usuarios y grupos de esos orígenes de identidades y no de IAM Identity Center. Al eliminar usuarios y grupos de IAM Identity Center, no se eliminarán del todo si su origen de identidad es Active Directory o un proveedor de identidades externo.

Si necesita desaprovisionar usuarios o grupos de IAM Identity Center, primero debe [eliminar cualquier asignación de conjuntos de permisos](#) o aplicaciones a los usuarios o grupos que desee desaprovisionar. De lo contrario, tendrá conjuntos de permisos y asignaciones de aplicaciones sin asignar en su IAM Identity Center.

# Administración de su fuente de identidad

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Después de configurar la fuente de identidad, puede buscar usuarios o grupos para concederles acceso de inicio de sesión único a Cuentas de AWS las aplicaciones o a ambos.

Solo puede tener una fuente de identidad por organización en AWS Organizations. Puede elegir una de las siguientes opciones como origen de identidad:

- [Proveedor de identidad externo](#): elija esta opción si desea administrar los usuarios en un proveedor de identidades (IdP) externo, como Okta o Microsoft Entra ID.
- [Su Active Directory local o AWS administrado](#): elija esta opción si desea conectar su. Active Directory (AD)
- [Directorio de Identity Center](#): cuando se activa IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminada. Con el directorio de Identity Center, puede crear sus usuarios y grupos y asignar su nivel de acceso a sus aplicaciones Cuentas de AWS y a las suyas.

## Note

El Centro de Identidad de IAM no SAMBA4 admite Simple AD como fuente de identidad.

## Temas

- [Consideraciones para cambiar la fuente de identidad](#)
- [Cambiar su fuente de identidad](#)
- [Atributos de usuario y grupo compatibles en IAM Identity Center](#)
- [Proveedores de identidades externos](#)
- [Directorio Microsoft AD](#)

## Consideraciones para cambiar la fuente de identidad

Aunque puede cambiar su fuente de identidad en cualquier momento, le recomendamos que considere cómo este cambio podría afectar a su implementación actual.

Si ya administra usuarios y grupos en un origen de identidad, cambiar a un origen de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del Centro de identidades de IAM, perderán el acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones.

No cambie la fuente de identidad de IAM Identity Center sin revisar las siguientes consideraciones antes de proceder. Si desea continuar con el cambio de la fuente de identidad, consulte [Cambiar su fuente de identidad](#) para obtener más información.

## Cambiar entre el directorio IAM Identity Center y Active Directory

Si ya administra usuarios y grupos en Active Directory, le recomendamos que considere la posibilidad de conectar su directorio al habilitar IAM Identity Center y elegir su origen de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.

### Important

Al cambiar el tipo de origen de identidad en IAM Identity Center a Active Directory o desde Active Directory, tenga en cuenta que el ID del almacén de identidades cambiará. Esto puede tener las siguientes implicaciones:

- La URL del portal de AWS acceso predeterminado cambiará. Deberá comunicar la nueva URL a sus empleados y actualizar los marcadores, las listas de direcciones permitidas de puertas de enlace o firewall y las configuraciones en las que se hace referencia a esta URL. Le recomendamos que realice este cambio en un período de mantenimiento programado para minimizar las interrupciones para los usuarios.
- Si utiliza una clave de KMS gestionada por el cliente para el cifrado en reposo en IAM Identity Center y ha configurado la política de claves de KMS con el contexto de cifrado, tenga en cuenta que el contexto de cifrado del almacén de identidades cambiará. Por ejemplo, en el ARN del almacén de identidades "arn:aws:identitystore::123456789012:identitystore/d-922763e9b3", "d-922763e9b3" es el ID del almacén de identidades. Para evitar la interrupción del servicio durante esta transición, modifique temporalmente su política de claves de KMS para utilizar un patrón comodín: "arn:aws:identitystore::123456789012:identitystore/\*".

Si ya administra usuarios y grupos en el directorio predeterminado de Identity Center, tenga en cuenta lo siguiente:

- **Asignaciones, usuarios y grupos eliminados:** al cambiar la fuente de identidad a Active Directory, se eliminan los usuarios y grupos del directorio de Identity Center. Este cambio también elimina las asignaciones. En este caso, después de cambiar a Active Directory, debe sincronizar los usuarios y grupos de Active Directory con el directorio de Identity Center y, a continuación, volver a aplicar sus asignaciones.

Si decide no usar Active Directory, debe crear los usuarios y grupos en el directorio de Identity Center y, a continuación, realizar las asignaciones.

- **Las asignaciones no se eliminan cuando se eliminan las identidades:** cuando se eliminan las identidades del directorio de Identity Center, las asignaciones correspondientes también se eliminan en IAM Identity Center. Sin embargo, cuando se eliminan las identidades (ya sea en Active Directory o en las identidades sincronizadas) en Active Directory, las asignaciones correspondientes no se eliminan.
- **Sin sincronización saliente para APIs:** si utiliza Active Directory como fuente de identidad, le recomendamos que utilice las opciones [Crear, Actualizar y Eliminar](#) APIs con precaución. El Centro de identidades de IAM no admite la sincronización saliente, por lo que su fuente de identidad no se actualiza automáticamente con los cambios que realiza en los usuarios o grupos que la utilizan. APIs
- **La URL del portal de acceso cambiará:** al cambiar la fuente de identidad entre el IAM Identity Center y Active Directory, también se cambiará la URL del portal de acceso. AWS
- **Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs,** los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Directorio Microsoft AD](#).

## Cómo cambiar de IAM Identity Center a un IdP externo

Si cambia la fuente de identidad de IAM Identity Center a un proveedor de identidades (IdP) externo, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las aserciones correctas: las asignaciones de usuario, las asignaciones grupales y las pertenencias a grupos seguirán funcionando siempre y cuando el nuevo IdP envíe las aserciones correctas (por ejemplo, el nombre SAML). IDs Estas confirmaciones deben coincidir con los nombres de usuario y grupos de IAM Identity Center.
- No hay sincronización saliente: IAM Identity Center no admite la sincronización saliente, por lo que su IdP externo no se actualizará automáticamente con los cambios que realice en los usuarios y grupos en IAM Identity Center.
- Aprovisionamiento de SCIM: si está usando el aprovisionamiento de SCIM, los cambios en los usuarios y grupos de su proveedor de identidades solo se reflejan en IAM Identity Center después de que su proveedor de identidades los envíe a IAM Identity Center. Consulte [Consideraciones para utilizar el aprovisionamiento automático](#).
- Retroceso: puede volver a utilizar su fuente de identidad para que utilice el IAM Identity Center en cualquier momento. Consulte [Cambiar de un IdP externo a IAM Identity Center](#).
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambia su fuente de identidad a un proveedor de identidad externo, las sesiones de usuario activas se conservan durante el resto de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso está establecida en ocho horas y cambiaste la fuente de identidad en la cuarta hora, las sesiones de usuario activas se mantendrán durante cuatro horas más. Para revocar las sesiones de usuario, consulte [the section called “Finalización de las sesiones activas de los usuarios del personal”](#).

Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

 Note

No podrá revocar las sesiones de los usuarios desde la consola de IAM Identity Center después de eliminar el usuario.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Proveedores de identidades externos](#).



## Cambiar de un IdP externo a IAM Identity Center

Si cambia la fuente de identidad de un proveedor de identidades (IdP) externo a IAM Identity Center, tenga en cuenta lo siguiente:

- IAM Identity Center conserva todas sus asignaciones.
- Forzar el restablecimiento de la contraseña: los usuarios que tenían contraseñas en IAM Identity Center pueden seguir iniciando sesión con sus contraseñas anteriores. Para los usuarios que estaban en el IdP externo y no en IAM Identity Center, el administrador debe forzar el restablecimiento de la contraseña.
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambie su fuente de identidad al IAM Identity Center, las sesiones de usuario activas se conservan durante el resto de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso es de ocho horas y ha cambiado la fuente de identidad a la cuarta hora, las sesiones de usuario activas seguirán ejecutándose durante cuatro horas más. Para revocar las sesiones de usuario, consulte [the section called “Finalización de las sesiones activas de los usuarios del personal”](#).

Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

### Note

No podrá revocar las sesiones de los usuarios desde la consola de IAM Identity Center después de eliminar el usuario.

- Soporte multirregional: si ha replicado el Centro de identidades de IAM en otras regiones o planea hacerlo, debe utilizar un proveedor de identidad externo como fuente de identidad. Para obtener más información, incluidos otros requisitos previos, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#)

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Administración de usuarios en el directorio de Identity Center](#).

## Cambiar de un IdP externo a otro IdP externo

Si ya utiliza un IdP externo como origen de identidad para IAM Identity Center y cambia a un IdP externo diferente, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las confirmaciones correctas: IAM Identity Center conserva todas sus tareas. Las asignaciones de usuarios, las asignaciones de grupos y la pertenencia a grupos seguirán funcionando siempre que el nuevo IdP envíe las afirmaciones correctas (por ejemplo, el nombre SAML). IDs

Estas confirmaciones deben coincidir con los nombres de usuario de IAM Identity Center cuando los usuarios se autenticuen a través del nuevo IdP externo.

- Aprovisionamiento de SCIM: si utiliza SCIM para el aprovisionamiento en IAM Identity Center, le recomendamos que revise la información específica del IdP en esta guía y la documentación proporcionada por el IdP para asegurarse de que el nuevo proveedor haga coincidir correctamente los usuarios y los grupos cuando SCIM esté habilitado.
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambie su fuente de identidad a otro proveedor de identidad externo, las sesiones de usuario activas se conservan durante el tiempo restante de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso es de ocho horas y cambiaste la fuente de identidad a la cuarta hora, las sesiones de usuario activas se mantendrán durante cuatro horas más. Para revocar las sesiones de usuario, consulte [the section called “Finalización de las sesiones activas de los usuarios del personal”](#).

Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

### Note

No podrá revocar las sesiones de los usuarios desde la consola de IAM Identity Center después de eliminar el usuario.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Proveedores de identidades externos](#).

## Cambiar de Active Directory a un IdP externo

Si cambia la fuente de identidad de un IdP externo a Active Directory o de Active Directory a un IdP externo, tenga en cuenta lo siguiente:

- Se eliminan los usuarios, los grupos y las asignaciones: todos los usuarios, grupos y asignaciones se eliminan de IAM Identity Center. Ninguna información de usuario o grupo se ve afectada ni en el IdP externo ni en Active Directory.
- Aprovisionamiento de usuarios: si cambia a un IdP externo, debe configurar IAM Identity Center para aprovisionar a los usuarios. Como alternativa, debe aprovisionar manualmente los usuarios y grupos para el IdP externo antes de poder configurar las asignaciones.
- Creación de asignaciones y grupos: si cambia a Active Directory, debe crear asignaciones con los usuarios y grupos que se encuentran en el directorio de Active Directory.
- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).
- Soporte multirregional: si ha replicado el Centro de identidades de IAM en otras regiones o planea hacerlo, debe utilizar un proveedor de identidad externo como fuente de identidad. Para obtener más información, incluidos otros requisitos previos, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#)

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Directorio Microsoft AD](#).

## Cambiar su fuente de identidad

El siguiente procedimiento describe cómo cambiar de un directorio que proporciona IAM Identity Center (el directorio predeterminado de Identity Center) a Active Directory o a un proveedor de identidad externo, o viceversa. Antes de continuar, revise la información incluida en [Consideraciones para cambiar la fuente de identidad](#). Para completar este procedimiento, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

 **Warning**

En función de su implementación actual, este cambio elimina cualquier asignación de usuarios y grupos que haya configurado en IAM Identity Center. Este cambio también eliminará sus Cuentas de AWS funciones de IAM del conjunto de permisos. En consecuencia, es posible que deba actualizar sus políticas de recursos y asegurarse de que esto no interrumpa su acceso a AWS KMS las claves y a los clústeres de Amazon EKS. Para obtener más información, consulte [Hacer referencia a conjuntos de permisos en las políticas de recursos, los mapas de configuración de Amazon EKS Cluster y las políticas AWS KMS clave](#).

Cuando esto ocurra, todos los usuarios y grupos, incluido el usuario administrativo del Centro de Identidad de IAM, perderán el acceso de inicio de sesión único a sus aplicaciones y a sus Cuentas de AWS aplicaciones.

Cómo cambiar la fuente de identidad:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Origen de la identidad. Elija Acciones y, a continuación, elija Cambiar fuente de identidad.
4. En Elegir fuente de identidad, seleccione la fuente a la que desee cambiar y, a continuación, seleccione Siguiente.

Si va a cambiar a Active Directory, elija el directorio disponible en el menú de la página siguiente.

 **Important**

Al cambiar la fuente de identidad a o desde Active Directory, se eliminan los usuarios y grupos del directorio de Identity Center. Este cambio también elimina cualquier asignación que haya configurado en IAM Identity Center.

 Note

Si ha replicado el Centro de identidades de IAM en otras regiones, no podrá cambiar el tipo de fuente de identidad. Solo puede reemplazar el IdP externo actual por otro. Para cambiar el tipo de fuente de identidad, primero tendrás que eliminar todas las regiones adicionales. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#)

Si va a cambiar a un proveedor de identidad externo, recomendamos que siga los pasos descritos en [Cómo conectarse a un proveedor de identidades externo](#).

5. Cuando haya leído el aviso legal y esté listo para continuar, introduzca Aceptar.
6. Elija Cambiar fuente de identidad. Si va a cambiar su fuente de identidad a Active Directory, vaya al siguiente paso.
7. Si cambia la fuente de identidad a Active Directory, accederá a la página de Configuración. Utilice la página de configuración para realizar cualquiera de las siguientes operaciones:
  - Seleccione Iniciar la configuración guiada. Para obtener información sobre cómo completar el proceso de configuración guiada, consulte [Configuración guiada](#).
  - En la sección Fuente de identidad, elija Acciones y, a continuación, elija Administrar la sincronización para configurar el Alcance de la sincronización, la lista de usuarios y grupos que se van a sincronizar.

## Atributos de usuario y grupo compatibles en IAM Identity Center

Esta guía proporciona una referencia para la compatibilidad con los atributos de SCIM en IAM Identity Center. Enumera los atributos del usuario y del grupo de la especificación SCIM que son compatibles con el almacén de identidades de IAM Identity Center e identifica atributos y subatributos específicos que no son compatibles.

Los atributos son fragmentos de información que le ayudan a definir e identificar a usuarios individuales o a agrupar objetos, como `name`, `email` o `members`. IAM Identity Center es compatible con los atributos más utilizados mediante la entrada manual y el aprovisionamiento automático de SCIM.

- [Para obtener información sobre la especificación del Sistema para la gestión de identidades entre dominios \(SCIM\), consulte https://tools.ietf.org/html/rfc7642.](https://tools.ietf.org/html/rfc7642)
- Para obtener información sobre el aprovisionamiento manual y automático, consulte [Aprovisionamiento cuando los usuarios provienen de un IdP externo.](#)
- Para obtener información acerca de la asignación de atributos, consulte [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos.](#)

Dado que IAM Identity Center admite el SCIM para los casos de uso del aprovisionamiento automático, el directorio de Identity Center admite todos los mismos atributos de usuario y grupo que figuran en la especificación del SCIM, con algunas excepciones. En las siguientes secciones, se describen los atributos que IAM Identity Center no admite.

## Objetos de usuario no admitidos

El almacén de identidades del IAM Identity Center admite todos los atributos del esquema de usuario del SCIM (<https://tools.ietf.org/html/rfc7643#section-8.3>), excepto los siguientes:

- password
- ims
- photos
- entitlements
- x509Certificates

Se admiten todos los subatributos de los usuarios, excepto los siguientes:

- Subatributo 'display' de cualquier atributo con valores múltiples (por ejemplo, emails o phoneNumbers)
- Subatributo 'version' del atributo 'meta'

## Objetos de grupo no admitidos

[Se admiten todos los atributos del esquema de grupo SCIM \(/rfc7643#section-8.4\). https://tools.ietf.org/html](https://tools.ietf.org/html/rfc7643#section-8.4)

Se admiten todos los subatributos de los grupos, excepto los siguientes:

- Subatributo 'display' de cualquier atributo con valores múltiples (por ejemplo, miembros).

## Proveedores de identidades externos

Con IAM Identity Center, puede conectar las identidades de sus empleados existentes de proveedores de identidad externos (IdPs) mediante el lenguaje de marcado de aserciones de seguridad (SAML) 2.0 y los protocolos del Sistema de gestión de identidades entre dominios (SCIM). Esto permite a los usuarios iniciar sesión en el portal de acceso AWS con sus credenciales corporativas. A continuación, pueden acceder a sus cuentas, funciones y aplicaciones asignadas alojadas en un servidor externo. IdPs

Por ejemplo, puede conectar un IdP externo, como Okta o Microsoft Entra ID, a IAM Identity Center. A continuación, sus usuarios pueden iniciar sesión en el portal de AWS acceso con sus Microsoft Entra ID credenciales Okta o credenciales existentes. Para controlar lo que pueden hacer sus usuarios una vez que han iniciado sesión, puede asignarles permisos de acceso de forma centralizada en todas las cuentas y aplicaciones de su AWS organización. Además, los desarrolladores pueden simplemente iniciar sesión en AWS Command Line Interface (AWS CLI) con sus credenciales actuales y beneficiarse de la generación y rotación automáticas de credenciales a corto plazo.

Si utiliza un directorio autogestionado en Active Directory o un directorio AWS Managed Microsoft AD, consulte. [Directorio Microsoft AD](#)

### Note

El protocolo SAML no proporciona una forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

## Aprovisionamiento cuando los usuarios provienen de un IdP externo

Al utilizar un IdP externo, debe aprovisionar todos los usuarios y grupos aplicables en el Centro de Identidad de IAM antes de poder realizar cualquier asignación o aplicación. Cuentas de AWS Para ello, puede configurar el [Aprovisionamiento de usuarios y grupos desde un proveedor de identidades externo utilizando SCIM](#) para sus usuarios y grupos o bien utilizar el [Aprovisionamiento manual](#). Independientemente de cómo aprovisiona a los usuarios, IAM Identity Center redirige la Consola

de administración de AWS interfaz de línea de comandos y la autenticación de la aplicación a su IdP externo. A continuación, IAM Identity Center concede el acceso a esos recursos en función de las políticas que cree en IAM Identity Center. Para obtener más información sobre la capacidad aprovisionada, consulte [Aprovisionamiento de usuarios y grupos](#).

## Temas

- [Cómo conectarse a un proveedor de identidades externo](#)
- [Cómo cambiar los metadatos de un proveedor de identidades externo en IAM Identity Center](#)
- [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#)
- [Perfil SCIM e implementación de SAML 2.0](#)

## Cómo conectarse a un proveedor de identidades externo

Existen diferentes requisitos previos, consideraciones y procedimientos de aprovisionamiento para el dispositivo externo compatible. IdPs Hay step-by-step tutoriales disponibles para varios: IdPs

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping Identity](#)

Para obtener más información sobre las consideraciones externas IdPs que admite IAM Identity Center, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

En el siguiente procedimiento se proporciona una descripción general del procedimiento que se utiliza con todos los proveedores de identidades externos.

## Cómo conectarse a un proveedor de identidades externo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.



3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:
  - a. En Metadatos del proveedor de servicios, seleccione Descargar archivo de metadatos para descargar el archivo de metadatos y guardarlo en el sistema. El proveedor de identidades externo necesita el archivo de metadatos SAML de IAM Identity Center.

 Note

El archivo de metadatos de SAML que descargue contiene el servicio de consumo de aserciones IPv4 (ACS) de pila única y doble. URLs Además, si su centro de identidad de IAM está replicado en otras regiones, el archivo de metadatos contiene el ACS de cada región adicional. URLs Si su IdP externo tiene un límite en la cantidad de ACS URLs, tendrá que eliminar el ACS innecesario. URLs Por ejemplo, si su organización ha adoptado por completo los terminales de doble pila y ya no utiliza los terminales IPv4 exclusivos, puede eliminar estos últimos. Un enfoque alternativo es no utilizar el archivo de metadatos, sino copiar y pegar el ACS URLs en el IdP externo.

- b. En Metadatos del proveedor de identidad, elija Elegir archivo y busque el archivo de metadatos que descargó de su proveedor de identidades externo. A continuación, cargue el archivo. Este archivo de metadatos contiene el certificado x509 público necesario que se utiliza para confiar en los mensajes que se envían desde el IdP.
  - c. Elija Siguiente.

 Important

Al cambiar la fuente a o desde Active Directory, se eliminan todas las asignaciones de usuarios y grupos existentes. Debe volver a aplicar las asignaciones manualmente una vez que haya cambiado correctamente la fuente.

6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.

7. Elija Cambiar fuente de identidad. Un mensaje de estado le informa de que ha cambiado correctamente el origen de identidad.

## Cómo cambiar los metadatos de un proveedor de identidades externo en IAM·Identity·Center

Puede cambiar los metadatos de su proveedor de identidades externo que proporcionó con anterioridad a IAM·Identity·Center. Estos cambios afectan a la capacidad de los usuarios para iniciar sesión y acceder a los AWS recursos a través del Centro de identidad de IAM. El siguiente procedimiento describe cómo actualizar los metadatos del IdP externo que están almacenados en IAM·Identity·Center. Para completar este procedimiento, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Cómo eliminar los metadatos de un proveedor de identidades externo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Origen de la identidad. Elija Acciones y luego Administrar autenticación.
4. En la sección Metadatos del proveedor de identidad, seleccione Editar metadatos del IdP. Puede realizar los cambios en la URL de inicio de sesión del IdP o en la URL del emisor del IdP para su IdP externo en esta página. Seleccione Guardar cambios cuando haya realizado todos los cambios necesarios.

## Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos

IAM Identity Center implementa los siguientes protocolos basados en estándares para la federación de identidades:

- SAML 2.0 para la autenticación de usuarios
- SCIM para el aprovisionamiento

Se espera que cualquier proveedor de identidades (IdP) que implemente estos protocolos estándar interactúe correctamente con IAM Identity Center, teniendo en cuenta las siguientes consideraciones especiales:

- SAML

- IAM Identity Center requiere un formato de identificador de nombre SAML para la dirección de correo electrónico (es decir, `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`).
- [El valor del campo NameID en las aserciones debe ser una cadena \(/rfc2822\) que cumpla con las especificaciones addr-spec \(«»\) \(https://tools.ietf.org/html/rfc2822 #section -3.4.1\). name@domain.com https://tools.ietf.org/html](https://tools.ietf.org/html/rfc2822)
- El archivo de metadatos no puede tener más de 75 000 caracteres.
- Los metadatos deben contener un ID de entidad, un certificado X509 y formar parte de la URL de inicio de sesión. SingleSignOnService
- No se admite el cifrado SSE-KMS.
- El Centro de identidades de IAM no admite la firma de las solicitudes de autenticación SAML que envía a fuentes externas. IdPs
- El IdP debe ser compatible con el servicio al consumidor de múltiples afirmaciones (ACS) URLs si planea replicar el centro de identidad de IAM en otras regiones y aprovechar al máximo las ventajas de un centro de identidad de IAM multirregional. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#). El uso de una única URL de ACS puede afectar a la experiencia del usuario en otras regiones. Su región principal seguirá funcionando con normalidad. Para obtener más información sobre la experiencia del usuario en otras regiones con una única URL de ACS, consulte [the section called “Uso de aplicaciones AWS gestionadas sin varios ACS URLs”](#) y [the section called “Cuenta de AWS resiliencia de acceso sin varios ACS URLs”](#).

- SCIM

- [La implementación del SCIM del IAM Identity Center se basa en los SCIM RFCs 7642 \(https://tools.ietf.org/html/rfc7642\), 7643 \(/rfc7643\) y 7644 \(https://tools.ietf.org/html/rfc7644\) y en los requisitos de interoperabilidad establecidos en el borrador de marzo de https://tools.ietf.org/html2020 del Perfil SCIM básico 1.0 \(#rfc .section.4\). FastFed https://openid.net/specs/fastfed-scim-1\\_0-02.html](https://tools.ietf.org/html/rfc7642) Las diferencias entre estos documentos y la implementación actual en IAM Identity Center se describen en la sección [Operaciones de API compatibles](#) de la Guía para desarrolladores de implementación del SCIM de IAM Identity Center.

IdPs no se admiten aquellos que no se ajusten a los estándares y consideraciones mencionados anteriormente. Póngase en contacto con su IdP si cualquier pregunta o necesita más información sobre la conformidad de sus productos con estas normas y consideraciones.

Si tiene problemas para conectar su IdP al IAM Identity Center, compruebe lo siguiente:

- AWS CloudTrail se registra filtrando por el nombre del evento ExternalIdPDirectoryIniciar sesión
- Registros específicos de IdP: registros and/or de depuración
- [Resolución de problemas de IAM Identity Center](#)

#### Note

Algunos IdPs, como los del [Tutoriales de orígenes de identidad de IAM Identity Center](#), ofrecen una experiencia de configuración simplificada para el IAM Identity Center en forma de «aplicación» o «conector» creado específicamente para el IAM Identity Center. Si su IdP ofrece esta opción, le recomendamos que la utilice, teniendo cuidado al elegir el elemento creado específicamente para IAM Identity Center. Otros elementos denominados «AWS», «AWS federación» o nombres genéricos similares de «»AWS pueden utilizar otros enfoques de federación y es posible and/or que no funcionen como se esperaba con el IAM Identity Center.

## Perfil SCIM e implementación de SAML 2.0

Tanto SCIM como SAML son consideraciones importantes a la hora de configurar IAM Identity Center.

### Implementación de SAML 2.0

IAM Identity Center admite la federación de identidades con [lenguaje de marcado para confirmaciones de seguridad SAML 2.0](#). Esto permite al Centro de Identidad de IAM autenticar las identidades de proveedores de identidad externos (). IdPs SAML 2.0 es un estándar abierto que se utiliza para intercambiar aserciones de SAML de forma segura. SAML 2.0 transfiere información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML (denominado proveedor de servicios o SP). El servicio de IAM Identity Center utiliza esta información para proporcionar un inicio de sesión único federado. El inicio de sesión único permite a los usuarios acceder a las aplicaciones Cuentas de AWS y configurarlas en función de sus credenciales de proveedor de identidad existentes.

El Centro de identidad de IAM añade las capacidades de IdP de SAML a su almacén del Centro de identidades de IAM o a un proveedor AWS Managed Microsoft AD de identidad externo. A continuación, los usuarios pueden iniciar sesión de forma única en los servicios compatibles con SAML, incluidas las aplicaciones Consola de administración de AWS y las de terceros, como, y. Microsoft 365 Concur Salesforce

Sin embargo, el protocolo SAML no proporciona ninguna forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

## Perfil SCIM

IAM Identity Center es compatible con el estándar Sistema de la administración de identidades entre dominios (SCIM) v2.0. El SCIM mantiene las identidades de su IAM Identity Center sincronizadas con las identidades de su IdP. Esto incluye cualquier aprovisionamiento, actualización y desaprovisionamiento de usuarios entre su IdP y IAM Identity Center.

Para obtener más información acerca de cómo implementar una capa personalizada, consulte [Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM](#). Para obtener más información sobre la implementación del SCIM de IAM Identity Center, consulte la [Guía para desarrolladores de implementación de IAM Identity Center SCIM](#).

## Temas

- [Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM](#)
- [Rotar certificados SAML 2.0](#)

## Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos de su proveedor de identidades (IdP) a IAM Identity Center mediante el protocolo Sistema de administración de identidades entre dominios (SCIM) v2.0. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario del proveedor de identidades (IdP) con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y su IdP. Esta conexión se configura en el IdP mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center.

## Temas

- [Consideraciones para utilizar el aprovisionamiento automático](#)

- [Cómo monitorizar la caducidad del token de acceso](#)
- [Generar un token de acceso](#)
- [Habilitar el aprovisionamiento automático](#)
- [Eliminar un token de acceso](#)
- [Deshabilitar el aprovisionamiento automático](#)
- [Rotar un token de acceso](#)
- [Auditoría y conciliación de recursos aprovisionados automáticamente](#)
- [Aprovisionamiento manual](#)

### Consideraciones para utilizar el aprovisionamiento automático

Antes de comenzar a implementar el SCIM, le recomendamos revisar primero las siguientes consideraciones importantes sobre su funcionamiento con IAM Identity Center. Para conocer otras consideraciones de aprovisionamiento, consulte los [Tutoriales de orígenes de identidad de IAM Identity Center](#) aplicables a su IdP.

- Si va a aprovisionar una dirección de correo electrónico principal, el valor de este atributo debe ser único para cada usuario. En algunos casos IdPs, es posible que la dirección de correo electrónico principal no sea una dirección de correo electrónico real. Por ejemplo, puede ser un nombre principal universal (UPN) que solo se parece a un correo electrónico. Es IdPs posible que tengan una dirección de correo electrónico secundaria o «otra» que contenga la dirección de correo electrónico real del usuario. Debe configurar SCIM en su IdP para asignar la dirección de correo electrónico única no nula al atributo de dirección de correo electrónico principal de IAM Identity Center. Además, debe asignar el identificador de inicio de sesión único no nulo del usuario al atributo de nombre de usuario de IAM Identity Center. Compruebe si su IdP tiene un valor único que sea tanto el identificador de inicio de sesión como el nombre de correo electrónico del usuario. Si es así, puede asignar ese campo de IdP al correo electrónico principal de IAM Identity Center y al nombre de usuario de IAM Identity Center.
- Para que la sincronización de SCIM funcione, cada usuario debe tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización. Si falta alguno de estos valores en un usuario, este no se aprovisionará.
- Si necesita utilizar aplicaciones de terceros, primero tendrá que asignar el atributo de asunto de SAML saliente al atributo de nombre de usuario. Si la aplicación de terceros necesita una dirección de correo electrónico enrutable, debe proporcionar el atributo de correo electrónico a su IdP.

- El proveedor de identidades controla los intervalos de aprovisionamiento y actualización de SCIM. Los cambios en los usuarios y grupos de su proveedor de identidades solo se reflejan en IAM Identity Center después de que su proveedor de identidades los envíe a IAM Identity Center. Consulte con su proveedor de identidades para obtener más información sobre la frecuencia de las actualizaciones de usuarios y grupos.
- Actualmente, SCIM no proporciona atributos con varios valores (como varios correos electrónicos o números de teléfono para un usuario determinado). Los intentos de sincronizar atributos con varios valores en IAM Identity Center con SCIM fallarán. Para evitar errores, asegúrese de que solo se pase un valor único para cada atributo. Si tiene usuarios con atributos de varios valores, elimine o modifique las asignaciones de atributos duplicadas en SCIM en su IdP para la conexión con IAM Identity Center.
- Compruebe que el mapeo SCIM de `externalId` en su IdP corresponde a un valor que sea único, que esté siempre presente y que tenga menos probabilidades de cambiar para sus usuarios. Por ejemplo, su IdP puede proporcionar un `objectId` garantizado u otro tipo de identificador que no se vea afectado por los cambios en los atributos del usuario, como el nombre y el correo electrónico. Si es así, puede asignar ese valor al campo `externalId` de SCIM. Esto garantiza que tus usuarios no pierdan sus AWS derechos, asignaciones o permisos si necesitas cambiarles el nombre o el correo electrónico.
- Usuarios que aún no se han asignado a una aplicación o que no se Cuenta de AWS pueden aprovisionar en el Centro de identidades de IAM. Para sincronizar usuarios y grupos, asegúrese de que estén asignados a la aplicación u otra configuración que represente la conexión de su IdP a IAM Identity Center.
- El comportamiento de desaprovisionamiento de los usuarios lo administra el proveedor de identidades y puede variar según su implementación. Consulte con su proveedor de identidades para obtener más información sobre el desaprovisionamiento de usuarios.
- Tras configurar el aprovisionamiento automático con SCIM para su IdP, ya no podrá añadir ni editar usuarios en la consola de IAM Identity Center. Si necesita agregar o modificar un usuario, debe hacerlo desde su IdP externo u origen de identidad.

Para obtener más información sobre la implementación de SCIM de IAM Identity Center, consulte la [guía para desarrolladores de implementación de IAM Identity Center SCIM](#).

## Cómo monitorizar la caducidad del token de acceso

Los tokens de acceso SCIM se generan con una validez de un año. Cuando tu token de acceso SCIM caduque en 90 días o menos, te AWS envía recordatorios a la consola del IAM Identity

Center y al AWS Health panel de control para ayudarte a cambiar el token. Al rotar el token de acceso de SCIM antes de que caduque, asegura de forma continua el aprovisionamiento automático de la información de usuarios y grupos. Si el token de acceso SCIM caduca, se interrumpe la sincronización de la información de usuarios y grupos de su proveedor de identidades con IAM Identity Center, por lo que el aprovisionamiento automático ya no puede realizar actualizaciones ni crear y eliminar información. La interrupción del aprovisionamiento automático puede aumentar los riesgos de seguridad y afectar al acceso a sus servicios.

Los recordatorios de la consola de Identity Center persisten hasta que rote el token de acceso SCIM y elimine los tokens de acceso no utilizados o vencidos. Los eventos del AWS Health panel de control se renuevan semanalmente entre 90 y 60 días, dos veces por semana entre 60 y 30 días, tres veces por semana entre 30 y 15 días y todos los días desde 15 días hasta que caduquen los tokens de acceso del SCIM.

### Generar un token de acceso

Siga el siguiente procedimiento para generar un nuevo token de acceso en la consola de IAM Identity Center.

#### Note

Este procedimiento requiere que haya habilitado previamente el aprovisionamiento automático. Para obtener más información, consulte [Habilitar el aprovisionamiento automático](#).

### Cómo generar un nuevo token de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione Generar token.
4. En el cuadro de diálogo Generar un nuevo token de acceso, copie el nuevo token de acceso y guárdelo en un lugar seguro.
5. Seleccione Cerrar.



## Habilitar el aprovisionamiento automático

Siga el siguiente procedimiento para habilitar el aprovisionamiento automático de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo SCIM.

### Note

Antes de comenzar con este procedimiento, le recomendamos que revise primero las consideraciones de aprovisionamiento aplicables a su IdP. Para obtener más información, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#) de su IdP.

### Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo Aprovisionamiento automático de entrada, copie el punto de conexión de SCIM y el token de acceso. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-55555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Después de completar este procedimiento, debe configurar el aprovisionamiento automático en su IdP. Para obtener más información, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#) de su IdP.

## Eliminar un token de acceso

Siga el procedimiento que se detalla a continuación para eliminar un token de acceso actual de la consola de IAM Identity Center.

### Cómo eliminar una clave de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione el token de acceso que desee eliminar y, a continuación, Eliminar.
4. En el cuadro de diálogo Eliminar el token de acceso, revise la información, escriba ELIMINAR y, a continuación, elija Eliminar el token de acceso.

## Deshabilitar el aprovisionamiento automático

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

### Important

Debe eliminar el token de acceso antes de iniciar este procedimiento. Para obtener más información, consulte [Eliminar un token de acceso](#).

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar el aprovisionamiento.

3. En la página de aprovisionamiento automático, seleccione Deshabilitar.
4. En el cuadro de diálogo Desactivar el aprovisionamiento automático, revise la información, escriba DISABLE y, a continuación, elija Deshabilitar el aprovisionamiento automático.

## Rotar un token de acceso

Un directorio de IAM Identity Center admite hasta 2 tokens de acceso a la vez. Para generar un token de acceso adicional antes de cualquier rotación, elimine los tokens de acceso caducados o no utilizados.

Si su token de acceso SCIM está a punto de caducar, puede seguir el procedimiento que se describe a continuación para rotar un token de acceso existente en la consola de IAM Identity Center.

## Cómo eliminar un token de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, anote el ID del token que desee rotar.
4. Siga los pasos que encontrará en [Generar un token de acceso](#) para crear un nuevo token. Si ya ha creado el número máximo de tokens de acceso a SCIM, primero tendrá que eliminar uno de los tokens actuales.
5. Vaya al sitio web de su proveedor de identidades y configure el nuevo token de acceso para el aprovisionamiento de SCIM y, a continuación, pruebe la conectividad con IAM Identity Center con el nuevo token de acceso de SCIM. Una vez que haya confirmado que el aprovisionamiento funciona correctamente con el nuevo token, continúe con el siguiente paso de este procedimiento.
6. Siga los pasos que se indican en [Eliminar un token de acceso](#) para eliminar el token de acceso que anotó anteriormente. También puede usar la fecha de creación del token como una pista sobre qué token eliminar.

## Auditoría y conciliación de recursos aprovisionados automáticamente

SCIM le permite aprovisionar usuarios, grupos y membresías grupales de forma automática desde su origen de identidad a IAM Identity Center. Esta guía le ayuda a verificar y conciliar estos recursos para mantener una sincronización precisa.

### ¿Por qué auditar sus recursos?

Las auditorías periódicas ayudan a garantizar que sus controles de acceso sigan siendo precisos y que su proveedor de identidades (IdP) permanezca correctamente sincronizado con IAM Identity Center. Esto es particularmente importante para el cumplimiento de las normas de seguridad y la administración de los accesos.

Recursos que se pueden auditar:

- Users
- Groups
- Membresías grupales

Puede usar [comandos CLI APIs](#) de AWS Identity Store para realizar la auditoría y la reconciliación. En los ejemplos siguientes se utilizan comandos de AWS CLI . Para obtener información sobre las alternativas de API, consulte [las operaciones correspondientes](#) en la referencia de Identity Store API.

### ¿Cómo auditar los recursos?

A continuación, se muestran ejemplos de cómo auditar estos recursos mediante AWS CLI comandos.

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Acceso de administrador a IAM Identity Center.
- AWS CLI instalado y configurado. Para obtener más información, consulte la [Guía del usuario de la interfaz de línea de comandos de AWS](#) .
- Permisos de IAM necesarios para los comandos del almacén de identidades.

### Paso 1: enumeración de los recursos actuales

Puede ver sus recursos actuales mediante AWS CLI.

 Note

Al utilizar el AWS CLI, la paginación se gestiona automáticamente a menos que lo especifique `--no-paginate`. Si llama a la API directamente (por ejemplo, con un SDK o un script personalizado), gestione `NextToken` en la respuesta. Esto garantiza que recupere todos los resultados en varias páginas.

## Example para usuarios

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

## Example para grupos

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

## Example para membresías grupales

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

## Paso 2: comparar con su origen de identidad

Compare los recursos de la lista con su origen de identidad para identificar cualquier discrepancia, como las siguientes:

- Falta de recursos que deberían aprovisionarse en IAM Identity Center.
- Recursos adicionales que deberían eliminarse de IAM Identity Center.

## Example para usuarios

```
# Create missing users
```

```
aws identitystore create-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-name USERNAME \  
  --display-name DISPLAY_NAME \  
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \  
  --emails Value=EMAIL,Primary=true  
  
# Delete extra users  
aws identitystore delete-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-id USER_ID
```

## Example para grupos

```
# Create missing groups  
aws identitystore create-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  [group attributes]  
  
# Delete extra groups  
aws identitystore delete-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

## Example para membresías grupales

```
# Add missing members  
aws identitystore create-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID \  
  --member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --membership-id MEMBERSHIP_ID
```

## Consideraciones

- Los comandos están sujetos a las [cuotas de servicio y a la limitación de las API](#).
- Si encuentra muchas diferencias durante la reconciliación, realice cambios pequeños y graduales en AWS Identity Store. Esto le ayuda a evitar errores que afecten a varios usuarios.

- La sincronización con SCIM puede anular los cambios manuales. Compruebe la configuración de su IdP para comprender este comportamiento.

## Aprovisionamiento manual

Algunos IdPs no son compatibles con el Sistema de Gestión de Identidad entre Dominios (SCIM) o tienen una implementación de SCIM incompatible. En esos casos, puede aprovisionar usuarios manualmente a través de la consola de IAM Identity Center. Cuando añada usuarios a IAM Identity Center, asegúrese de configurar el nombre de usuario para que sea idéntico al nombre de usuario que tiene en su IdP. Como mínimo, debe tener una dirección de correo electrónico y un nombre de usuario únicos. Para obtener más información, consulte [Exclusividad del nombre de usuario y de la dirección de correo electrónico](#).

También debe gestionar todos los grupos manualmente en IAM Identity Center. Para ello, debe crear los grupos y añadirlos mediante la consola de IAM Identity Center. No es necesario que estos grupos coincidan con los que existen en su IdP. Para obtener más información, consulte [Groups](#).

## Rotar certificados SAML 2.0

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y su proveedor de identidades (IdP) externo. Al añadir un IdP externo a IAM Identity Center, también debe obtener al menos un certificado SAML 2.0 X.509 público del IdP externo. Por lo general, ese certificado se instala automáticamente durante el intercambio de metadatos SAML del IdP durante la creación de relaciones de confianza.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

## Temas

- [Rotar un certificado SAML 2.0](#)
- [Indicadores de estado de caducidad de certificados](#)

## Rotar un certificado SAML 2.0

Es posible que tenga que importar certificados periódicamente para rotar los certificados no válidos o vencidos emitidos por su proveedor de identidades. Esto ayuda a evitar la interrupción

de la autenticación o el tiempo de inactividad. Todos los certificados importados se activan automáticamente. Los certificados solo se deben eliminar después de asegurarse de que ya no se utilizan con el proveedor de identidades asociado.

También debe tener en cuenta que es IdPs posible que algunos no admitan varios certificados. En este caso, el hecho de rotar los certificados con ellos IdPs podría suponer una interrupción temporal del servicio para los usuarios. El servicio se restablece cuando la confianza con ese IdP se ha restablecido correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

 Note

Como práctica recomendada de seguridad, ante cualquier indicio de que un certificado SAML existente está en peligro o se está usando de forma incorrecta, debe retirarlo inmediatamente y cambiarlo.

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Obtención de un nuevo certificado del IdP
- Importación del nuevo certificado a IAM Identity Center
- Activación del nuevo certificado en el IdP
- Eliminación del certificado anterior

Siga todos los procedimientos que se detallan a continuación para completar el proceso de rotación del certificado y, al mismo tiempo, evitar cualquier tiempo de inactividad de la autenticación.

#### Paso 1: obtención de un nuevo certificado del IdP

Vaya al sitio web del IdP y descargue su certificado SAML 2.0. Asegúrese de que el archivo del certificado se descargue en formato codificado PEM. La mayoría de los proveedores le permiten crear varios certificados SAML 2.0 en el IdP. Es probable que se marquen como deshabilitados o inactivos.

#### Paso 2: importación del nuevo certificado a IAM Identity Center

Siga el procedimiento que se detalla a continuación para importar el nuevo certificado mediante la consola de IAM Identity Center.



1. En la [consola de IAM Identity Center](#), elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar certificados SAML 2.0, seleccione Importar certificado.
4. En el cuadro de diálogo Importar certificado SAML 2.0, seleccione Elegir archivo, navegue hasta el archivo de certificado, selecciónelo y, a continuación, elija Importar certificado.

En este punto, IAM Identity Center confiará en todos los mensajes SAML entrantes firmados desde los 2 certificados que haya importado.

### Paso 3: activación del nuevo certificado en el IdP

Regrese al sitio web del IdP y marque el nuevo certificado que creó anteriormente como principal o activo. En este punto, todos los mensajes SAML firmados por el IdP deberían usar el nuevo certificado.

### Paso 4: eliminación del certificado anterior

Siga el procedimiento que se detalla para completar el proceso de rotación de certificados para su IdP. Siempre debe haber al menos un certificado válido en la lista y no se puede eliminar.

#### Note

Asegúrese de que su proveedor de identidades ya no firme las respuestas de SAML con este certificado antes de eliminarlo.

1. En la página Administrar certificados SAML 2.0, seleccione el certificado que desea eliminar. Elija Eliminar.
2. En el cuadro de diálogo Eliminar el certificado SAML 2.0, escriba **DELETE** para confirmarlo y, a continuación, elija Eliminar.
3. Regrese al sitio web del IdP y lleve a cabo los pasos necesarios para eliminar el certificado inactivo anterior.

## Indicadores de estado de caducidad de certificados

La página Administrar certificados SAML 2.0 muestra iconos indicadores de estado en colores en la columna Fecha de caducidad situada junto a cada certificado de la lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido y seguirá siendo válido durante al menos 90 días más.

Cómo comprobar el estado de la renovación de un certificado:

1. En la [consola de IAM Identity Center](#), elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar la autenticación de SAML 2.0, en Administrar certificados de SAML 2.0, consulte el estado de los certificados de la lista tal y como se indica en la columna Caduca el.

## Directorio Microsoft AD

Con AWS IAM Identity Center, puede conectar un directorio autoadministrado en Active Directory (AD) o un directorio AWS Managed Microsoft AD mediante AWS Directory Service. Este directorio de Microsoft AD define el grupo de identidades que los administradores pueden extraer al utilizar la consola de Centro de identidades de IAM para asignar el acceso de inicio de sesión único. Tras conectar el directorio corporativo al Centro de identidades de IAM, puede conceder a sus usuarios o grupos de AD acceso a las aplicaciones o a Cuentas de AWS ambas opciones.

AWS Directory Service le ayuda a configurar y ejecutar un AWS Managed Microsoft AD directorio independiente alojado en la Nube de AWS. También puede utilizarlo Directory Service para conectar sus AWS recursos con un AD autogestionado existente. Para configurarlo AWS Directory Service para que funcione con su AD autogestionado, primero debe configurar relaciones de confianza para extender la autenticación a la nube.

El centro de identidad de IAM utiliza la conexión proporcionada por Directory Service para realizar la autenticación de transferencia a la instancia de AD de origen. Si la utilizas AWS Managed Microsoft AD como fuente de identidad, el Centro de Identidad de IAM puede funcionar con usuarios de AWS Managed Microsoft AD cualquier dominio conectado a través de un fideicomiso de AD. Si desea

ubicar a sus usuarios en 4 o más dominios, los usuarios deben usar la sintaxis de DOMAIN\user como nombre de usuario al iniciar sesión en Centro de identidades de IAM.

#### Notas

- Como paso previo, asegúrese de que su AD Connector o directorio en AWS Managed Microsoft AD in Directory Service reside en su cuenta AWS Organizations de administración.
- Centro de identidades de IAM no admite Simple AD basado en SAMBA 4 como directorio conectado.
- El centro de identidad de IAM no puede sincronizar los principios de seguridad extranjeros (). FSPs Si un grupo AWS Managed Microsoft AD contiene miembros de un dominio de confianza FSPs, esos miembros no se sincronizarán.

Para ver una demostración del proceso de uso de Active Directory como origen de identidad para IAM Identity Center, consulte el siguiente vídeo de YouTube:

[Uso de Active Directory como fuente de identidad para AWS IAM Identity Center | Amazon Web Services](#)

## Consideraciones sobre el uso de Active Directory

Si quiere utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si lo está utilizando AWS Managed Microsoft AD, debe habilitar el Centro de Identidad de IAM en el mismo Región de AWS lugar donde está configurado su AWS Managed Microsoft AD directorio. Centro de identidades de IAM almacena los datos de asignación en la misma región que el directorio. Para administrar Centro de identidades de IAM, es posible que deba cambiarse a la región en la que está configurado Centro de identidades de IAM. Además, tenga en cuenta que el portal de AWS acceso utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

Debe tener un AD Connector o AWS Managed Microsoft AD directorio existente configurado y debe residir en AWS Directory Service su cuenta AWS Organizations de administración. Solo puede conectar un directorio AD Connector o un directorio AWS Managed Microsoft AD a la vez. Si

necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte lo siguiente:

- [Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- Utilice un Active Directory que resida en la cuenta de administrador delegada:

Si planea habilitar la administración delegada del IAM Identity Center y usar Active Directory como fuente de identidad del IAM Identity Center, puede usar un AD Connector existente o un AWS Managed Microsoft AD directorio configurado en el AWS Directorio que resida en la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de Centro de identidades de IAM de cualquier otra fuente a Active Directory o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir (ser propiedad de) la cuenta de miembro administrador delegado de Centro de identidades de IAM si existe; de lo contrario, debe estar en la cuenta de administración.

## Conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio a IAM Identity Center.

Puede conectar un AWS Managed Microsoft AD directorio o un directorio autogestionado en Active Directory con IAM Identity Center.

### Note

El Centro de Identidad de IAM no SAMBA4 admite Simple AD como fuente de identidad.

## AWS Managed Microsoft AD

1. Revise la guía en [Directorio Microsoft AD](#).
2. Siga los pasos de [Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Directorio autogestionado en Active Directory

1. Revise la guía en [Directorio Microsoft AD](#).
2. Siga los pasos de [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## IdP externo

1. Revise la guía en [Proveedores de identidades externos](#).
2. Siga los pasos de [Cómo conectarse a un proveedor de identidades externo](#).
3. Configure su IdP para aprovisionar usuarios al Centro de identidades de IAM.

### Note

Antes de configurar el aprovisionamiento automático y basado en grupos de todas las identidades de sus empleados desde su IdP al Centro de identidades de IAM, le recomendamos que sincronice el único usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM.

## Sincronice un usuario administrativo en el Centro de identidades de IAM

Tras conectar el directorio a IAM Identity Center, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con IAM Identity Center.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.

6. En Usuarios y grupos añadidos, haga lo siguiente:
  - a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
  - b. Seleccione la casilla de verificación que hay junto al nombre del archivo.
  - c. Elija Enviar
7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar el usuario a ese conjunto de permisos. Para obtener más información, consulte [Crea un conjunto de permisos](#).

## Aprovisionamiento cuando los usuarios provienen de Active Directory

El Centro de identidades de IAM utiliza la conexión proporcionada por el Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades del Centro de identidades de IAM. La información de la contraseña no se sincroniza con Centro de identidades de IAM, ya que la autenticación de los usuarios se realiza directamente desde el directorio de origen de Active Directory. Las aplicaciones utilizan estos datos de identidad para facilitar los escenarios de búsqueda, autorización y colaboración dentro de la aplicación sin devolver la actividad de LDAP al directorio de origen de Active Directory.

Para obtener más información sobre aprovisionamiento, consulte [Aprovisionamiento de usuarios y grupos](#).

### Temas

- [Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos](#)
- [Centro de identidades de IAM y sincronización de AD configurable](#)

## Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM

Utilice el siguiente procedimiento para conectar un directorio gestionado por AWS Directory Service al AWS Managed Microsoft AD Centro de Identidad de IAM.

Para conectarse AWS Managed Microsoft AD al Centro de Identidad de IAM

1. Abra la [consola de IAM Identity Center](#).

### Note

Antes de continuar con el paso siguiente, compruebe que la consola de Centro de identidades de IAM utiliza alguna de las regiones donde se encuentra su directorio de AWS Managed Microsoft AD .

2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir origen de identidad, seleccione Active Directory y, a continuación, seleccione Siguiente.
5. En Conectar Active Directory, elija un directorio AWS Managed Microsoft AD de la lista y, a continuación, Siguiente.
6. En Confirmar el cambio, revise la información; cuando esté todo listo, escriba ACEPTAR y, a continuación, elija Cambiar fuente de identidad.

### Important

Para especificar un usuario de Active Directory como usuario administrativo en Centro de identidades de IAM, primero debe sincronizar el usuario al que desea conceder permisos administrativos desde Active Directory con Centro de identidades de IAM. Para ello, siga los pasos que se indican en [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM

Los usuarios del directorio autogestionado de Active Directory (AD) también pueden tener acceso mediante un inicio de sesión único Cuentas de AWS y a las aplicaciones del portal de acceso. AWS Para configurar el acceso de inicio de sesión único para estos usuarios, puede realizar una de las siguientes acciones:

- Cree una relación de confianza bidireccional: cuando se crean relaciones de confianza bidireccionales entre un directorio autogestionado de AD AWS Managed Microsoft AD y un directorio autogestionado de AD, los usuarios del directorio autogestionado de AD pueden iniciar sesión con sus credenciales corporativas en diversos servicios y aplicaciones empresariales. AWS Las relaciones de confianza unidireccionales no funcionan con Centro de identidades de IAM.

AWS IAM Identity Center requiere una confianza bidireccional para tener permisos para leer la información de usuarios y grupos de tu dominio a fin de sincronizar los metadatos de usuarios y grupos. Centro de identidades de IAM utiliza estos metadatos al asignar el acceso a conjuntos de permisos o aplicaciones. Las aplicaciones también utilizan los metadatos de usuarios y grupos para colaborar como, por ejemplo, cuando se comparte un panel con otro usuario o grupo. La confianza Directory Service de Microsoft Active Directory en su dominio permite que IAM Identity Center confíe en su dominio para la autenticación. La confianza en la dirección opuesta otorga AWS permisos para leer los metadatos de los usuarios y grupos.

Para obtener más información acerca de la configuración de una relación de confianza bidireccional, consulte [Cuándo crear una relación de confianza](#) en la Guía de administración de AWS Directory Service .

### Note

Para poder utilizar AWS aplicaciones, como el IAM Identity Center, para leer los usuarios del Directory Service directorio de dominios de confianza, las Directory Service cuentas requieren permisos sobre el userAccountControl atributo de los usuarios de confianza. Sin permisos de lectura para este atributo, las aplicaciones de AWS no pueden determinar si la cuenta está habilitada o deshabilitada.

El acceso de lectura a este atributo se proporciona de forma predeterminada cuando se crea una confianza. Si deniega el acceso a este atributo (no se recomienda), impedirá que aplicaciones como Identity Center puedan leer a los usuarios de confianza. La solución



consiste en permitir específicamente el acceso de lectura al `userAccountControl` atributo de las cuentas de AWS servicio de la OU AWS reservada (con el prefijo `AWS_`).

- Crear un conector AD: Un conector AD es una puerta de enlace de directorio que puede redirigir solicitudes del directorio al Active Directory autoadministrado sin almacenar en caché la información que hay en la nube. Para obtener más información, consulte [Conectarse a un directorio](#) en la Guía de administración de AWS Directory Service . A continuación, se presentan las consideraciones a tener en cuenta al usar el Conector AD:
  - Si va a conectar Centro de identidades de IAM a un directorio de un conector AD, cualquier restablecimiento de contraseñas de usuario en el futuro deberá realizarse desde AD. Esto significa que los usuarios no podrán restablecer sus contraseñas desde el portal de AWS acceso.
  - Si utiliza un conector AD para conectar el servicio de dominio de Active Directory al Centro de identidades de IAM, Centro de identidades de IAM solo tiene acceso a los usuarios y grupos del dominio único al que se conecta el conector AD. Si necesita admitir varios dominios o bosques, utilice Directory Service para Microsoft Active Directory.

 Note

El Centro de identidades de IAM no funciona con directorios Simple AD SAMBA4 basados en.

## Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos

Las asignaciones de atributos se utilizan para asignar los tipos de atributos que existen en Centro de identidades de IAM con atributos similares en sus fuentes de identidad externas, como Google Workspace, Microsoft Active Directory (AD) y Okta. Centro de identidades de IAM recupera los atributos de usuario de la fuente de identidad y los asigna a los atributos de usuario de Centro de identidades de IAM.

Si su IAM Identity Center está sincronizado para usar un proveedor de identidades (IdP) externo, por ejemplo, Google Workspace, Okta o Ping, como origen de identidad, tendrá que asignar sus atributos en su IdP.

IAM Identity Center rellena previamente un conjunto de atributos en la pestaña Asignaciones de atributos de la página de configuración. Centro de identidades de IAM utiliza estos atributos

de usuario para rellenar las aserciones de SAML (como atributos de SAML) que se envían a la aplicación. Estos atributos de usuario se recuperan, a su vez, de su fuente de identidad. Cada aplicación determina la lista de atributos de SAML 2.0 que necesita para un inicio de sesión único correcto. Para obtener más información, consulte [Asignación de atributos de su aplicación con atributos de IAM Identity Center](#).

IAM Identity Center también administra un conjunto de atributos en la sección Asignaciones de atributos de la página de configuración de Active Directory si utiliza AD como origen de identidad. Para obtener más información, consulte [Asignación de los atributos de usuario entre IAM Identity Center y el directorio Microsoft AD](#).

### Atributos de proveedores de identidad externos compatibles

En la siguiente tabla se enumeran todos los atributos del proveedor de identidades (IdP) externo que se admiten y se pueden asignar a los atributos que se pueden utilizar al configurar [Atributos para controlar el acceso](#) en IAM Identity Center. Al usar aserciones de SAML, puede usar cualquier atributo que admita su IdP.

#### Atributos compatibles en su IdP

```
${path:userName}
```

```
${path:name.familyName}
```

```
${path:name.givenName}
```

```
${path:displayName}
```

```
${path:nickName}
```

```
${path:emails[primary eq true].value}
```

```
${path:addresses[type eq "work"].streetAddress}
```

```
${path:addresses[type eq "work"].locality}
```

```
${path:addresses[type eq "work"].region}
```

```
${path:addresses[type eq "work"].postalCode}
```

```
${path:addresses[type eq "work"].country}
```

## Atributos compatibles en su IdP

`${path:addresses[type eq "work"].formatted}``${path:phoneNumbers[type eq "work"].value}``${path:userType}``${path:title}``${path:locale}``${path:timezone}``${path:enterprise.employeeNumber}``${path:enterprise.costCenter}``${path:enterprise.organization}``${path:enterprise.division}``${path:enterprise.department}``${path:enterprise.manager.value}`

## Asignaciones predeterminadas entre IAM Identity Center y Microsoft AD

En la tabla siguiente se muestran las asignaciones predeterminadas de los atributos de usuario de Centro de identidades de IAM a los atributos de usuario del directorio Microsoft AD. Centro de identidades de IAM solo admite la lista de atributos de la columna Atributo de usuario en Centro de identidades de IAM.

| Atributo de usuario en Centro de identidades de IAM | Asignaciones a este atributo en su Active Directory |
|-----------------------------------------------------|-----------------------------------------------------|
| displayname                                         | <code>\${displayname}</code>                        |
| emails[?primary].value *                            | <code>\${mail}</code>                               |

| Atributo de usuario en Centro de identidades de IAM | Asignaciones a este atributo en su Active Directory |
|-----------------------------------------------------|-----------------------------------------------------|
| externalid                                          | \${objectguid}                                      |
| name.givenname                                      | \${givenname}                                       |
| name.familyname                                     | \${sn}                                              |
| name.middlename                                     | \${initials}                                        |
| sid                                                 | \${objectsid}                                       |
| username                                            | \${userprincipalname}                               |

\* El atributo de correo electrónico de Centro de identidades de IAM debe ser único en el directorio.

| Atributo de usuario en IAM Identity Center | Asignaciones a este atributo en su Active Directory |
|--------------------------------------------|-----------------------------------------------------|
| externalid                                 | \${objectguid}                                      |
| description                                | \${description}                                     |
| displayname                                | \${samaccountname}@{associateddomain}               |

## Consideraciones

- Si no tiene ninguna asignación para sus usuarios y grupos en IAM Identity Center cuando habilite la sincronización de AD configurable, se utilizan las asignaciones predeterminadas en las tablas anteriores. Para obtener información acerca de cómo personalizar estas asignaciones, consulte [Configuración de las asignaciones de atributos para su sincronización](#).
- Algunos atributos de IAM Identity Center no se pueden modificar porque son inmutables y se asignan de forma predeterminada a atributos de directorio específicos de Microsoft AD.

Por ejemplo, el “nombre de usuario” es un atributo obligatorio en el IAM Identity Center. Si asigna “nombre de usuario” a un atributo del directorio de AD con un valor vacío, el IAM Identity Center

considerará el valor `windowsUpn` como el valor predeterminado de “nombre de usuario”. Si desea cambiar la asignación de atributos de “nombre de usuario” de la asignación actual, confirme que los flujos del IAM Identity Center que dependen del “nombre de usuario” sigan funcionando según lo previsto antes de realizar el cambio.

## Atributos de Microsoft AD compatibles con IAM Identity Center

En la siguiente tabla se proporciona la lista completa de los atributos del directorio Microsoft AD admitidos y que se pueden asignar a atributos de usuario de Centro de identidades de IAM.

### Atributos admitidos en el directorio de Microsoft AD

`${samaccountname}`

`${description}`

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

`${associateddomain}`

## Consideraciones

- Puede especificar cualquier combinación de atributos del directorio de Microsoft AD compatibles para asignarlos a un único atributo de IAM Identity Center.

### Atributos de IAM Identity Center compatibles para Microsoft AD

En la siguiente tabla se proporciona la lista completa de los atributos de Centro de identidades de IAM admitidos y que se pueden asignar a atributos de usuario del directorio Microsoft AD. Posteriormente, cuando configure las asignaciones de los atributos de la aplicación podrá usar estos mismos atributos de Centro de identidades de IAM para asignarlos con los atributos reales utilizados por dicha aplicación.

#### Atributos en IAM Identity Center compatibles para Active Directory

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

### Asignación de los atributos de usuario entre IAM Identity Center y el directorio Microsoft AD

Puede utilizar el siguiente procedimiento para especificar cómo deben asignarse sus atributos de usuario de IAM Identity Center a los atributos correspondientes de su directorio de Microsoft AD.

## Cómo asignar atributos de Centro de identidades de IAM a atributos de su directorio

1. Abra la [consola de Centro de identidades de IAM](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Gestionar asignaciones de atributos para el control de acceso, busque el atributo en Centro de identidades de IAM que desea asignar y, a continuación, escriba un valor en el cuadro de texto. Por ejemplo, es posible que desee asignar el atributo de usuario **email** de Centro de identidades de IAM al atributo del directorio de Microsoft AD **`\${mail}`**.
5. Seleccione Save changes (Guardar cambios).

## Centro de identidades de IAM y sincronización de AD configurable

La sincronización con Active Directory (AD) configurable de Centro de identidades de IAM le permite configurar de forma explícita las identidades de Microsoft Active Directory que se sincronizan automáticamente en Centro de identidades de IAM y controlar el proceso de sincronización.

- Con este método de sincronización, haga lo siguiente:
  - Controle los límites de los datos definiendo explícitamente los usuarios y grupos de Microsoft Active Directory que se sincronizan automáticamente en Centro de identidades de IAM. Puede [añadir usuarios y grupos](#) o [eliminar usuarios y grupos](#) para cambiar el alcance de la sincronización en cualquier momento.
  - Asigne a los usuarios y grupos sincronizados [acceso mediante inicio de sesión único a Cuentas de AWS](#) o [acceso a las aplicaciones](#). Las aplicaciones pueden ser aplicaciones AWS administradas o aplicaciones administradas por el cliente.
  - Controle el proceso de sincronización [pausando y reanudando la sincronización](#) según sea necesario. Esto le ayuda a regular la carga de los sistemas de producción.

### Requisitos y consideraciones previos

Antes de utilizar la sincronización de AD configurable, tenga en cuenta los siguientes requisitos y consideraciones:

- Especificación de usuarios y grupos de Active Directory para la sincronización

Antes de poder utilizar el Centro de identidades de IAM para asignar a nuevos usuarios y grupos el acceso a Cuentas de AWS las aplicaciones AWS gestionadas o gestionadas por los clientes, debe especificar los usuarios y grupos de Active Directory que desee sincronizar y, a continuación, sincronizarlos con el Centro de identidades de IAM.

- **Sincronización de AD configurable:** Centro de identidades de IAM no busca usuarios y grupos directamente en el controlador de dominio. En su lugar, primero debe especificar la lista de usuarios y grupos que desea sincronizar. Puede configurar esta lista, también conocida como ámbito de sincronización, de una de las siguientes maneras, en función de si tiene usuarios y grupos que ya están sincronizados en Centro de identidades de IAM o si tiene nuevos usuarios y grupos que vaya a sincronizar por primera vez mediante la sincronización configurable de AD.
- **Usuarios y grupos existentes:** si tiene usuarios y grupos que ya están sincronizados en Centro de identidades de IAM, el ámbito de sincronización de la sincronización configurable de AD se rellena previamente con una lista de esos usuarios y grupos. Para asignar nuevos usuarios o grupos, debe añadirlos específicamente al ámbito de sincronización. Para obtener más información, consulte [Añadir usuarios y grupos a su ámbito de sincronización](#).
- **Nuevos usuarios y grupos:** si quiere asignar a nuevos usuarios y grupos el acceso a las aplicaciones y Cuentas de AWS, debe especificar qué usuarios y grupos quiere añadir al ámbito de sincronización en la sincronización configurable de AD antes de poder utilizar Centro de identidades de IAM para realizar la asignación. Para obtener más información, consulte [Añadir usuarios y grupos a su ámbito de sincronización](#).

#### • Asignaciones a grupos anidados en Active Directory

Los grupos que son miembros de otros grupos se llaman grupos anidados (o grupos secundarios).

- **Sincronización AD configurable:** el uso de la sincronización de AD configurable para realizar asignaciones a un grupo de Active Directory que contiene otros grupos anidados puede aumentar el número de usuarios que tienen acceso a Cuentas de AWS o las aplicaciones. En este caso, la asignación se aplica a todos los usuarios, incluidos los de los grupos anidados. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, los miembros del grupo B también consiguen el acceso.
- **Actualización de los flujos de trabajo automatizados**

Si tiene flujos de trabajo automatizados que utilizan las acciones de la API del almacén de identidades de Centro de identidades de IAM y las acciones de la API de asignación de Centro



de identidades de IAM para asignar a los nuevos usuarios y grupos el acceso a las cuentas y a las aplicaciones y sincronizarlos en Centro de identidades de IAM, debe ajustar esos flujos de trabajo antes del 15 de abril de 2022 para que funcionen según lo previsto con la sincronización AD configurable. La sincronización de AD configurable cambia el orden en que se realizan la asignación y el aprovisionamiento de usuarios y grupos, así como la forma en que se realizan las consultas.

- Sincronización AD configurable: el aprovisionamiento se produce primero y no se realiza automáticamente. En su lugar, primero debe añadir usuarios y grupos de forma explícita al almacén de identidades, agregándolos a su ámbito de sincronización. Para obtener información sobre los pasos recomendados para automatizar la configuración de sincronización para una sincronización AD configurable, consulte [Automatizar la configuración de sincronización para una sincronización AD configurable](#).

## Temas

- [Cómo funciona la sincronización de AD configurable](#)
- [Configuración de las asignaciones de atributos para su sincronización](#)
- [Configuración de la primera sincronización de Active Directory a IAM Identity Center](#)
- [Añadir usuarios y grupos a su ámbito de sincronización](#)
- [Eliminación de usuarios y grupos de su ámbito de sincronización](#)
- [Pausa y reanudación de la sincronización](#)
- [Automatizar la configuración de sincronización para una sincronización AD configurable](#)

## Cómo funciona la sincronización de AD configurable

Centro de identidades de IAM actualiza los datos de identidad basados en anuncios en el almacén de identidades mediante el siguiente proceso. Para obtener más información acerca de los requisitos previos, consulte [Requisitos y consideraciones previos](#).

## Creación

Tras conectar el directorio autogestionado de Active Directory o el AWS Managed Microsoft AD directorio gestionado por Directory Service el Centro de identidades de IAM, puede configurar de forma explícita los usuarios y grupos de Active Directory que desee sincronizar en el almacén de identidades del Centro de identidades de IAM. Las identidades que elija se sincronizarán aproximadamente cada 3 horas en el almacén de identidades de Centro de identidades de IAM. Según el tamaño del directorio, el proceso de sincronización puede tardar más.

Los grupos que son miembros de otros grupos (llamados grupos anidados o grupos secundarios) también se escriben en el almacén de identidades.

Solo puede asignar el acceso a nuevos usuarios o grupos después de que estén sincronizados en el almacén de identidades de Centro de identidades de IAM.

## Actualización

Los datos de identidad del almacén de identidades de Centro de identidades de IAM se mantienen actualizados al leer periódicamente los datos del directorio de origen de Active Directory. De forma predeterminada, IAM Identity Center sincroniza los datos de su Active Directory cada hora en un ciclo de sincronización. Los datos pueden tardar entre 30 minutos y 2 horas en sincronizarse con el IAM Identity Center, según el tamaño de su Active Directory.

Los objetos de usuario y grupo que se encuentran en el ámbito de la sincronización y sus pertenencias se crean o actualizan en Centro de identidades de IAM para asignarlos a los objetos correspondientes del directorio de origen de Active Directory. En el caso de los atributos de usuario, solo el subconjunto de atributos que aparece en la sección Atributos para controlar el acceso de la consola de Centro de identidades de IAM se actualiza en Centro de identidades de IAM. Las actualizaciones de atributos que realice en Active Directory pueden tardar un ciclo de sincronización en reflejarse en el IAM Identity Center.

También puede actualizar el subconjunto de usuarios y grupos que sincroniza en el almacén de identidades de Centro de identidades de IAM. Puede optar por añadir nuevos usuarios o grupos a este subconjunto o eliminarlos. Todas las identidades que añada se sincronizarán en la próxima sincronización programada. Las identidades que elimine del subconjunto dejarán de actualizarse en el almacén de identidades de Centro de identidades de IAM. Los usuarios que no estén sincronizados durante más de 28 días quedarán inhabilitados en el almacén de identidades de Centro de identidades de IAM. Los objetos de usuario correspondientes se deshabilitarán automáticamente en el almacén de identidades de Centro de identidades de IAM durante el siguiente ciclo de sincronización, a menos que formen parte de otro grupo que siga formando parte del ámbito de sincronización.

## Eliminación

Los usuarios y grupos se eliminan del almacén de identidades de Centro de identidades de IAM cuando los objetos de usuario o grupo correspondientes se eliminan del directorio de origen de Active Directory. Como alternativa, puede eliminar de forma explícita los objetos de usuario del almacén de identidades de Centro de identidades de IAM mediante la consola de Centro de

identidades de IAM. Si utiliza la consola de Centro de identidades de IAM, también debe eliminar los usuarios del ámbito de sincronización para garantizar que no se vuelvan a sincronizar con Centro de identidades de IAM durante el siguiente ciclo de sincronización.

También puede pausar y reiniciar la sincronización en cualquier momento. Si pausa la sincronización durante más de 28 días, se deshabilitarán todos los usuarios.

### Configuración de las asignaciones de atributos para su sincronización

Cómo obtener más información acerca de los atributos disponibles, consulte [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos](#).

Cómo configurar las asignaciones de atributos de Centro de identidades de IAM a su directorio:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar sincronización, seleccione Ver asignaciones de atributos.
5. En Atributos de usuario de Active Directory, configure los atributos del almacén de identidades de Centro de identidades de IAM y los atributos de usuario de Active Directory. Por ejemplo, puede que desee asignar el atributo email del almacén de identidades de Centro de identidades de IAM al atributo `objectguid` del directorio de usuarios de Active Directory.

#### Note

En Atributos de grupo, no se pueden cambiar los atributos del almacén de identidades de IAM Identity Center ni los atributos de grupo de Active Directory.

6. Seleccione Save changes (Guardar cambios). Esto le llevará a la página de Administrar sincronización.

### Configuración de la primera sincronización de Active Directory a IAM Identity Center

Si va a sincronizar sus usuarios y grupos de Active Directory con IAM Identity Center por primera vez, siga estos pasos. También puede seguir los pasos que se describen en [Cambiar su fuente de identidad](#) para cambiar el origen de identidad de IAM Identity Center a Active Directory.

## Configuración guiada

1. Abra la [consola de Centro de identidades de IAM](#).

### Note

Asegúrese de que la consola del IAM Identity Center utilice una de las ubicaciones Regiones de AWS de su AWS Managed Microsoft AD directorio antes de continuar con el siguiente paso.

2. Seleccione Configuración.
3. En la parte superior de la página, en el mensaje de notificación, seleccione Iniciar configuración guiada.
4. En el paso 1 (opcional): configurar las asignaciones de atributos, revise las asignaciones de atributos de usuario y grupo predeterminadas. Si no es necesario realizar cambios, seleccione Siguiente. Si es necesario realizar cambios, realice los cambios y, a continuación, seleccione Guardar cambios.
5. En el paso 2 (opcional): configurar el alcance de la sincronización, seleccione la pestaña Usuarios. A continuación, introduzca el nombre de usuario exacto del usuario que quiere añadir a su ámbito de sincronización y seleccione Añadir. Seleccione la pestaña Grupos. A continuación, introduzca el nombre de grupo exacto del grupo que quiere añadir a su ámbito de sincronización y seleccione Añadir. A continuación, elija Siguiente. Si quiere añadir usuarios y grupos a su ámbito de sincronización más adelante, no realice ningún cambio y seleccione Siguiente.
6. En el paso 3: revisar y guardar la configuración, confirme las asignaciones de atributos en el paso 1: asignaciones de atributos y sus usuarios y grupos en el paso 2: ámbito de sincronización. Seleccione Guardar configuración. Esto le llevará a la página Administrar sincronización.

## Añadir usuarios y grupos a su ámbito de sincronización

### Note

Al añadir grupos al ámbito de sincronización, sincronice los grupos directamente desde el dominio local de confianza, en lugar de hacerlo desde los grupos del dominio. AWS Managed Microsoft AD Los grupos sincronizados directamente desde el dominio de confianza

contienen objetos de usuario reales a los que el Centro de Identidad de IAM puede acceder y sincronizarlos correctamente.

Agregue sus usuarios y grupos de Active Directory al IAM Identity Center siguiendo estos pasos.

Para agregar usuarios

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.
6. En Usuarios y grupos agregados, revise el usuario que desea agregar.
7. Seleccione Enviar.
8. En el panel de navegación, seleccione Usuarios. Si el usuario que ha especificado no se muestra en la lista, elija el icono de actualización para actualizar la lista de usuarios.

Cómo añadir grupos:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de administrar la sincronización, elija la pestaña Grupos y, continuación, seleccione Añadir usuarios y grupos.
5. Seleccione la pestaña Groups (Grupos). En Grupo, introduzca el nombre exacto del grupo y seleccione Añadir.
6. En Usuarios y grupos añadidos, revise el grupo que desea agregar.
7. Seleccione Enviar.
8. En el panel de navegación, elija Grupos. Si el grupo que ha especificado no se muestra en la lista, seleccione el icono de actualización para actualizar la lista de grupos.

## Eliminación de usuarios y grupos de su ámbito de sincronización

Para obtener más información sobre lo que ocurre cuando elimina usuarios y grupos del ámbito de sincronización, consulte [Cómo funciona la sincronización de AD configurable](#).

Cómo eliminar usuarios:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Elija la pestaña Users.
5. En Usuarios en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los usuarios, seleccione la casilla de verificación situada junto al nombre de usuario.
6. Elija Eliminar .

Cómo eliminar grupos:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Seleccione la pestaña Groups (Grupos).
5. En Grupos en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los grupos, seleccione la casilla de verificación situada junto al nombre del grupo.
6. Elija Eliminar .

## Pausa y reanudación de la sincronización

Al pausar la sincronización, se pausan todos los ciclos de sincronización futuros e impide que los cambios que realice en los usuarios y grupos de Active Directory se reflejen en Centro de identidades de IAM. Tras reanudar la sincronización, el ciclo de sincronización recoge los cambios de la siguiente sincronización programada.

## Cómo pausar la sincronización:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Pausar la sincronización.

## Cómo reanudar la sincronización:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Reanudar la sincronización.

### Note

Si aparece Pausar la sincronización en lugar de Reanudar la sincronización, significa que la sincronización de Active Directory con Centro de identidades de IAM ya se ha reanudado.

## Automatizar la configuración de sincronización para una sincronización AD configurable

Para garantizar que su flujo de trabajo automatizado funcione según lo esperado con la sincronización de AD configurable, le recomendamos que realice los siguientes pasos para automatizar la configuración de la sincronización.

## Cómo automatizar la configuración de sincronización para una sincronización AD configurable:

1. En Active Directory, cree un Grupo de sincronización principal que contenga todos los usuarios y grupos que desee sincronizar en Centro de identidades de IAM. Por ejemplo, puede asignar un nombre al grupo. IAMIdentityCenterAllUsersAndGroups
2. En Centro de identidades de IAM, añada el grupo de sincronización principal a su lista de sincronización configurable. Centro de identidades de IAM sincronizará todos los usuarios,

grupos, subgrupos y miembros de todos los grupos incluidos en el grupo de sincronización principal.

3. Use las acciones de la API de administración de usuarios y grupos de Active Directory proporcionadas por Microsoft para añadir o eliminar usuarios y grupos del grupo de sincronización principal.

## Administración de usuarios en el directorio de Identity Center

IAM Identity Center ofrece las siguientes funciones para sus usuarios y grupos:

- Cree sus usuarios y grupos.
- Añada sus usuarios como miembros a los grupos.
- Asigne a los grupos el nivel de acceso deseado a Cuentas de AWS sus aplicaciones.

Para gestionar los usuarios y los grupos en el almacén del Centro de Identidad de IAM, AWS es compatible con las operaciones de la API que se indican en las [acciones del Centro de Identidad](#).

## Aprovisionamiento cuando los usuarios están en IAM Identity Center

Al crear usuarios y grupos directamente en IAM Identity Center, el aprovisionamiento es automático. Estas identidades están disponibles de inmediato para su uso al realizar asignaciones y para que las utilicen las aplicaciones. Para obtener más información, consulte [Aprovisionamiento de usuarios y grupos](#).

## Cambio de su fuente de identidad

Si prefiere administrar los usuarios en AWS Managed Microsoft AD, puede dejar de usar el directorio del Centro de identidad en cualquier momento y, en su lugar, conectar el Centro de identidad de IAM al directorio de Microsoft AD mediante Directory Service. Para obtener información, consulte las consideraciones para [Cambiar entre el directorio IAM Identity Center y Active Directory](#).

Si prefiere administrar los usuarios en un proveedor de identidades (IdP) externo, puede conectar IAM Identity Center a su IdP y habilitar el aprovisionamiento automático. Para obtener información, consulte las consideraciones para [Cómo cambiar de IAM Identity Center a un IdP externo](#).

### Temas

- [Agregue usuarios a su directorio de Identity Center](#)



- [Agregue grupos al directorio del Identity Center](#)
- [Agregar usuarios a grupos](#)
- [Eliminación de grupos de IAM Identity Center](#)
- [Eliminación de usuarios del IAM Identity Center](#)
- [Eliminar usuarios de los grupos](#)
- [Editar las propiedades de los usuarios del directorio de IAM Identity Center](#)

## Agregue usuarios a su directorio de Identity Center

Los usuarios y grupos que cree en su directorio de Identity Center solo estarán disponibles en IAM Identity Center. Utilice el siguiente procedimiento para añadir usuarios a su directorio de Identity Center. Como alternativa, puede llamar a la operación de la AWS API [CreateUser](#) para añadir usuarios.

### Console

Para añadir un usuario

1. Abra la consola de [IAM Identity Center](#).
2. Seleccione Usuarios.
3. Elija Agregar usuario, y proporcione la siguiente información necesaria:
  - a. Nombre de usuario: este nombre de usuario es obligatorio para iniciar sesión en el portal de AWS acceso y no se puede cambiar más adelante. Debe tener entre 1 y 100 caracteres de longitud.
  - b. Contraseña: puede enviar un correo electrónico con las instrucciones de configuración de la contraseña (esta es la opción predeterminada) o generar una contraseña de un solo uso. Si va a crear un usuario administrativo y envía un correo electrónico, asegúrese de especificar una dirección de correo electrónico a la que pueda acceder.
    - i. Enviar un correo electrónico a este usuario con instrucciones de configuración: esta opción envía automáticamente al usuario un correo electrónico de Amazon Web Services con el asunto Invitación a unirse a AWS IAM Identity Center. El correo electrónico invita al usuario, en nombre de su empresa, a acceder al portal de acceso AWS de IAM Identity Center y registrar una contraseña. La invitación por correo electrónico caducará en siete días. Si esto ocurre, para volver a enviar el

correo electrónico, seleccione Restablecer contraseña y, a continuación, Enviar un correo electrónico al usuario con instrucciones para restablecer la contraseña. Antes de que el usuario acepte la invitación, verá el enlace Enviar correo electrónico de verificación, que sirve para verificar su dirección de correo electrónico. Sin embargo, este paso es opcional y desaparecerá cuando el usuario acepte la invitación y registre una contraseña.

 Note

En algunas regiones, IAM Identity Center envía correos electrónicos a los usuarios que utilizan Amazon Simple Email Service desde otra Región de AWS. Para obtener información sobre cómo se envían los correos electrónicos, consulte [Correos electrónicos entre regiones con Amazon SES](#).

Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws.com` o `no-reply@login.awsapps.com`. Le recomendamos que configure su sistema de correo electrónico para que acepte los mensajes con estas direcciones de correo electrónico como remitente y no los trate como correo basura o no deseado.

- ii. Genere una contraseña de un solo uso que pueda compartir con este usuario: esta opción le proporciona la URL del portal de AWS acceso y los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico. El usuario tendrá que verificar su dirección de correo electrónico. Puede iniciar el proceso si selecciona el enlace Enviar correo electrónico de verificación. El enlace de verificación por correo electrónico caducará en siete días. Si esto ocurre, para volver a enviar el enlace de verificación por correo electrónico, seleccione Restablecer contraseña y, a continuación, Generar una contraseña de un solo uso y compartir la contraseña con el usuario.
- c. Correo electrónico: la dirección de correo electrónico debe ser única.
- d. Confirmación de la dirección de correo electrónico
- e. Nombre: debe introducir un nombre aquí para que funcione el aprovisionamiento automático. Para obtener más información, consulte [Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM](#).

- f. Apellido: debe introducir un nombre aquí para que funcione el aprovisionamiento automático.
- g. Display name (Nombre de visualización)

 Note

(Opcional) Si corresponde, puede especificar valores para atributos adicionales, como el ID inmutable de Microsoft 365 del usuario, para ayudar a proporcionarle acceso de inicio de sesión único a determinadas aplicaciones empresariales.

- 4. Elija Siguiente.
- 5. Si corresponde, seleccione uno o más grupos a los que desee añadir al usuario y elija Siguiente.
- 6. Revise la información que especificó para el paso 1: especificar los detalles del usuario y el paso 2: agregar el usuario a los grupos (opcional). Elija Editar en uno de los pasos para realizar cualquier cambio. Tras confirmar que se ha especificado la información correcta para ambos pasos, elija Añadir usuario.

## AWS CLI

Para añadir un usuario

El siguiente comando `create-user` crea un nuevo usuario en su directorio de Identity Center.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

Salida:

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

**Note**

Cuando crea usuarios con el comando de la CLI `create-user` o la operación de la API [CreateUser](#), los usuarios no tienen contraseñas. Puede actualizar la configuración de IAM Identity Center para enviar a estos usuarios un correo electrónico de verificación tras su primer intento de inicio de sesión para que puedan configurar una contraseña. Si no habilita esta configuración, debe generar y compartir una contraseña de un solo uso con el usuario. Para obtener más información, consulte [Envío por correo electrónico de una contraseña de un solo uso a los usuarios creados con la API o la CLI](#).

## Agregue grupos al directorio del Identity Center

Utilice el siguiente procedimiento para añadir grupos a su directorio de Identity Center. Como alternativa, puedes llamar a la operación de la AWS API [CreateGroup](#) para añadir grupos.

### Console

Para añadir un grupo

1. Abrir la consola de [IAM Identity Center](#).
2. Elija Grupos.
3. Elija Crear grupo.
4. Escriba un Nombre de grupo y, opcionalmente, una Descripción. La descripción debe proporcionar detalles sobre qué permisos se han asignado o se asignará al grupo. En Añadir usuarios al grupo: opcional, busque los usuarios que desea añadir como miembros. A continuación, seleccione la casilla de verificación situada junto a cada uno de ellos.
5. Elija Crear grupo.

### AWS CLI

Para añadir un grupo

El siguiente comando `create-group` crea un nuevo grupo en el directorio de Identity Center.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group for Developers" \  
  --users-to-add [{"username": "john.doe", "password": "P@ssw0rd"}]
```

```
--description "Group that contains all developers"
```

Salida:

```
{
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",
  "IdentityStoreId": "d-1234567890"
}
```

Tras añadir este grupo al directorio de Identity Center, puede asignar el acceso de inicio de sesión único al grupo. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

## Agregar usuarios a grupos

Utilice el siguiente procedimiento para añadir usuarios como miembros de un grupo que ha creado anteriormente en su directorio de Identity Center. Como alternativa, puedes llamar a la operación de la AWS API [CreateGroupMembership](#) para añadir un usuario como miembro de un grupo.

### Console

Cómo añadir un usuario como miembro de un grupo

1. Abra la consola de [IAM Identity Center](#).
2. Elija Grupos.
3. Elija el nombre de grupo que desea actualizar.
4. En la página de detalles del grupo, en Usuarios de este grupo, elija Añadir usuarios al grupo.
5. En la página Añadir usuarios al grupo, en Otros usuarios, localice los usuarios que desea añadir como miembros. A continuación, marque la casilla de verificación situada junto a cada uno de ellos.
6. Elija Agregar usuarios.

### AWS CLI

Cómo añadir un usuario como miembro de un grupo

El siguiente comando `create-group-membership` agrega un nuevo usuario en su directorio de Identity Center.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

## Eliminación de grupos de IAM Identity Center

Al eliminar un grupo del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones para todos los usuarios que son miembros de este grupo. Una vez que se elimina un grupo, no se puede deshacer la acción. Utilice el siguiente procedimiento para eliminar un grupo de su directorio de Identity Center.

### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar grupos en IAM, consulte [Eliminar un grupo de usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

### Console

Para eliminar un grupo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Grupos.
3. Hay 2 formas de eliminar un grupo:
  - En la página Grupos, puede seleccionar varios grupos para su eliminación. Elija el nombre de grupo que desee eliminar y seleccione Eliminar grupo.

- Elija el nombre de grupo que desea eliminar. En la página de detalles del grupo, elija Eliminar grupo.
4. Es posible que se le pida que confirme su intención de eliminar el grupo.
    - Si elimina varios grupos a la vez, confírmelo escribiendo **“Delete”** en el cuadro de diálogo Eliminar grupo.
    - Si elimina un solo grupo que contiene usuarios, confirme su intención escribiendo el nombre del grupo que desea eliminar en el cuadro de diálogo Eliminar grupo.
  5. Elija Eliminar grupo. Si ha seleccionado varios grupos para eliminarlos, elija Eliminar # grupos.

## AWS CLI

Para eliminar un grupo

El siguiente comando `delete-group` elimina el grupo especificado de su directorio de Identity Center.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

## Eliminación de usuarios del IAM Identity Center

Al eliminar un usuario del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones. Tras eliminar un usuario, no podrá deshacer esta acción. Utilice el siguiente procedimiento para eliminar un usuario de su directorio de Identity Center.

### Note

Si deshabilita el acceso de un usuario o lo elimina en el Centro de identidad de IAM, dicho usuario no podrá iniciar sesión inmediatamente en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión. Para obtener más información, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

**⚠ Important**

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar usuarios en IAM, consulte [Eliminar un usuario de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

## Console

### Cómo eliminar un usuario

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Hay 2 formas de eliminar un usuario:
  - En la página Usuarios, puede seleccionar varios usuarios para su eliminación. Seleccione el nombre de usuario que desee eliminar y seleccione Eliminar usuarios.
  - Elija el nombre de usuario que desea eliminar. En la página de detalles del usuario, vaya a la pestaña Eliminar usuario.
4. Si elimina varios usuarios a la vez, confirme su intención escribiendo **Delete** en el cuadro de diálogo Eliminar usuario.
5. Seleccione Eliminar usuario(s). Si ha seleccionado varios usuarios para eliminarlos, elija Eliminar # usuarios.

## AWS CLI

### Cómo eliminar un usuario

El siguiente comando `delete-user` elimina un usuario de su directorio de Identity Center.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```



## Eliminar usuarios de los grupos

Utilice el siguiente procedimiento para eliminar miembros de un grupo. Como alternativa, puede llamar a la operación de la AWS API [DeleteGroupMembership](#) para eliminar un usuario de un grupo.

### Console

#### Eliminación de un usuario de un grupo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Grupos.
3. Elija el grupo que desea actualizar.
4. En la página de detalles del grupo, en Usuarios de este grupo, elija los usuarios que desee eliminar.
5. Elija Eliminar usuarios del grupo.
6. En el cuadro de diálogo Eliminar usuarios, elija Eliminar usuarios del grupo para comprobar que desea eliminar el acceso de los usuarios a la cuenta y las aplicaciones asignadas al grupo.

### AWS CLI

#### Eliminación de un usuario de un grupo

El siguiente comando `delete-group-membership` elimina un miembro de un grupo.

```
aws identitystore delete-group-membership
  --identity-store-id d-1234567890 \
  --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

## Editar las propiedades de los usuarios del directorio de IAM Identity Center

Utilice el siguiente procedimiento para editar las propiedades de un usuario en su directorio de Identity Center. Como alternativa, puedes llamar a la operación de AWS API [UpdateUser](#) para actualizar las propiedades del usuario.

## Console

### Cómo editar las propiedades de los usuarios de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Elija el usuario que desee editar.
4. En la página Perfil, al lado de Detalles del perfil seleccione Editar.
5. En la página Editar detalles del perfil, actualice las propiedades que corresponda. A continuación, elija Save changes (Guardar cambios).

#### Note

(Opcional) Puede modificar atributos adicionales como el número de empleado y la ID inmutable de Office 365 para ayudar a asignar la identidad del usuario en IAM Identity Center a determinadas aplicaciones empresariales que los usuarios necesiten utilizar.

#### Note

El atributo Correo electrónico es un campo editable y el valor que proporcione debe ser único.

## AWS CLI

### Cómo editar las propiedades de los usuarios de IAM Identity Center

El siguiente comando `update-user` actualiza el alias del usuario.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

# Configure el acceso de la fuerza laboral a AWS los recursos

Configure la forma en que los usuarios de su fuerza laboral se autentican y acceden a AWS los recursos a través del Centro de identidad de IAM. En esta sección se describen los siguientes componentes que rigen el acceso de los usuarios del personal a su entorno de AWS :

- **Sesiones de autenticación:** comprenda cómo IAM Identity Center administra los diferentes tipos de sesiones de usuario, desde las sesiones del portal interactivo hasta las sesiones de aplicaciones en segundo plano, y cómo interactúan entre sí.
- **Administración del acceso de los usuarios:** configure la duración de las sesiones, desactive las cuentas de usuario e implemente bloques de acceso en toda la organización para mantener la seguridad y el cumplimiento.
- **Administración de contraseñas:** para los usuarios creados en el directorio de Identity Center, establezca los requisitos de contraseña, gestione la configuración de las credenciales de los usuarios y administre el restablecimiento de las contraseñas de los usuarios.
- **Autenticación multifactor:** para los usuarios creados en el directorio de Identity Center, mejore la seguridad con la MFA mediante aplicaciones de autenticación, claves de seguridad o autenticadores integrados para proteger los inicios de sesión de los usuarios.

## Temas

- [Descripción de las sesiones de autenticación en IAM Identity Center](#)
- [Configuración de la duración de la sesión en IAM Identity Center](#)
- [Deshabilite el acceso de los usuarios Cuentas de AWS y las aplicaciones en el Centro de Identidad de IAM](#)
- [Denegación de acceso a los usuarios con las políticas de control de servicios](#)
- [Administración del acceso para usuarios en el directorio de Identity Center](#)

## Descripción de las sesiones de autenticación en IAM Identity Center

Cuando un usuario inicia sesión en el [portal de acceso de AWS](#), IAM Identity Center crea una sesión de autenticación que representa la identidad verificada del usuario.

Una vez autenticado, el usuario puede acceder a todas sus [aplicaciones asignadas Cuentas de AWS y AWS administradas](#) por el [cliente para las](#) que los administradores le hayan otorgado permiso de uso, sin necesidad de iniciar sesión adicionales.

## Tipos de sesiones de autenticación

### Sesiones interactivas de usuario

Cuando un usuario inicia sesión en el portal de AWS acceso, el Centro de Identidad de IAM crea una sesión interactiva para el usuario. Esta sesión representa el estado autenticado del usuario en IAM Identity Center y sirve de base para crear otros tipos de sesiones. Las sesiones interactivas de usuario pueden durar el tiempo configurado en IAM Identity Center, que puede ser de hasta 90 días.

Las sesiones interactivas de usuario son el principal mecanismo de autenticación. Finalizan cuando el usuario cierra sesión o cuando un administrador finaliza su sesión. La duración de estas sesiones debe configurarse cuidadosamente en función de los requisitos de seguridad de la organización.

Para obtener información acerca de la configuración de la duración de la sesión interactiva del usuario, consulte [the section called “Configuración de la duración de la sesión”](#).

### Sesiones de aplicación

Las sesiones de aplicación son las conexiones autenticadas entre los usuarios y las aplicaciones AWS gestionadas (como Kiro o Amazon Quick) que IAM Identity Center establece mediante el inicio de sesión único.

De forma predeterminada, las sesiones de la aplicación tienen una duración de una hora, pero se actualizan automáticamente mientras la sesión interactiva del usuario subyacente siga siendo válida. Este mecanismo de actualización proporciona una experiencia fluida a los usuarios y, al mismo tiempo, mantiene los controles de seguridad. Cuando finaliza una sesión interactiva de usuario, ya sea mediante el cierre de sesión del usuario o mediante una acción del administrador, las sesiones de la aplicación finalizarán en el siguiente intento de actualización, normalmente en 30 minutos.

### Sesiones de usuario en segundo plano

Las sesiones de usuario en segundo plano son sesiones de duración prolongada diseñadas para aplicaciones que necesitan ejecutar procesos durante horas o días sin interrupción. Actualmente, este tipo de sesión se aplica principalmente a [Amazon SageMaker Studio](#), donde los científicos de datos pueden realizar tareas de formación en aprendizaje automático que tardan muchas horas en completarse.

Para obtener información sobre cómo configurar la duración de las sesiones de usuario en segundo plano, consulte [User background sessions](#).

## Sesiones de Kiro

Puede ampliar las sesiones de Kiro para que los desarrolladores que utilizan Kiro puedan IDEs mantener la autenticación durante un máximo de 90 días. Esta característica reduce las interrupciones de inicio de sesión mientras trabaja en el código.

Estas sesiones son independientes de otros tipos de sesiones y no afectan a las sesiones interactivas de usuarios ni a otras aplicaciones administradas por AWS . En función de cuándo haya activado IAM Identity Center, es posible que esta característica esté habilitada de forma predeterminada.

Para obtener información sobre la configuración de sesiones ampliadas de Kiro, consulte. [???](#)

## Sesiones de roles de IAM creados por IAM Identity Center

El IAM Identity Center crea un tipo de sesión diferente cuando los usuarios acceden al Consola de administración de AWS o. AWS CLI En estos casos, IAM Identity Center utiliza la sesión de inicio de sesión para obtener una sesión de IAM asumiendo un rol de IAM especificado en el conjunto de permisos del usuario.

### Important

A diferencia de las sesiones de aplicación, las sesiones de roles de IAM funcionan de forma independiente una vez establecidas. Persisten durante el tiempo configurado en el conjunto de permisos, que puede ser de hasta 12 horas, independientemente del estado de la sesión de inicio de sesión original. Este comportamiento garantiza que las operaciones de CLI o las sesiones de consola de larga duración no finalicen inesperadamente.

## Formas de finalizar las sesiones de usuario en IAM Identity Center

### Iniciadas por el usuario

Cuando un usuario cierra sesión en el portal de AWS acceso, la sesión de inicio de sesión finaliza, lo que impide que el usuario acceda a nuevos recursos.

Sin embargo, las sesiones de aplicación existentes no finalizan de forma instantánea. En cambio, finalizarán en aproximadamente 30 minutos, cuando se intente realizar la siguiente actualización y se descubra que la sesión de inicio de sesión ya no es válida. Las sesiones de rol de IAM existentes continúan hasta que caduquen en función de la configuración del conjunto de permisos, lo que podría ocurrir hasta 12 horas después.

## Iniciadas por el administrador

Cualquier persona de su organización con permisos administrativos en IAM Identity Center, normalmente administradores de TI o equipos de seguridad, puede [finalizar la sesión de un usuario](#). Esta acción funciona de la misma manera que si los usuarios cerraran sesión ellos mismos, lo que permite a los administradores exigir a los usuarios que vuelvan a iniciar sesión cuando sea necesario. Esta capacidad resulta útil cuando las políticas de seguridad cambian o cuando se detecta una actividad sospechosa.

Cuando un administrador de IAM Identity Center [elimina a un usuario](#) o [deshabilita su acceso](#), el usuario pierde el acceso al portal de acceso de AWS y no puede volver a iniciar sesión para iniciar una nueva sesión de aplicación o rol de IAM. El usuario perderá el acceso a las sesiones de la aplicación existentes en menos de 30 minutos. Todas las sesiones de rol de IAM existentes continuarán en función de la duración configurada en el conjunto de permisos de IAM Identity Center. El tiempo máximo de duración de la sesión puede ser de 12 horas.

## Qué sucede con el acceso de los usuarios al finalizar una sesión

Esta referencia proporciona información detallada sobre el comportamiento de las sesiones de IAM Identity Center cuando se toman medidas administrativas. Las tablas de esta sección muestran la duración y los efectos de las acciones de administración de usuarios y los cambios de permisos en el acceso al portal de AWS acceso, las aplicaciones y las Cuenta de AWS sesiones.

### Administración de usuarios

En esta tabla se resume cómo los cambios en la administración de usuarios afectan al acceso a AWS los recursos, las sesiones de aplicaciones y las sesiones de AWS cuentas.

| Action                          | El usuario pierde acceso a IAM Identity Center                   | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las sesiones existentes<br>Cuenta de AWS                                                           |
|---------------------------------|------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Acceso de usuario deshabilitado | Con efecto inmediato                                             | Con efecto inmediato                                    | En menos de 30 minutos                                              | En menos de 12 horas.<br>La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |
| Se elimina el usuario           | Con efecto inmediato                                             | Con efecto inmediato                                    | En menos de 30 minutos                                              | En menos de 12 horas.<br>La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |
| Se revoca la sesión del usuario | El usuario debe volver a iniciar sesión para recuperar el acceso | Con efecto inmediato                                    | En menos de 30 minutos                                              | En menos de 12 horas.<br>La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |

| Action                          | El usuario pierde acceso a IAM Identity Center                   | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las sesiones existentes Cuenta de AWS                                                           |
|---------------------------------|------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Se cierra la sesión del usuario | El usuario debe volver a iniciar sesión para recuperar el acceso | Con efecto inmediato                                    | En menos de 30 minutos                                              | En menos de 12 horas. La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |

## Pertenencia a grupos

En esta tabla se resume cómo los cambios en los permisos de los usuarios y la pertenencia a grupos afectan al acceso a AWS los recursos, las sesiones de aplicaciones y las sesiones de AWS cuenta.

| Action                                                   | El usuario pierde acceso a IAM Identity Center               | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las sesiones existentes Cuenta de AWS                                                           |
|----------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Aplicación o Cuenta de AWS acceso eliminados del usuario | No, el usuario puede seguir accediendo a IAM Identity Center | Con efecto inmediato                                    | En menos de 1 hora                                                  | En menos de 12 horas. La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |



| Action                                                                             | El usuario pierde acceso a IAM Identity Center               | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las sesiones existentes Cuenta de AWS                                                           |
|------------------------------------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Se elimina un usuario del grupo al que se le asignó una aplicación o Cuenta de AWS | No, el usuario puede seguir accediendo a IAM Identity Center | En menos de 1 hora                                      | En un plazo de 2 horas                                              | En menos de 12 horas. La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |
| Aplicación o Cuenta de AWS acceso eliminados del grupo                             | No, el usuario puede seguir accediendo a IAM Identity Center | Con efecto inmediato                                    | En menos de 1 hora                                                  | En menos de 12 horas. La duración depende de la duración de la sesión de rol de IAM configurada para el conjunto de permisos. |

#### Note

El portal de AWS acceso AWS CLI reflejará los permisos de usuario actualizados una hora después de añadir o eliminar un usuario de ese grupo.

### Descripción de las diferencias de tiempo

- Con efecto inmediato: acciones que requieren una reautenticación inmediata.

- Entre 30 minutos y 2 horas: las sesiones de aplicación necesitan tiempo para comprobarse en IAM Identity Center y detectar cualquier cambio.
- En menos de 12 horas: las sesiones de rol de IAM funcionan de forma independiente y solo finalizan cuando vence la duración configurada.

## Cierre de sesión único

IAM Identity Center no admite el cierre de sesión único mediante SAML (un protocolo que cierra automáticamente la sesión de los usuarios en todas las aplicaciones conectadas cuando cierran sesión en una de ellas) iniciado por un proveedor de identidades que actúa como [origen de identidad](#). Además, no envía el cierre de sesión único mediante SAML a las [aplicaciones de SAML 2.0](#) que utilizan IAM Identity Center como proveedor de identidad.

## Prácticas recomendadas para la administración de sesiones

La administración eficaz de sesiones requiere una configuración y una supervisión cuidadosas. Las organizaciones deben configurar la duración de las sesiones acordes con sus requisitos de seguridad y, por lo general, utilizar duraciones más cortas para aplicaciones y entornos confidenciales.

La implementación de procesos para finalizar sesiones cuando los usuarios cambian de rol o abandonan la organización es esencial para mantener los límites de seguridad. La revisión periódica de las sesiones activas debe incorporarse a las prácticas de supervisión de seguridad a fin de detectar comportamientos anómalos que puedan indicar problemas de seguridad, como patrones de acceso inusuales, horarios o ubicaciones de inicio de sesión inesperados o acceso a recursos fuera de las funciones laborales normales.

## Configuración de la duración de la sesión en IAM Identity Center

Puede configurar la duración de la sesión para los usuarios de su fuerza laboral cuando utilizan el IAM Identity Center Portal de acceso a AWS y las aplicaciones que funcionan con él, incluida Kiro. El IAM Identity Center ofrece los siguientes tipos de sesiones: sesiones interactivas para el usuario, sesiones en segundo plano para el usuario y sesiones ampliadas para Kiro.

### Temas

- [Sesiones interactivas de usuario](#)

- [Sesiones de usuario en segundo plano](#)
- [Sesiones ampliadas para Kiro](#)
- [Visión y finalización de las sesiones activas de los usuarios de su personal](#)
- [Consideraciones sobre la duración de la sesión para usar fuentes de identidad, la AWS CLI y AWS SDKs](#)

## Sesiones interactivas de usuario

[Las sesiones interactivas para el usuario son sesiones vinculadas al inicio de sesión del usuario en el portal de acceso o al AWS acceso a las aplicaciones gestionadas.AWS](#) La duración de la sesión de autenticación en las aplicaciones Portal de acceso a AWS y aplicaciones es el período máximo durante el que un usuario puede iniciar sesión sin volver a autenticarse. Si finaliza una sesión en el portal de AWS acceso activo, también finalizará cualquier sesión de estas aplicaciones administradas.

La duración predeterminada de la sesión para las sesiones interactivas de usuario es de 8 horas. Puede especificar una duración diferente, que puede variar entre un mínimo de 15 minutos y un máximo de 90 días. Los valores de duración personalizados se deben introducir en minutos y estar entre 15 minutos y 129 600 minutos (90 días). Para obtener más información, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

Para obtener información sobre cómo las fuentes de identidad del Centro de Identidad de IAM pueden afectar a la duración de la sesión interactiva del usuario, consulte [the section called “Consideraciones sobre las fuentes de identidad, la AWS CLI y AWS SDKs”](#).

Para configurar la duración de una sesión interactiva de usuario

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Duración de la sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar la duración de la sesión.
5. En el cuadro de diálogo Configurar la duración de la sesión, en Sesiones interactivas de usuario, elija la duración máxima de la sesión para sus usuarios utilizando la flecha desplegable. Elija la duración de la sesión y, a continuación, seleccione Guardar.

 Note

Los cambios en la duración de la sesión se aplican solo a las sesiones nuevas. Las sesiones actuales mantienen su duración original.

6. Volverá a la pestaña Autenticación. Aparece un mensaje de notificación verde sobre la pestaña que indica que la configuración de la sesión se actualizó correctamente.

## Sesiones de usuario en segundo plano

Las sesiones de usuario en segundo plano permiten a un usuario iniciar un trabajo de larga duración en una aplicación AWS gestionada como [Amazon SageMaker Studio](#), sin que el usuario tenga que permanecer conectado mientras se ejecuta el trabajo. El trabajo se ejecuta de forma inmediata y utiliza la capacidad de [propagación de identidades de confianza](#) de IAM Identity Center para garantizar que se mantengan los permisos del usuario mientras el trabajo se ejecuta en segundo plano. El trabajo puede seguir ejecutándose aunque el usuario apague el ordenador, caduque su sesión de inicio de sesión en el IAM Identity Center o cierre sesión en el portal de acceso. AWS Esta capacidad permite a los científicos de datos, a los ingenieros de machine learning y a otras personas iniciar flujos de trabajo de análisis y machine learning que se ejecutan en segundo plano sin la participación activa del usuario.

Las sesiones de usuario en segundo plano están habilitadas de forma predeterminada para las aplicaciones AWS gestionadas compatibles, como Amazon SageMaker Studio. Sin embargo, para utilizar esta capacidad, debe habilitar la propagación de identidades de confianza en Amazon SageMaker Studio al crear o actualizar un dominio. Para obtener más información, consulte [Habilitar la propagación de identidades de confianza en su dominio de Amazon SageMaker AI](#).

La duración de sesión predeterminada para las sesiones de usuario en segundo plano es de 7 días. Puede especificar una duración diferente, que puede variar entre un mínimo de 15 minutos y un máximo de 90 días. Los valores de duración personalizados se deben introducir en minutos y estar entre 15 minutos y 129 600 minutos (90 días).

Tenga en cuenta las siguientes consideraciones para las sesiones de usuario en segundo plano:

- Solo se puede crear una sesión de usuario en segundo plano cuando un usuario inicia manualmente un trabajo en Amazon SageMaker Studio. Esta capacidad no es compatible con los flujos de trabajo automatizados y programados.

- Para ver una lista de AWS las regiones que admiten sesiones de usuario en segundo plano, consulte [AWS Regiones compatibles](#).
- Puede ver las sesiones en segundo plano de los usuarios en CloudTrail. Para obtener más información, consulte [Identifying user background session details](#).
- También puede finalizar las sesiones activas de un usuario de su organización. Para obtener más información, consulte [End active sessions for your workforce users](#).

Para configurar la duración de una sesión de usuario en segundo plano

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Duración de la sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar la duración de la sesión.
5. En el cuadro de diálogo Configurar la duración de la sesión, si la casilla Habilitar sesiones de usuario en segundo plano aún no está seleccionada, selecciónela. Desactive la casilla de verificación para deshabilitar las sesiones de usuario en segundo plano.

 Note

Las sesiones actuales no se ven afectadas si deshabilita las sesiones de usuario en segundo plano.

6. En Sesiones de usuario en segundo plano, seleccione la duración máxima de la sesión seleccionando la flecha desplegable. Elija la duración de la sesión y, a continuación, seleccione Guardar.

 Note

Los cambios en la duración de la sesión se aplican solo a las sesiones nuevas. Las sesiones actuales mantienen su duración original.

7. Volverá a la pestaña Autenticación. Aparece un mensaje de notificación verde sobre la pestaña que indica que la configuración de la sesión se actualizó correctamente.

 Note

Una aplicación administrada por el cliente no puede crear una sesión de usuario en segundo plano.

## Sesiones ampliadas para Kiro

Si sus desarrolladores utilizan Kiro como parte de un entorno de desarrollo integrado (IDE), puede establecer la duración de la sesión de Kiro en 90 días. En función de cuándo haya activado el Centro de identidad de IAM, es posible que la duración prolongada de las sesiones de Kiro esté habilitada de forma predeterminada. Esta sesión prolongada no afecta a la duración de la sesión del portal de AWS acceso ni de otras aplicaciones AWS gestionadas.

Para obtener información sobre cómo las fuentes de identidad del Centro de Identidad de IAM pueden afectar a la duración prolongada de la sesión, consulte [the section called “Consideraciones sobre las fuentes de identidad, la AWS CLI y AWS SDKs”](#).

 Note

Se puede acceder a Kiro desde las consolas configuradas como comerciales Regiones de AWS que están habilitadas de forma predeterminada. Si tu instancia del IAM Identity Center se encuentra en una región en la que no se puede acceder a Kiro actualmente, habilitar una sesión prolongada de 90 días no anulará la configuración predeterminada. Esto significa que la duración de la sesión permanece inalterada, independientemente de si habilita una duración de sesión prolongada de 90 días o no. Para obtener más información, consulte [AWS las regiones compatibles con Kiro](#).

Para extender una sesión para Kiro

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Duración de la sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar la duración de la sesión.

5. En el cuadro de diálogo Configurar la duración de la sesión, active la casilla Habilitar sesiones prolongadas para Kiro. Desactive la casilla de verificación para deshabilitar las sesiones de sesión prolongadas para Kiro.
6. Pulse Guardar para volver a la página de configuración.

## Visión y finalización de las sesiones activas de los usuarios de su personal

Como administrador de IAM Identity Center, puede ver la lista de las sesiones activas de los usuarios de su personal y, si es necesario, finalizar una o más sesiones de un usuario. Por ejemplo, es probable que deba finalizar las sesiones de un usuario cuando:

- El usuario ya no necesita las sesiones.
- El usuario no debe mantener su estado de autenticación actual. Esto puede ocurrir cuando deja la empresa o cambian sus permisos.

Puede ver y finalizar estas sesiones a través de la consola de IAM Identity Center. Los usuarios también pueden ver y finalizar sus propias sesiones mediante el portal de AWS acceso. Para obtener información sobre cómo los usuarios de su personal pueden ver y finalizar sus sesiones sin la ayuda de un administrador, consulte [Visualización y finalización de la sesión activa](#).

### Note

La finalización de una sesión activa para un usuario del Centro de Identidad de IAM no finaliza ninguna sesión de rol de IAM activa en el Consola de administración de AWS quirófano. AWS CLI Para obtener más información, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

Para finalizar una sesión activa de un usuario del personal (consola de IAM Identity Center)

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. En la página Usuarios, elija el nombre de usuario cuyas sesiones desee administrar. Esto lo dirigirá a una página con la información del usuario.
4. En la página del usuario, elija la pestaña Sesiones activas. El número entre paréntesis junto a Sesiones activas indica el número de sesiones activas de este usuario.

## 5. Búsqueda de sesiones de usuario en segundo plano (opcional)

Para buscar sesiones por el nombre de recurso de Amazon (ARN) del trabajo que utiliza la sesión, en la lista Tipo de sesión, elija Sesiones de usuario en segundo plano y, a continuación, introduzca el ARN del trabajo en el cuadro de búsqueda.

### Note

Solo puede finalizar las sesiones activas que estén cargadas. Si un usuario tiene muchas sesiones, elija Cargar más sesiones activas para ver las sesiones adicionales.

6. Seleccione la casilla de verificación situada junto a cada sesión que desea finalizar y, a continuación, seleccione Finalizar sesiones.
7. Aparecerá un cuadro de diálogo que confirma que está finalizando las sesiones activas. Revise la información y, si desea continuar, escriba `confirm` y, luego, seleccione Finalizar sesiones.
8. Se le devuelve a la página del usuario. Aparecerá una barra de notificación verde para indicar que las sesiones seleccionadas se eliminaron correctamente.

## Consideraciones sobre la duración de la sesión para usar fuentes de identidad, la AWS CLI y AWS SDKs

Las siguientes son consideraciones para configurar la duración de la sesión si utiliza Microsoft Active Directory (AD) o un proveedor de identidad externo (IdP) como fuente de identidad, o los AWS Command Line Interface kits de desarrollo de AWS software (SDKs) u otras herramientas de AWS desarrollo para acceder a AWS los servicios mediante programación.

### Microsoft Active Directory, sesiones interactivas para el usuario y sesiones ampliadas para Kiro

Si usa Microsoft Active Directory (AD) como fuente de identidad y configura la duración de la sesión para las sesiones interactivas de usuario o las sesiones extendidas para Kiro, tenga en cuenta las siguientes consideraciones.

### Note

Estas consideraciones no se aplican a las sesiones de usuario en segundo plano.



Ya sea que utilice AD Connector AWS Managed Microsoft AD o esté configurado en AWS Directory Service, la vida útil máxima de los tickets de Kerberos de usuario definidos en Microsoft AD puede afectar al tiempo de validez de las sesiones interactivas de usuario y las sesiones prolongadas de Kiro. Para obtener más información acerca de esta configuración, consulte [Duración máxima del ticket de usuario](#) en el sitio web de Microsoft.

- **AWS Managed Microsoft AD:** Si se utiliza AWS Managed Microsoft AD configurado en AWS Directory Service, la duración máxima de los tickets de Kerberos de usuario se fija en 10 horas. Por lo tanto, la duración de la sesión interactiva del usuario se establece en 10 horas o menos, entre la configuración del Centro de Identidad de IAM. Por ejemplo, si establece la duración de la sesión interactiva del usuario en 12 horas, los usuarios deberán volver a autenticarse en el portal de AWS acceso después de 10 horas. El mismo límite de 10 horas se aplica a las sesiones prolongadas de Kiro.
- **Conector AD:** si utiliza un conector AD configurado en AWS Directory Service, la vida útil máxima de los tickets de Kerberos de los usuarios se define en Microsoft AD detrás del conector AD. El valor predeterminado es de 10 horas y tiene el mismo efecto en las sesiones interactivas y prolongadas de los usuarios que en las sesiones prolongadas. AWS Managed Microsoft AD Aunque este límite se puede configurar en Microsoft AD, le recomendamos que trabaje con su administrador de TI para tener en cuenta los riesgos, especialmente porque esta configuración puede afectar a la duración de la sesión de otras aplicaciones cliente de Microsoft AD.

## Proveedores de identidad externos, sesiones interactivas para el usuario y sesiones ampliadas para Kiro

Si utiliza un proveedor de identidad (IdP) externo y configura la duración de la sesión para las sesiones interactivas de usuario o las sesiones extendidas para Kiro, tenga en cuenta las siguientes consideraciones.

### Note

Estas consideraciones no se aplican a las sesiones de usuario en segundo plano.

IAM Identity Center utiliza los atributos de `SessionNotOnOrAfter` de las aserciones de SAML para ayudar a determinar durante cuánto tiempo puede ser válida la sesión.

- Si `SessionNotOnOrAfter` se incluye en una afirmación de SAML, la duración de una sesión del portal de AWS acceso (interactiva para el usuario) y de una sesión extendida no se ve afectada por la duración de la sesión de IdP externa. Por ejemplo, si la duración de su sesión de IdP es de 24 horas y ha establecido una duración de sesión de 18 horas en el Centro de identidad de IAM, sus usuarios deberán volver a autenticarse en el AWS portal de acceso después de 18 horas. Del mismo modo, si estableces una sesión prolongada de 90 días para Kiro, tus usuarios de Kiro deberán volver a autenticarse después de 90 días.
- Si `SessionNotOnOrAfter` se incluye en una afirmación de SAML, el valor de duración de la sesión se establece en la duración más corta de la sesión del portal de AWS acceso (interactiva para el usuario) o de la sesión extendida y la duración de la sesión del IdP de SAML. Si establece una duración de sesión de 72 horas en el Centro de identidades de IAM y su IdP tiene una duración de sesión de 18 horas, sus usuarios tendrán acceso a los AWS recursos durante las 18 horas definidas en su IdP. Del mismo modo, si estableces una sesión prolongada de 90 días para Kiro, tus usuarios de Kiro deberán volver a autenticarse en Kiro al cabo de 18 horas.
- Si la duración de la sesión de su IdP es superior a la establecida en IAM Identity Center, sus usuarios podrán iniciar una nueva sesión en IAM Identity Center sin tener que volver a introducir sus credenciales, en función de la sesión de inicio de sesión aún válida con su IdP.

## AWS CLI y sesiones de SDK

Si utiliza la AWS CLI u otras herramientas de AWS desarrollo para acceder a AWS los servicios mediante programación, se deben cumplir los siguientes requisitos previos para establecer la duración de la sesión para el portal de AWS acceso y las AWS aplicaciones administradas. AWS SDKs

- Debe [configurar la duración de la sesión del portal de AWS acceso](#) en la consola de IAM Identity Center.
- Debe definir un perfil para la configuración de inicio de sesión único en su archivo de configuración compartido AWS . Este perfil se utiliza para conectarse al portal de AWS acceso. Le recomendamos que utilice la configuración del proveedor de tokens de SSO. Con esta configuración, el AWS SDK o la herramienta pueden recuperar automáticamente los tokens de autenticación actualizados. Para obtener más información, consulte [Configuración del proveedor de tokens de SSO](#) en la Guía de referencia de los SDK y las herramientas de AWS .
- Los usuarios deben ejecutar una versión del SDK AWS CLI o una versión que sea compatible con la administración de sesiones.

## Versiones mínimas de las AWS CLI que admiten la administración de sesiones

Las siguientes son las versiones mínimas de las AWS CLI que admiten la administración de sesiones.

- AWS CLI V2 2.9 o posterior
- AWS CLI V1 1.27.10 o posterior

### Note

Para los casos de uso de acceso a cuentas, si sus usuarios utilizan el conjunto de permisos AWS CLI, si actualiza el conjunto de permisos justo antes de que caduque la sesión del Centro de Identidad de IAM y la duración de la sesión se establece en 20 horas, mientras que la duración del conjunto de permisos se establece en 12 horas, la AWS CLI sesión dura un máximo de 20 horas más 12 horas para un total de 32 horas. Para obtener más información sobre la CLI de IAM Identity Center, consulte [Referencia de comandos de la AWS CLI](#).

Sus versiones mínimas SDKs admiten la administración de sesiones de IAM Identity Center

Las siguientes son las versiones mínimas de las SDKs que admiten la gestión de sesiones del IAM Identity Center.

| SDK     | Versión mínima                                                                                  |
|---------|-------------------------------------------------------------------------------------------------|
| Python  | 1.26.10                                                                                         |
| PHP     | 3,245.0                                                                                         |
| Ruby    | aws-sdk-core 3.167,0                                                                            |
| Java V2 | AWS SDK para Java v2 (2.18.13)                                                                  |
| Go V2   | SDK completo: versión 11/11/2022 y módulos Go específicos: 1.18.0 credentials/v1.13.0, config/v |
| JS V2   | 2.1253.0                                                                                        |

| SDK   | Versión mínima |
|-------|----------------|
| JS V3 | v3.210.0       |
| C++   | 1.9.372        |
| .NET  | v3.7.400.0     |

## Deshabilite el acceso de los usuarios Cuentas de AWS y las aplicaciones en el Centro de Identidad de IAM

Cuando deshabilita un acceso de usuario en su directorio IAM Identity Center, no puede editar sus detalles de usuario, restablecer su contraseña, añadir el usuario a un grupo ni ver los grupos a los que pertenece. Al deshabilitar el acceso de los usuarios, estos no podrán iniciar sesión en el portal de AWS acceso y dejarán de tener acceso a sus aplicaciones Cuentas de AWS y aplicaciones asignadas. Utilice la opción de deshabilitar el acceso de los usuarios para eliminar el acceso temporal cuando sea posible que necesite restaurarlo más adelante.

Siga el procedimiento que se detalla a continuación para deshabilitar el acceso de los usuarios al directorio de Identity Center mediante la consola de IAM Identity Center.

### Note

Si deshabilita el acceso de un usuario o lo elimina en el Centro de identidad de IAM, se impedirá inmediatamente a ese usuario iniciar sesión en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión. Para obtener más información, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

### Cómo inhabilitar el acceso de usuarios de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).

### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales

de usuario de IAM. Si busca instrucciones sobre cómo deshabilitar en IAM, consulte [Administrar usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

2. Seleccione Usuarios.
3. Seleccione el nombre de usuario del usuario cuyo acceso desee deshabilitar.
4. Debajo del nombre de usuario de la persona cuyo acceso desee inhabilitar, en la sección Información general, elija Inhabilitar el acceso del usuario.
5. En el cuadro de diálogo Desactivar el acceso de usuarios, seleccione Desactivar el acceso de usuarios.

## Denegación de acceso a los usuarios con las políticas de control de servicios

Para denegar inmediatamente el acceso y realizar llamadas a la API autorizadas cuando se deshabilita el acceso de un usuario de IAM Identity Center o se elimina al usuario, puede hacer lo siguiente:

1. [Añadir o actualizar](#) la [política insertada](#) de los conjuntos de permisos asignados al usuario añadiendo un efecto explícito Deny para todas las acciones que se realicen en todos los recursos.
2. Especifique la clave de condición `aws:userid` o `identitystore:userid`.

Como alternativa, puede utilizar una [Política de control de servicios](#) para denegarle el acceso del usuario a todas las cuentas de miembros de la organización.

### Example SCP de ejemplo para denegar el acceso

Esta política de denegación bloquea todas AWS las acciones de un usuario específico, independientemente de los demás permisos que se le hayan concedido en otros lugares. Esta política anula cualquier política de Allow.

### JSON

```
{  
  "Version": "2012-10-17",  
  "Statement" : [  
    {  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "aws:iam:*",  
      "Resource": "*" }  
    ]  
}
```

```
{
  "Effect": "Deny",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:UserId": "*:deleteduser@domain.com"
    }
  }
}
```

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

## Administración del acceso para usuarios en el directorio de Identity Center

Aprenda a administrar contraseñas y la autenticación multifactor (MFA) para los usuarios en el directorio de IAM Identity Center. Estas funciones de seguridad ayudan a proteger las cuentas de los usuarios.

 Note

Estas funciones no se aplican a los usuarios de Active Directory ni a los usuarios de proveedores de identidad externos.

Los administradores pueden administrar tanto las contraseñas como la MFA a través de la consola de IAM Identity Center. Estas funciones de seguridad solo funcionan con el directorio de Identity Center integrado.

## Administración de contraseñas

La administración de contraseñas incluye las siguientes capacidades:

- Restablezca las contraseñas con instrucciones por correo electrónico
- Generar contraseñas de un solo uso
- Configure la verificación automática del correo electrónico para los usuarios creados por la API

AWS impone requisitos de seguridad fijos, incluidas las reglas de complejidad y las restricciones de reutilización de contraseñas.

## MFA

La MFA está habilitada de forma predeterminada y admite hasta ocho dispositivos por usuario.

Los tipos de dispositivos admitidos incluyen los siguientes:

- Aplicaciones de autenticación
- Claves de seguridad
- Autenticadores biométricos integrados

Los administradores pueden registrar y administrar los dispositivos MFA para los usuarios.

### Temas

- [Configuración de contraseñas de usuario](#)
- [MFA para usuarios de Identity Center](#)

## Configuración de contraseñas de usuario

En el caso de los usuarios creados en el directorio de Identity Center, los administradores pueden administrar las políticas de contraseñas, gestionar los usuarios sin contraseñas iniciales y restablecer las contraseñas cuando sea necesario. Estas funciones de administración de contraseñas se aplican únicamente a los usuarios del directorio de Identity Center integrado. Si utiliza Active Directory o un proveedor de identidades externo, debe administrar las contraseñas en esos sistemas.

### Opciones de administración de contraseñas

- **Requisitos de contraseña:** requisitos de seguridad que los usuarios deben cumplir al configurar o cambiar las contraseñas. Esto incluye reglas de complejidad y restricciones de reutilización.
- **Configuración de contraseña de un solo uso:** configure la verificación del correo electrónico para los usuarios creados mediante la API o la CLI que no tienen contraseñas iniciales. También puede generar contraseñas temporales para un acceso inmediato.
- **Restablecimiento de contraseñas:** restablezca las contraseñas para usuarios que están bloqueados o que necesitan credenciales nuevas. Puede enviar instrucciones de restablecimiento por correo electrónico o generar contraseñas de un solo uso.

### Temas

- [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#)
- [Envío por correo electrónico de una contraseña de un solo uso a los usuarios creados con la API o la CLI](#)
- [Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final](#)

## Requisitos de contraseñas para administrar identidades en IAM Identity Center

### Note

Estos requisitos se aplican únicamente a los usuarios creados en el directorio de Identity Center. Si ha configurado una fuente de identidad distinta de IAM Identity Center para la autenticación, como [Active Directory](#) o un [proveedor de identidad externo](#), las políticas de contraseñas para sus usuarios se definen y aplican en esos sistemas, no en IAM Identity Center. Si su fuente de identidad es AWS Managed Microsoft AD, consulte [Administrar las políticas de contraseñas AWS Managed Microsoft AD para](#) obtener más información.



Al utilizar IAM Identity Center como fuente de identidad, los usuarios deben cumplir los siguientes requisitos de contraseña para establecer o cambiar su contraseña:

- Las contraseñas distinguen entre mayúsculas y minúsculas.
- Las contraseñas deben tener una longitud de entre 8 y 64 caracteres.
- También deben contener al menos un carácter de cada una de las siguientes cuatro categorías:
  - Letras minúsculas (a-z)
  - Letras mayúsculas (A-Z)
  - Números (0-9)
  - Caracteres no alfanuméricos (~!@#\$%^&\*\_-+=`|\\(){}[]:;'"<>,.?/)
- Las tres últimas contraseñas no se pueden volver a utilizar.
- No se pueden usar contraseñas que se conozcan públicamente a través de un conjunto de datos que haya obtenido cualquier tercero mediante una filtración de datos.

Envío por correo electrónico de una contraseña de un solo uso a los usuarios creados con la API o la CLI

Cuando crea usuarios con la operación de la API [CreateUser](#) o el comando de la CLI `create-user`, los usuarios no tienen contraseñas. Puede actualizar la configuración de IAM Identity Center para enviar a estos usuarios un correo electrónico de verificación después de que intenten iniciar sesión por primera vez, si especificó un correo electrónico para el usuario cuando se creó. Cuando un usuario recibe el correo electrónico de verificación, debe establecer una nueva contraseña para iniciar sesión.

Si no habilita esta configuración, debe [generar y compartir una contraseña de un solo uso](#) con los usuarios que cree mediante la API `CreateUser` o el comando de la CLI `create-user`.

Cómo enviar un correo electrónico de verificación de dirección de correo electrónico a los usuarios creados con la API `CreateUser` o el comando de la CLI **`create-user`**

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación estándar, seleccione Configurar.

5. En el cuadro de diálogo Configurar la autenticación estándar, active la casilla Enviar correo electrónico OTP. A continuación, elija Guardar. El estado pasa de Deshabilitado a Habilitado.

## Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final

Este procedimiento es para los administradores que necesitan restablecer la contraseña de un usuario del directorio de IAM Identity Center. Utilizará la consola de IAM Identity Center para restablecer las contraseñas.

### Consideraciones sobre los proveedores de identidad y los tipos de usuario

- Microsoft Active Directory o un proveedor externo: si va a conectar IAM Identity Center a Microsoft Active Directory o a un proveedor externo, las contraseñas de usuario se deben restablecer desde Active Directory o desde el proveedor externo. Esto significa que las contraseñas de esos usuarios no se pueden restablecer desde la consola de IAM Identity Center.
- Usuarios del directorio de IAM Identity Center: si es usuario de IAM Identity Center, puede restablecer su propia contraseña de IAM Identity Center. Para ello, consulte [Restablecer la contraseña de usuario del portal de AWS acceso](#).

### Cómo restablecer la contraseña de un usuario final de IAM Identity Center

#### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo cambiar contraseñas para usuarios de IAM, consulte [Administración de contraseñas para usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Elija el nombre del usuario cuya contraseña desea restablecer.
4. En la página de detalles del usuario, vaya a la pestaña Restablecer contraseña.

5. En el cuadro de diálogo Restablecer contraseña, seleccione una de las siguientes opciones y después elija Restablecer contraseña:

- a. Enviar un correo electrónico al usuario con instrucciones para restablecer la contraseña: esta opción envía automáticamente al usuario una dirección de correo electrónico de Amazon Web Services que le explica cómo restablecer su contraseña.

 Warning

Como práctica recomendada de seguridad, compruebe que la dirección de correo electrónico de este usuario sea correcta antes de seleccionar esta opción. Si este correo electrónico de restablecimiento de contraseña se enviara a una dirección de correo electrónico incorrecta o mal configurada, un destinatario malintencionado podría usarlo para obtener acceso no autorizado a su AWS entorno.

- b. Generar una contraseña de un solo uso y compartirla con el usuario: esta opción le proporcionará los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico.

## MFA para usuarios de Identity Center

 Important

Actualmente, los [proveedores de identidad externos](#) no admiten la MFA en IAM Identity Center.

IAM Identity Center viene preconfigurado con la autenticación multifactor (MFA) activada de forma predeterminada, de modo que todos los usuarios deben iniciar sesión con la MFA además de su nombre de usuario y contraseña. Esto garantiza que los usuarios deban iniciar sesión en el portal de AWS acceso mediante los dos factores siguientes:

- Su nombre de usuario y contraseña. Este es el primer factor y es un elemento que los usuarios saben.
- Ya sea un código, una clave de seguridad o datos biométricos. Este es el segundo factor y es un elemento que los usuarios tienen (posesión) o son (biométrico). El segundo factor puede ser un

código de autenticación generado desde su dispositivo móvil, una clave de seguridad conectada a su ordenador o el escaneo biométrico del usuario.

En conjunto, estos múltiples factores proporcionan una mayor seguridad al impedir el acceso no autorizado a sus AWS recursos, a menos que se haya completado correctamente una impugnación de MFA válida.

Cada usuario puede registrar hasta 2 aplicaciones de autenticación virtual, que son aplicaciones de autenticación de contraseñas de un solo uso instaladas en su dispositivo móvil o tableta, y 6 autenticadores FIDO, que incluyen autenticadores y claves de seguridad integrados, para un total de 8 dispositivos MFA. Obtener más información sobre [Tipos de MFA disponibles para IAM Identity Center](#).

## Temas

- [Tipos de MFA disponibles para IAM Identity Center](#)
- [Configuración de la MFA en IAM Identity Center](#)
- [Registre un dispositivo MFA para usuarios](#)
- [Cambiar el nombre y eliminar dispositivos MFA en IAM Identity Center](#)

## Tipos de MFA disponibles para IAM Identity Center

La autenticación multifactor (MFA) es un mecanismo simple y eficaz para mejorar la seguridad de los usuarios. El primer factor del usuario, su contraseña, es un secreto que debe memorizar, también conocido como factor de conocimiento. Otros factores pueden ser factores de posesión (algo que posea, como una clave de seguridad) o factores inherentes (algo que sea suyo y solo suyo, como un escaneo biométrico). Se recomienda encarecidamente que configure una MFA para agregar una capa adicional para la seguridad de su cuenta.

La MFA de IAM Identity Center admite los siguientes tipos de dispositivos: Todos los tipos de MFA se admiten tanto para el acceso a la consola desde un navegador como para el uso de la AWS CLI versión 2 con IAM Identity Center.

- [FIDO2 autenticadores](#), incluidos los autenticadores y las claves de seguridad integrados
- [Aplicaciones de autenticación virtual](#)
- Su propia implementación conectada a través de [MFA en RADIUS](#) AWS Managed Microsoft AD

Un usuario puede tener hasta 8 dispositivos MFA, que incluyen hasta 2 aplicaciones de autenticación virtual y 6 autenticadores FIDO, registrados en una Cuenta de AWS. También puede configurar los ajustes de MFA para que requieran la MFA siempre que se intente iniciar sesión desde un nuevo dispositivo o navegador, o cuando inicien sesión desde una dirección IP desconocida. Para obtener más información acerca de cómo configurar los ajustes de MFA para sus usuarios, consulte [Elegir tipos de MFA para la autenticación de usuarios](#) y [Configurar la aplicación de dispositivos MFA](#).

## FIDO2 autenticadores

[FIDO2](#) es un estándar que incluye CTAP2 [WebAuthn](#) y se basa en la criptografía de clave pública. Las credenciales FIDO son eficaces ante intentos de suplantación de identidad porque son exclusivas del sitio web en el que se crearon, por ejemplo AWS.

AWS admite los dos factores de forma más comunes para los autenticadores FIDO: los autenticadores integrados y las claves de seguridad. Consulte la sección que aparece a continuación para obtener más información sobre los tipos más comunes de autenticadores FIDO.

### Temas

- [Autenticadores integrados](#)
- [Claves de seguridad](#)
- [Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO](#)

## Autenticadores integrados

Algunos ordenadores y teléfonos móviles actuales tienen autenticadores integrados, como el TouchID del MacBook o una cámara compatible con Windows Hello. Si su dispositivo tiene un autenticador integrado compatible con FIDO, puede usar su huella digital, su rostro o el PIN del dispositivo como segundo factor.

## Claves de seguridad

Las llaves de seguridad son autenticadores de hardware externos compatibles con FIDO que puede comprar y conectar a su dispositivo a través de USB, BLE o NFC. Cuando se le pida la MFA, solo tiene que realizar un gesto con el sensor de la tecla. Algunos ejemplos de claves de seguridad incluyen las claves feitianas, YubiKeys y las claves de seguridad más comunes crean credenciales FIDO vinculadas al dispositivo. Para obtener una lista de todas las llaves de seguridad certificadas por FIDO, consulte los [productos certificados por FIDO](#).

## Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO

Existen varios proveedores externos que admiten la autenticación FIDO en las aplicaciones móviles, como características disponibles en administradores de contraseñas, tarjetas inteligentes con modo FIDO y otros formatos. Estos dispositivos compatibles con FIDO pueden funcionar con IAM Identity Center, pero le recomendamos que pruebe usted mismo un autenticador FIDO antes de activar esta opción como MFA.

### Note

Algunos autenticadores FIDO pueden crear credenciales FIDO reconocibles, conocidas como claves de acceso. Las claves de acceso pueden estar vinculadas al dispositivo que las crea o pueden sincronizarse y guardarse copias de seguridad en una nube. Por ejemplo, se puede registrar una clave de acceso con el Apple Touch ID en un MacBook compatible y, a continuación, iniciar sesión en un sitio desde un portátil Windows con Google Chrome con la clave de acceso en iCloud siguiendo las instrucciones que aparecen en pantalla al iniciar sesión. Para obtener más información sobre qué dispositivos admiten claves de acceso sincronizables y la interoperabilidad actual de claves entre sistemas operativos y navegadores, consulte [Asistencia para dispositivos](#) en [passkeys.dev](https://passkeys.dev), un recurso proporcionado por la Alianza FIDO y el Consorcio World Wide Web (W3C).

## Aplicaciones de autenticación virtual

Las aplicaciones de autenticación son autenticadores de terceros basados en contraseñas de un solo uso (OTP). Puede utilizar una aplicación de autenticación instalada en su dispositivo móvil o tableta como dispositivo MFA autorizado. La aplicación de autenticación de terceros debe cumplir con RFC 6238, que es un algoritmo de contraseña temporal de un solo uso (TOTP) basado en estándares y capaz de generar códigos de autenticación de seis dígitos.

Cuando se le pida la MFA, el usuario debe introducir un código válido de su aplicación de autenticación en el cuadro de entrada que aparece. Cada dispositivo MFA asignado a un usuario debe ser único. Se pueden registrar dos aplicaciones de autenticación para un usuario determinado.

## Aplicaciones de autenticación probada

Cualquier aplicación compatible con TOTP funcionará con la MFA de IAM Identity Center. La siguiente tabla muestra las aplicaciones de autenticación de terceros conocidas que puede elegir.

| Sistema operativo | Aplicación de autenticación probada                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Android           | <a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a> |
| iOS               | <a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a> |

## MFA en RADIUS

El [servicio de autenticación remota para usuarios por acceso telefónico \(RADIUS\)](#) es un protocolo cliente-servidor estándar del sector que proporciona administración de autenticación, autorización y contabilidad para que los usuarios puedan conectarse a los servicios de red. Directory Service incluye un cliente RADIUS que se conecta al servidor RADIUS en el que ha implementado la solución de MFA. Para obtener más información, consulte [Activar autenticación multifactor de AWS Managed Microsoft AD](#).

Puede utilizar MFA en RADIUS o MFA en IAM Identity Center para los inicios de sesión de los usuarios en el portal de usuarios, pero no en ambos. La MFA en IAM Identity Center es una alternativa a la MFA RADIUS en los casos en que desee una autenticación AWS nativa de dos factores para acceder al portal.

Al habilitar la MFA en IAM Identity Center, los usuarios necesitan un dispositivo de MFA para iniciar sesión en el portal de acceso AWS. Si ya había utilizado MFA RADIUS, la activación de la MFA en IAM Identity Center anula de manera efectiva el MFA RADIUS para los usuarios que inician sesión en el portal de acceso. Sin embargo, la MFA de RADIUS sigue siendo un desafío para los usuarios cuando inician sesión en todas las demás aplicaciones con las que funcionan Directory Service, como Amazon RDS for SQL Server.

Si el MFA está deshabilitado en la consola del IAM Identity Center y ha configurado el MFA RADIUS con él, el MFA RADIUS rige el inicio de sesión en el Directory Service portal de acceso. Esto significa que IAM Identity Center recurre a la configuración de MFA en RADIUS si la MFA está deshabilitada.

## Configuración de la MFA en IAM Identity Center

Puede configurar las capacidades de autenticación multifactor (MFA) en el Centro de identidad de IAM cuando su fuente de identidad esté configurada con el almacén de identidades del Centro de

identidades de IAM AWS Managed Microsoft AD o AD Connector. Actualmente, los [proveedores de identidad externos](#) no admiten la MFA en IAM Identity Center.

Las siguientes son recomendaciones generales de MFA, en función de los ajustes de IAM Identity Center y de las preferencias organizativas.

- Se recomienda a los usuarios que registren varios autenticadores de respaldo para todos los tipos de MFA habilitados. Esta práctica puede evitar la pérdida de acceso en caso de que un dispositivo MFA se rompa o se pierda.
- No elija la opción Exigirles que proporcionen una contraseña de un solo uso enviada por correo electrónico si sus usuarios deben iniciar sesión en el portal de acceso para AWS acceder a su correo electrónico. Por ejemplo, sus usuarios podrían utilizar Microsoft 365 el portal de AWS acceso para leer su correo electrónico. En este caso, los usuarios no podrán recuperar el código de verificación ni podrán iniciar sesión en el portal de AWS acceso. Para obtener más información, consulte [Configurar la aplicación de dispositivos MFA](#).
- Si ya utiliza el MFA RADIUS con el que configuró Directory Service, no necesita habilitar el MFA en IAM Identity Center. La MFA de IAM Identity Center es una alternativa a la MFA en RADIUS para los usuarios de Microsoft Active Directory de IAM Identity Center. Para obtener más información, consulte [MFA en RADIUS](#).
- El siguiente YouTube vídeo ofrece una descripción general del Centro de identidades de MFA e IAM:

### [IAM Identity Center: Multi-factor authentication defaults for new instances](#)

#### Temas

- [Solicitar MFA a los usuarios](#)
- [Elegir tipos de MFA para la autenticación de usuarios](#)
- [Configurar la aplicación de dispositivos MFA](#)
- [Permita a los usuarios registrar sus propios dispositivos MFA](#)

#### Solicitar MFA a los usuarios

Puede seguir los siguientes pasos para determinar con qué frecuencia se solicita a los usuarios de la fuerza laboral la autenticación multifactor (MFA) cada vez que intentan iniciar sesión en el portal de acceso AWS . Antes de comenzar, le recomendamos que comprenda los [Tipos de MFA disponibles para IAM Identity Center](#).



 Important

Las instrucciones figuran en esta sección aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo desactivar la MFA para los usuarios de IAM, consulte [Desactivación de dispositivos de MFA](#) en la Guía del usuario de AWS Identity and Access Management .

 Note

Si utiliza un IdP externo, la sección de Autenticación multifactor no estará disponible. Su IdP externo gestiona la configuración de MFA en lugar de IAM Identity Center.

Para configurar la MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Solicitar MFA a los usuarios, elija uno de los siguientes modos de autenticación en función del nivel de seguridad que necesite su empresa:

- Cada vez que inician sesión (siempre activo)

En este modo (la configuración predeterminada), IAM Identity Center requiere que se pregunte a los usuarios con un dispositivo MFA registrado cada vez que inicien sesión. Esta es la configuración más segura y garantiza que se apliquen las políticas organizativas o de cumplimiento al exigir que se utilice la MFA cada vez que inicien sesión en el portal de AWS acceso. Por ejemplo, PCI DSS recomienda encarecidamente la MFA durante cada inicio de sesión para acceder a las aplicaciones que admiten transacciones de pago de alto riesgo.

- Solo cuando su contexto de inicio de sesión cambie (en función del contexto)

En este modo, IAM Identity Center ofrece a los usuarios la opción de confiar en su dispositivo durante el inicio de sesión. Cuando un usuario indica que quiere confiar en un dispositivo, IAM Identity Center solicita al usuario la MFA una vez y analiza el contexto de inicio de sesión (como el dispositivo, el navegador y la ubicación) para los siguientes inicios de sesión del usuario. Para los inicios de sesión posteriores, IAM Identity Center determina si el usuario inicia sesión con un contexto en el que anteriormente se confiaba. Si el contexto de inicio de sesión del usuario cambia, IAM Identity Center solicita al usuario la MFA además de sus credenciales de dirección de correo electrónico y contraseña.

Este modo facilita su uso a los usuarios que inician sesión con frecuencia desde su lugar de trabajo, pero es menos seguro que la opción siempre activa. Solo se les solicita a los usuarios la MFA si cambia su contexto de inicio de sesión.

- Nunca (desactivado)

Mientras estén en este modo, todos los usuarios iniciarán sesión únicamente con su nombre de usuario y contraseña estándar. Al elegir esta opción, se deshabilita la MFA de IAM Identity Center, por lo que no se recomienda.

Si bien la MFA está deshabilitada en el directorio de usuarios de Identity Center, no puede administrar los dispositivos MFA en sus detalles de usuario y los usuarios del directorio de Identity Center no pueden administrar los dispositivos MFA desde el portal de acceso. AWS

 Note

Si ya utiliza el MFA RADIUS y desea seguir utilizándolo como el tipo de MFA predeterminado, puede dejar el modo de autenticación desactivado para omitir las capacidades de MFA en IAM Identity Center. Directory Service Al cambiar del modo Desactivada al modo En función del contexto o Siempre activo, se anulará la configuración de MFA en RADIUS existente. Para obtener más información, consulte [MFA en RADIUS](#).

6. Elija Save changes (Guardar cambios).

Temas relacionados

- [Elegir tipos de MFA para la autenticación de usuarios](#)
- [Configurar la aplicación de dispositivos MFA](#)

- [Permita a los usuarios registrar sus propios dispositivos MFA](#)

## Elegir tipos de MFA para la autenticación de usuarios

Utilice el siguiente procedimiento para elegir los tipos de dispositivos con los que los usuarios pueden autenticarse cuando se solicite la autenticación multifactor (MFA) en el portal de acceso. AWS

### Cómo configurar los tipos de MFA para sus usuarios

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Los usuarios pueden autenticarse con estos tipos de MFA, elija uno de los siguientes tipos de MFA en función de las necesidades de su empresa. Para obtener más información, consulte [Tipos de MFA disponibles para IAM Identity Center](#).
  - Autenticadores y claves de seguridad integrados
  - Aplicaciones de autenticación
6. Seleccione Save changes (Guardar cambios).

### Configurar la aplicación de dispositivos MFA

Siga el procedimiento que se indica a continuación para determinar si los usuarios deben tener un dispositivo MFA registrado al iniciar sesión en el portal de acceso AWS .

Para obtener información sobre MFA en IAM, consulte [AWS Autenticación multifactor en IAM](#).

### Cómo configurar la aplicación de dispositivos de MFA para sus usuarios

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.

5. En la página Configurar la autenticación multifactor, en Si un usuario aún no tiene un dispositivo MFA registrado, elija una de las siguientes opciones en función de las necesidades de su empresa:

- Exija que registren un dispositivo MFA al iniciar sesión

Esta es la configuración predeterminada al configurar MFA por primera vez para IAM Identity Center. Utilice esta opción cuando desee solicitar a los usuarios que aún no tengan un dispositivo MFA registrado que autoinscriban un dispositivo durante el inicio de sesión tras una autenticación con contraseña correcta. Esto le permite proteger los AWS entornos de su organización con MFA sin tener que inscribir y distribuir individualmente los dispositivos de autenticación a sus usuarios. Durante la inscripción automática, sus usuarios pueden registrar cualquier dispositivo de los [Tipos de MFA disponibles para IAM Identity Center](#) disponibles que haya activado anteriormente. Tras completar el registro, los usuarios tienen la opción de asignar un nombre descriptivo a su dispositivo MFA recién inscrito, tras lo cual IAM Identity Center redirige al usuario a su destino original. Si el dispositivo del usuario se pierde o se lo roban, solo tiene que eliminarlo de su cuenta y IAM Identity Center le pedirá que registre automáticamente un dispositivo nuevo la próxima vez que inicie sesión.

- Solicite que proporcionen una contraseña de un solo uso enviada por correo electrónico para iniciar sesión

Use esta opción si desea que los códigos de verificación se envíen a los usuarios por correo electrónico. Como el correo electrónico no está enlazado a un dispositivo específico, esta opción no cumple con los requisitos de autenticación multifactor estándar del sector. Sin embargo, mejora la seguridad en comparación con tener solo una contraseña. La verificación por correo electrónico solo se solicitará si el usuario no ha registrado un dispositivo MFA. Si se ha habilitado el método de autenticación Dependiente del contexto, el usuario tendrá la oportunidad de marcar el dispositivo en el que recibe el correo electrónico como de confianza. Posteriormente, no se les pedirá que verifiquen un código de correo electrónico en futuros inicios de sesión desde esa combinación de dispositivo, navegador y dirección IP.

 Note

Si utiliza Active Directory como fuente de identidad habilitada para IAM Identity Center, la dirección de correo electrónico siempre se basará en el atributo de Active Directory email. Las asignaciones personalizadas de atributos de Active Directory no anularán este comportamiento.

- Bloquear su inicio de sesión

Utilice la opción Bloquear su inicio de sesión cuando desee obligar a todos los usuarios a utilizar MFA antes de que puedan iniciar sesión en AWS.

 Important

Si el método de autenticación está configurado como En función del contexto, el usuario puede seleccionar la casilla Este es un dispositivo de confianza en la página de inicio de sesión. En ese caso, no se le solicitará la MFA a ese usuario aunque tenga habilitada la configuración Bloquear su inicio de sesión. Si desea que se les pregunte a estos usuarios, cambie el método de autenticación a Siempre activo.

- Permitirles iniciar sesión

Utilice esta opción para indicar que los dispositivos MFA no son necesarios para que los usuarios inicien sesión en el portal de AWS acceso. A los usuarios que hayan decidido registrar dispositivos MFA se les seguirá solicitando la MFA.

6. Seleccione Save changes (Guardar cambios).

Permita a los usuarios registrar sus propios dispositivos MFA

Los administradores de IAM Identity Center pueden permitir que los usuarios registren automáticamente sus propios dispositivos MFA.

Cómo permitir a los usuarios registrar sus propios dispositivos MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Quién puede administrar los dispositivos MFA, elija Los usuarios pueden agregar y administrar sus propios dispositivos MFA.
6. Seleccione Save changes (Guardar cambios).

 Note

Tras configurar el registro automático de los usuarios, es posible que desee enviarles un enlace al procedimiento de [Registro de un dispositivo para MFA](#). En este tema se proporcionan instrucciones sobre cómo configurar sus propios dispositivos de MFA.

## Registre un dispositivo MFA para usuarios

Los administradores de IAM Identity Center pueden configurar un nuevo dispositivo MFA al que pueda acceder un usuario específico en la consola de IAM Identity Center. Deben tener acceso físico al dispositivo de MFA del usuario para poder registrarlo. Por ejemplo, si configura la MFA para un usuario que use un dispositivo de MFA que se ejecute en un smartphone, necesitará acceso físico al teléfono inteligente para completar el proceso de registro. También puede permitir a los usuarios configurar y administrar sus propios dispositivos MFA. Para obtener más información, consulte [Permita a los usuarios registrar sus propios dispositivos MFA](#).

### Cómo registrar un dispositivo MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija un usuario de la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Registrar dispositivo MFA.
4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:
  - Aplicación de autenticación
    1. En la página Configurar la aplicación de autenticación, IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
    2. Con el dispositivo de MFA físico, haga lo siguiente:
      - a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#). Si la aplicación de MFA admite varias cuentas

- (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo de MFA).
- b. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación.
    - i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
    - ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

 Important

Cuando configure un dispositivo MFA para que funcione con IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudar si el usuario asignado pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA. Así evita tener que crear un nuevo dispositivo MFA en IAM Identity Center para el usuario.

3. En la página Configurar la aplicación de autenticación, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

 Important

Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA está correctamente asociado al usuario. Sin embargo, el dispositivo MFA no está sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Asignar MFA. El dispositivo MFA ahora puede empezar a generar contraseñas de un solo uso y ya está listo para usarse con ellas. AWS

- Clave de seguridad

1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

 Note

La experiencia aquí varía en función de los distintos sistemas operativos y navegadores, así que sigue las instrucciones que se muestran en su navegador o plataforma. Una vez que el dispositivo de su usuario se haya registrado correctamente, tendrá la opción de asociar un nombre descriptivo para mostrar al dispositivo recién inscrito del usuario. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar. Si ha activado la opción que permite a los usuarios gestionar sus propios dispositivos, el usuario verá este nombre descriptivo en el portal de acceso AWS .

## Cambiar el nombre y eliminar dispositivos MFA en IAM Identity Center

Los administradores de IAM Identity Center pueden utilizar los siguientes procedimientos para cambiar el nombre o eliminar el dispositivo MFA de un usuario.

### Cómo cambiar el nombre de un dispositivo de MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija el usuario en la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Cambiar nombre.
4. Cuando se le solicite, introduzca el nuevo nombre y, a continuación, seleccione Cambiar nombre.

### Para eliminar un dispositivo MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija el usuario en la lista.



3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Eliminar.
4. Elija Eliminar y luego, Eliminar para confirmar la acción.

# Configuración del acceso a las aplicaciones

Con él AWS IAM Identity Center, puede controlar quién puede tener acceso mediante un inicio de sesión único a sus aplicaciones. Los usuarios obtienen acceso estable a estas aplicaciones en cuanto usan las credenciales de directorio para iniciar sesión.

IAM Identity Center se comunica de forma segura con estas aplicaciones a través de una relación de confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta confianza se puede crear de diferentes maneras, según el tipo de aplicación.

IAM Identity Center admite dos tipos de aplicaciones: aplicaciones administradas y [aplicaciones AWS administradas por el cliente](#). AWS las aplicaciones gestionadas se configuran directamente desde las consolas de aplicaciones correspondientes o a través de la aplicación APIs. Debe agregar las aplicaciones administradas por el cliente a la consola de IAM Identity Center y configurarlas con los metadatos correspondientes tanto para IAM Identity Center como para el proveedor de servicios.

Tras configurar las aplicaciones para que funcionen con IAM Identity Center, puede administrar los usuarios o grupos que acceden a las aplicaciones. De forma predeterminada, no hay ningún usuario asignado a las aplicaciones.

También puede conceder a sus empleados el Consola de administración de AWS acceso a una instancia específica Cuenta de AWS de su organización. Para obtener más información, consulte [Configurar el acceso a Cuentas de AWS](#).

## Temas

- [AWS aplicaciones gestionadas](#)
- [Aplicaciones administradas por el cliente](#)
- [Descripción general de la propagación de identidades de confianza](#)
- [Cómo configurar su propia aplicación OAuth 2.0](#)
- [Rotación de certificados de IAM Identity Center](#)
- [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#)
- [Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center](#)
- [Eliminar el acceso de los usuarios a las aplicaciones de SAML 2.0](#)
- [Asignación de atributos de su aplicación con atributos de IAM Identity Center](#)

# AWS aplicaciones gestionadas

AWS IAM Identity Center agiliza y simplifica la tarea de conectar a los usuarios de su fuerza laboral con aplicaciones AWS gestionadas como Kiro y Amazon Quick. Con IAM Identity Center, puede conectar su proveedor de identidades existente una vez y sincronizar usuarios y grupos de su directorio, o crear y administrar sus usuarios directamente en IAM Identity Center. Al proporcionar un punto de federación, IAM Identity Center elimina la necesidad de configurar la federación o la sincronización de usuarios y grupos para cada aplicación y reduce el esfuerzo administrativo. También obtiene una [visión común de las asignaciones de usuarios y grupos](#).

Para ver una tabla de AWS aplicaciones que funcionan con IAM Identity Center, consulte. [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#)

## Controlar el acceso a las aplicaciones AWS gestionadas

El acceso a las aplicaciones AWS gestionadas se controla de dos maneras:

- Entrada inicial a la aplicación

IAM Identity Center administra esto mediante asignaciones a la aplicación. De forma predeterminada, las asignaciones son obligatorias para las aplicaciones AWS administradas. Si es administrador de aplicaciones, puede elegir si desea solicitar asignaciones a una aplicación.

Si las asignaciones son obligatorias, cuando un usuario inicie sesión en Portal de acceso a AWS, solo verá el icono de la aplicación si está asignado a la aplicación directamente o mediante una asignación de grupo.

Si las asignaciones no son obligatorias, puede permitir que todos los usuarios de IAM Identity Center entren en la aplicación. En este caso, la aplicación administra el acceso a los recursos y todos los usuarios que visitan Portal de acceso a AWS.

### Important

Si es administrador del IAM Identity Center, puede utilizar la consola del IAM Identity Center para eliminar las asignaciones a las aplicaciones AWS gestionadas. Antes de eliminar las asignaciones, le recomendamos que colabore con el administrador de la aplicación. También debe colaborar con el administrador de la aplicación si tiene previsto modificar la configuración que determina si las asignaciones son obligatorias o automatizar las asignaciones de la aplicación.

- Acceso a los recursos de la aplicación

La aplicación administra esto mediante asignaciones de recursos independientes que controla.

AWS las aplicaciones gestionadas proporcionan una interfaz de usuario administrativa que puede utilizar para gestionar el acceso a los recursos de la aplicación. Por ejemplo, los administradores de Quick pueden asignar a los usuarios el acceso a los paneles en función de la pertenencia a un grupo. La mayoría de las aplicaciones AWS administradas también ofrecen una Consola de administración de AWS experiencia que permite asignar usuarios a la aplicación. La experiencia de la consola de estas aplicaciones podría integrar ambas funciones para combinar las capacidades de asignación de usuarios con la capacidad de administrar el acceso a los recursos de la aplicación.

## Compartición de información de identidad

### Consideraciones para compartir información de identidad en Cuentas de AWS

IAM Identity Center admite los atributos más utilizados en todas las aplicaciones. Estos atributos pueden ser el nombre y apellido, el número de teléfono, la dirección de correo electrónico, la dirección y el idioma preferido. Considere detenidamente qué aplicaciones y qué cuentas pueden utilizar esta información de identificación personal.

Puede controlar el acceso a esta información de cualquiera de las siguientes maneras:

- Puede optar por habilitar el acceso solo en la cuenta AWS Organizations de administración o en todas las cuentas de AWS Organizations.
- Como alternativa, puede usar las políticas de control de servicios (SCPs) para controlar qué aplicaciones pueden acceder a la información en qué cuentas se encuentran AWS Organizations.

Por ejemplo, si solo habilita el acceso a la cuenta AWS Organizations de administración, las aplicaciones de las cuentas de los miembros no tendrán acceso a la información. Sin embargo, si habilita el acceso en todas las cuentas, puede impedir SCPs el acceso a todas las aplicaciones, excepto a las que desee permitir.

Las políticas de control de servicios son una característica de AWS Organizations. Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

## Configuración de IAM Identity Center para compartir información de las identidades

IAM Identity Center proporciona un almacén de identidades que contiene los atributos de usuario y grupo, sin incluir las credenciales de inicio de sesión. Puede utilizar cualquiera de los siguientes métodos para mantener actualizados a los usuarios y grupos de su almacén de identidades de IAM Identity Center:

- Utilice el almacén de identidades de IAM Identity Center como fuente de identidades principal. Si elige este método, gestiona los usuarios, sus credenciales de inicio de sesión y los grupos desde la consola de IAM Identity Center o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Administración de usuarios en el directorio de Identity Center](#).
- Configure el aprovisionamiento (sincronización) de los usuarios y grupos procedentes de cualquiera de las siguientes fuentes de identidad en el almacén de identidades de IAM Identity Center:
  - Active Directory: para más información, consulte [Directorio Microsoft AD](#).
  - Proveedor de identidades externo: para más información, consulte [Proveedores de identidades externos](#).

Si elige este método de aprovisionamiento, seguirá administrando sus usuarios y grupos desde su origen de identidad y esos cambios se sincronizarán con el almacén de identidades de IAM Identity Center.

Sea cual sea la fuente de identidad que elija, el Centro de Identidad de IAM puede compartir la información del usuario y del grupo con AWS las aplicaciones gestionadas. De esta forma, puede conectar un origen de identidad a IAM Identity Center una vez y, a continuación, compartir la información de identidad con varias aplicaciones en la Nube de AWS. De este modo, se elimina la necesidad de configurar el aprovisionamiento de identidades y federaciones de forma independiente con cada aplicación. Esta característica de uso compartido también facilita el acceso de los usuarios a muchas aplicaciones en diferentes Cuentas de AWS.

## Restringir el uso de aplicaciones gestionadas AWS

Cuando habilita IAM Identity Center por primera vez, estará disponible como origen de identidad para las aplicaciones administradas por AWS en todas sus cuentas de AWS Organizations. Para restringir las aplicaciones, debe implementar políticas de control de servicios (SCPs). SCPs son una función AWS Organizations que puede utilizar para controlar de forma centralizada el número máximo de permisos que pueden tener las identidades (usuarios y roles) de su organización. Puede utilizarlas

SCPs para bloquear el acceso a la información de usuarios y grupos del Centro de Identidad de IAM e impedir que se inicie la aplicación, excepto en las cuentas designadas. Para obtener más información, consulte [las políticas de control de servicios \(SCPs\)](#) en la Guía del AWS Organizations usuario.

El siguiente ejemplo de SCP bloquea el acceso a la información de usuarios y grupos de IAM Identity Center e impide que se inicie la aplicación, excepto en las cuentas designadas (111111111111 y 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

## AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center

IAM Identity Center le permite conectar su origen de identidad existente o crear usuarios una sola vez. Esto permite a los administradores de aplicaciones gestionar el acceso a las siguientes aplicaciones AWS gestionadas sin necesidad de una federación independiente ni una sincronización de usuarios y grupos independientes.

Todas las aplicaciones AWS gestionadas de la siguiente tabla se integran con las [instancias organizativas del IAM Identity Center](#). La tabla también proporciona información sobre lo siguiente para una aplicación AWS gestionada compatible:

- Si la aplicación también se integra con instancias de cuenta de IAM Identity Center

- Si la aplicación puede permitir una propagación de identidades de confianza a través de IAM Identity Center
- Si la aplicación es compatible con IAM Identity Center configurado con una clave de KMS administrada por el cliente
- Si la aplicación admite el despliegue en otras regiones del Centro de Identidad de IAM

 Note

Las aplicaciones que admiten el despliegue en otras regiones del Centro de Identidad de IAM también admiten el Centro de Identidad de IAM configurado con una clave KMS administrada por el cliente. Todas las aplicaciones AWS gestionadas que se muestran aquí admiten el despliegue en la región principal. Para obtener más información, consulte [the section called “Implementación y administración de aplicaciones AWS administradas en múltiples Regiones de AWS”](#).

#### AWS aplicaciones gestionadas que se integran con IAM Identity Center

| AWS aplicación gestionada | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center | Es compatible con IAM Identity Center configurado con una <a href="#">clave de KMS administrada por el cliente</a> | Soporta el despliegue en <a href="#">regiones adicionales del Centro de Identidad de IAM</a> |
|---------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Amazon Athena SQL         | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon CodeCatalyst       | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon DataZone           | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |

| AWS aplicación gestionada                     | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center | Es compatible con IAM Identity Center configurado con una <a href="#">clave de KMS administrada por el cliente</a> | Soporta el despliegue en <a href="#">regiones adicionales del Centro de Identidad de IAM</a> |
|-----------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Capacidades de Amazon EKS                     | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon EMR en EC2                             | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon EMR en EKS                             | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon EMR sin servidor                       | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon EMR Studio                             | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon Kendra                                 | No                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon Managed Grafana                        | No                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon Monitron                               | No                                                                          | No                                                                                             | No                                                                                                                 | No                                                                                           |
| OpenSearch Servicio Amazon                    | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| OpenSearch Servicio Amazon Serverless Service | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |



| AWS aplicación gestionada        | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center | Es compatible con IAM Identity Center configurado con una <a href="#">clave de KMS administrada por el cliente</a> | Soporta el despliegue en <a href="#">regiones adicionales del Centro de Identidad de IAM</a> |
|----------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Amazon Q Business                | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon Quick                     | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon Redshift                  | Sí <sup>2</sup>                                                             | Sí                                                                                             | Sí                                                                                                                 | Sí                                                                                           |
| Amazon S3 Access Grants          | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | Sí                                                                                           |
| Amazon SageMaker Studio          | No                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon SageMaker Unified Studio  | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon WorkMail                  | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon WorkSpaces                | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Amazon WorkSpaces Secure Browser | No                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| AWS App Studio                   | Sí                                                                          | No                                                                                             | No                                                                                                                 | No                                                                                           |

| AWS aplicación gestionada            | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center | Es compatible con IAM Identity Center configurado con una <a href="#">clave de KMS administrada por el cliente</a> | Soporta el despliegue en <a href="#">regiones adicionales del Centro de Identidad de IAM</a> |
|--------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| AWS Deadline Cloud                   | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | Sí                                                                                           |
| AWS Glue                             | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| AWS IoT Events                       | No                                                                          | No                                                                                             | No                                                                                                                 | No                                                                                           |
| AWS IoT SiteWise                     | No                                                                          | No                                                                                             | No                                                                                                                 | No                                                                                           |
| AWS Lake Formation                   | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | Sí                                                                                           |
| AWS re:Post Private                  | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| AWS Supply Chain                     | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| AWS Systems Manager                  | No                                                                          | No                                                                                             | Sí                                                                                                                 | Sí, escritorio remoto Fleet Manager                                                          |
| AWS Transfer Family aplicaciones web | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |

| AWS aplicación gestionada              | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center | Es compatible con IAM Identity Center configurado con una <a href="#">clave de KMS administrada por el cliente</a> | Soporta el despliegue en <a href="#">regiones adicionales del Centro de Identidad de IAM</a> |
|----------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| AWS Transformación                     | Sí                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Acceso verificado de AWS               | No                                                                          | No                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Kiro                                   | Sí <sup>1</sup>                                                             | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| Aprobación multipartita                | No                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |
| OpenSearch user interface (Dashboards) | Sí                                                                          | Sí                                                                                             | Sí                                                                                                                 | No                                                                                           |

<sup>1</sup> En el caso de Kiro, se admiten las instancias de cuenta del IAM Identity Center, a menos que los usuarios necesiten acceder al conjunto completo de funciones de Kiro en los sitios web. AWS Para obtener más información, consulte [Configuración de Kiro en la Guía del usuario de Kiro](#).

<sup>2</sup> En el caso de Amazon Redshift, se admiten las instancias de cuenta de IAM Identity Center, excepto aplicaciones como Query Editor v2, que requieren conjuntos de permisos, que no son compatibles con las instancias de cuenta.

#### Note

Algunos AWS servicios, como Amazon Connect, no AWS Client VPN aparecen en esta tabla, aunque puede utilizarlos con IAM Identity Center. Esto se debe a que se integran con el

Centro de Identidad de IAM exclusivamente mediante SAML y, por lo tanto, se clasifican como aplicaciones gestionadas por el [cliente](#).

## Inicio rápido: configuración del IAM Identity Center para probar las aplicaciones gestionadas AWS

Si su administrador aún no le ha dado acceso al Centro de identidad de IAM, puede seguir los pasos de este tema para configurar el Centro de identidades de IAM para probar AWS las aplicaciones gestionadas. Aprenderá a activar el Centro de identidad de IAM, a crear un usuario directamente en el Centro de identidades de IAM y a asignar ese usuario a una aplicación gestionada. AWS

En este tema se proporcionan pasos de inicio rápido sobre cómo habilitar IAM Identity Center de cualquiera de las siguientes maneras:

- Con AWS Organizations: si elige esta opción, se crea una instancia de organización del Centro de identidades de IAM.
- Solo en su entorno específico Cuenta de AWS: si elige esta opción, se crea una instancia de cuenta del IAM Identity Center.

Para obtener información sobre los tipos de instancia, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Requisitos previos

Antes de habilitar IAM Identity Center, confirme lo siguiente:

- Tiene una Cuenta de AWS: si no la tiene Cuenta de AWS, consulte [Cómo empezar con una Cuenta de AWS](#) en la Guía de referencia sobre la gestión de AWS cuentas.
- La aplicación AWS gestionada funciona con el Centro de identidades de IAM: consulte la lista [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#) para confirmar que la aplicación AWS gestionada que desea probar funciona con el Centro de identidades de IAM.
- Ha revisado las consideraciones regionales: asegúrese de que la aplicación AWS gestionada que desea probar es compatible con el Región de AWS lugar donde habilita el Centro de Identidad de IAM. Para obtener más información, consulte la documentación de la aplicación administrada por AWS .

 Note

Debe implementar la aplicación AWS gestionada en la misma región en la que planea habilitar el IAM Identity Center.

## Configuración de una instancia organizativa del IAM Identity Center para probar las aplicaciones gestionadas AWS

 Note

En este tema se describe cómo habilitar el Centro de Identidad de IAM AWS Organizations, que es la forma recomendada de habilitar el Centro de Identidad de IAM.

### Confirmación de sus permisos

Para habilitar IAM Identity Center con AWS Organizations, debe iniciar sesión en la consola de AWS administración de una de las siguientes maneras:

- Un usuario con permisos administrativos en la Cuenta de AWS donde se habilitará IAM Identity Center con AWS Organizations.
- El usuario raíz (no se recomienda a menos que no existan otros usuarios administrativos).

 Important

El usuario raíz tiene acceso a todos los AWS servicios y recursos de la cuenta. Como práctica recomendada de seguridad, a menos que no tengas otras credenciales, no utilices las credenciales raíz de tu cuenta para acceder a AWS los recursos. Estas credenciales proporcionan acceso ilimitado a la cuenta y son difíciles de revocar.

### Paso 1. Habilite IAM Identity Center con AWS Organizations

1. Realice una de estas operaciones para iniciar sesión en la Consola de administración de AWS.

- Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione el usuario root e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo AWS utilizas de forma independiente Cuenta de AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. En la página de inicio de la consola de AWS administración, seleccione el servicio IAM Identity Center o vaya a la consola de [IAM Identity Center](#).
  3. Seleccione Activar y active IAM Identity Center con. AWS Organizations Al hacerlo, está creando una [instancia de organización](#) de IAM Identity Center.

## Paso 2. Cree un usuario administrativo en IAM Identity Center

En este procedimiento, se describe cómo crear un usuario directamente en el directorio integrado de Identity Center. Este directorio no está conectado a ningún otro directorio que su administrador pueda usar para administrar los usuarios del personal. Tras crear el usuario en IAM Identity Center, especificará las nuevas credenciales para este usuario. Cuando inicie sesión como este usuario para probar su aplicación AWS gestionada, iniciará sesión con las nuevas credenciales, no con las credenciales existentes que utilice para acceder a los recursos corporativos.

### Note

Le recomendamos que utilice este método solo con fines de creación de usuarios.

1. En el panel de navegación de la consola de IAM Identity Center, elija Usuarios y, a continuación, elija Agregar usuarios.
2. Siga las instrucciones de la consola para agregar el usuario. Mantenga seleccionado Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña y asegúrese de especificar una dirección de correo electrónico a la que tenga acceso.
3. En el panel de navegación, elija Cuentas de AWS, active la casilla de verificación situada junto a su cuenta y elija Asignar usuarios o grupos.
4. Seleccione la pestaña Usuarios, active la casilla de verificación situada junto al usuario que acaba de agregar y elija Siguiente.
5. Seleccione Crear conjunto de permisos y siga las instrucciones de la consola para crear el conjunto de permisos predefinido AdministratorAccess.

6. Cuando haya terminado, el nuevo conjunto de permisos aparecerá en la lista. Cierre la pestaña Conjuntos de permisos en la ventana del navegador, vuelva a la pestaña Asignar usuarios y grupos y elija el icono de actualización situado junto a Crear conjunto de permisos.
7. En la pestaña del navegador Asignar usuarios y grupos, el nuevo conjunto de permisos aparecerá en la lista. Active la casilla de verificación situada junto al nombre del conjunto de permisos, elija Siguiente y, a continuación, elija Enviar.
8. Cierre la sesión de la consola de .

### Paso 3. Inicie sesión en el portal de AWS acceso como usuario administrativo

El portal de AWS acceso es un portal web que proporciona al usuario que ha creado acceso a la consola AWS de administración. Antes de iniciar sesión en el portal de acceso de AWS , debe aceptar la invitación para unirse a IAM Identity Center y activar sus credenciales de usuario.

1. Busque un correo electrónico con el asunto Invitación a unirse a AWS IAM Identity Center.
2. Seleccione Aceptar invitación y siga las instrucciones de la página de registro para establecer una nueva contraseña, iniciar sesión y registrar un dispositivo MFA para su usuario.
3. Después de registrar su dispositivo MFA, se abre el portal de AWS acceso.
4. En el portal de AWS acceso, seleccione el suyo Cuenta de AWS y elija AdministratorAccess. Se lo redirigirá a la Consola de administración de AWS .

### Paso 4. Configure la aplicación AWS gestionada para que utilice IAM Identity Center

1. Con la sesión iniciada en la consola AWS de administración, abra la consola de la aplicación AWS gestionada que vaya a utilizar.
2. Siga las instrucciones de la consola para configurar la aplicación AWS gestionada para que utilice IAM Identity Center. Durante este proceso, puede asignar el usuario que ha creado a la aplicación.

## Configuración de una instancia de cuenta del IAM Identity Center para probar las aplicaciones gestionadas AWS

### Note

Una instancia de cuenta es una implementación única de IAM Identity Center a una única Cuenta de AWS. Debe habilitar esta instancia al mismo tiempo Región de AWS que la AWS aplicación que desea probar.

### Confirmación de aplicación

Todas las aplicaciones AWS gestionadas que funcionan con el IAM Identity Center se pueden utilizar con las instancias organizativas del IAM Identity Center. Sin embargo, solo algunas de estas aplicaciones se pueden utilizar con instancias de cuenta de IAM Identity Center. Revise la lista de regla de [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#).

Paso 1. Habilite una instancia de cuenta de IAM Identity Center.

1. Realice una de estas operaciones para iniciar sesión en la Consola de administración de AWS.
  - Nuevo para AWS (usuario raíz): inicie sesión como propietario de la cuenta; para ello, seleccione el usuario raíz e introduzca su Cuenta de AWS dirección de correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo AWS utilizas de forma independiente Cuenta de AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. En la página de inicio de la consola de AWS administración, seleccione el servicio IAM Identity Center o vaya a la consola de [IAM](#) Identity Center.
3. Seleccione Habilitar.
4. En la página Habilitar IAM Identity Center con AWS Organizations, seleccione habilitar una instancia de cuenta de IAM Identity Center.
5. En la página Habilitar la instancia de cuenta de IAM Identity Center, revise la información y, si lo desea, añada las etiquetas que desee asociar a esta instancia de cuenta. A continuación, elija Enable.



## Paso 2. Creación de un usuario en IAM Identity Center

En este procedimiento, se describe cómo crear un usuario directamente en el directorio integrado de Identity Center. Este directorio no está conectado a ningún otro directorio que su administrador pueda usar para administrar los usuarios del personal. Tras crear el usuario en IAM Identity Center, especificará las nuevas credenciales para este usuario. Cuando inicie sesión como este usuario para probar su aplicación AWS gestionada, iniciará sesión con las nuevas credenciales. Las nuevas credenciales no le permitirán acceder a otros recursos corporativos.

### Note

Le recomendamos que utilice este método solo con fines de creación de usuarios.

1. En el panel de navegación de la consola de IAM Identity Center, elija Usuarios y, a continuación, elija Agregar usuarios.
2. Siga las instrucciones de la consola para agregar el usuario. Mantenga seleccionado Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña y asegúrese de especificar una dirección de correo electrónico a la que tenga acceso.
3. Cierre la sesión de la consola de .

## Paso 3. Inicie sesión en el portal de AWS acceso como usuario del IAM Identity Center

El portal de AWS acceso es un portal web que proporciona al usuario que creó acceso a la consola AWS de administración. Antes de iniciar sesión en el portal de acceso de AWS , debe aceptar la invitación para unirse a IAM Identity Center y activar sus credenciales de usuario.

1. Busque un correo electrónico con el asunto Invitación a unirse a AWS IAM Identity Center.
2. Seleccione Aceptar invitación y siga las instrucciones de la página de registro para establecer una nueva contraseña, iniciar sesión y registrar un dispositivo MFA para su usuario.
3. Después de registrar su dispositivo MFA, se abre el portal de AWS acceso. Cuando haya aplicaciones disponibles, las encontrará en la pestaña Aplicaciones.

 Note

AWS las aplicaciones que admiten instancias de cuentas permiten a los usuarios iniciar sesión en las aplicaciones sin necesidad de permisos adicionales. Por lo tanto, la pestaña Cuentas permanecerá vacía.

Paso 4. Configure la aplicación AWS gestionada para que utilice el Centro de identidad de IAM

1. Con la sesión iniciada en la consola AWS de administración, abra la consola de la aplicación AWS gestionada que vaya a utilizar.
2. Siga las instrucciones de la consola para configurar la aplicación AWS gestionada para que utilice IAM Identity Center. Durante este proceso, puede asignar el usuario que ha creado a la aplicación.

## Visualización y modificación de los detalles de una aplicación AWS gestionada

Tras conectar una aplicación AWS gestionada al IAM Identity Center mediante la consola o APIs para la aplicación, la aplicación se registra en el IAM Identity Center. Una vez registrada una aplicación en IAM Identity Center, puede ver y cambiar detalles sobre la aplicación en la consola de IAM Identity Center.

La información sobre la aplicación incluye si son obligatorias las asignaciones de usuarios y grupos y, si corresponde, los usuarios y grupos asignados y las aplicaciones de confianza para la propagación de identidades. Para obtener más información acerca de la propagación de identidades de confianza, consulte [Descripción general de la propagación de identidades de confianza](#).

Para ver y cambiar la información sobre una aplicación AWS gestionada en la consola del IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada de AWS .
4. Elija el enlace de la aplicación administrada que desee abrir y ver.

5. Si desea cambiar la información sobre una aplicación AWS gestionada, seleccione Acción y, a continuación, seleccione Editar detalles.
6. Puede cambiar el nombre mostrado y la descripción de la aplicación, así como el método de asignación de usuarios y grupos.
  - a. Para cambiar el nombre para mostrar, introduzca el nombre deseado en el campo Nombre para mostrar y seleccione Guardar cambios.
  - b. Para cambiar la descripción, introduzca la descripción deseada en el campo Descripción y seleccione Guardar cambios.
  - c. Para cambiar el método de asignación de usuarios y grupos, realice el cambio deseado y seleccione Guardar cambios. Para obtener más información, consulte [the section called “Usuarios, grupos y aprovisionamiento”](#).

## Deshabilitar una aplicación AWS gestionada

Para evitar que los usuarios se autenticuen en una aplicación AWS gestionada, puede inhabilitar la aplicación en la consola del IAM Identity Center.

Para deshabilitar una aplicación gestionada AWS

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la página Aplicaciones, en Aplicaciones administradas por AWS , seleccione la aplicación que desee deshabilitar.
4. Con la aplicación seleccionada, seleccione Acciones y, a continuación, seleccione Deshabilitar.
5. En el cuadro de diálogo Desactivar aplicación, seleccione Desactivar.
6. En la lista Aplicaciones administradas por AWS , el estado de la aplicación aparece como Inactiva.

### Note

Si una aplicación AWS gestionada está deshabilitada, puede restaurar la capacidad de los usuarios de autenticarse en la aplicación seleccionando Acciones y, a continuación, Activar.

## Activación de sesiones de consola con identidad mejorada

Una sesión de consola con identidad mejorada mejora la sesión de AWS consola del usuario al proporcionar un contexto de usuario adicional para personalizar la experiencia de ese usuario. Actualmente, los usuarios de Kiro Pro admiten esta función [en AWS aplicaciones y sitios web](#).

Puede habilitar sesiones de consola con una identidad mejorada sin realizar cambios en los patrones de acceso existentes ni en la federación en la consola. AWS Si sus usuarios inician sesión en la AWS consola con IAM (por ejemplo, si inician sesión como usuarios de IAM o mediante un acceso federado con IAM), pueden seguir utilizando estos métodos. Si sus usuarios inician sesión en el portal de AWS acceso, pueden seguir utilizando sus credenciales de usuario del IAM Identity Center.

### Temas

- [Requisitos y consideraciones previos](#)
- [¿Cómo habilitar las sesiones identity-enhanced-console](#)
- [Cómo funcionan las sesiones de consola con identidad mejorada](#)

### Requisitos y consideraciones previos

Antes de habilitar sesiones de consola con identidad mejorada, revise los siguientes requisitos previos y consideraciones:

- Si sus usuarios acceden a Kiro en AWS aplicaciones y sitios web a través de una suscripción a Kiro Pro, debe habilitar las sesiones de consola con identidad mejorada.

#### Note

Los usuarios de Kiro pueden acceder a Kiro sin sesiones con identidad mejorada, pero no tendrán acceso a sus suscripciones a Kiro Pro.

- Las sesiones de consola con identidad mejorada requieren una [instancia de organización](#) de IAM Identity Center.
- La integración con Kiro no es compatible si habilitas el Centro de Identidad de IAM de forma opcional. Región de AWS
- Para habilitar sesiones de consola con identidad mejorada, debe tener los siguientes permisos:
  - `sso:CreateApplication`

- `sso:GetSharedSsoConfiguration`
- `sso:ListApplications`
- `sso:PutApplicationAssignmentConfiguration`
- `sso:PutApplicationAuthenticationMethod`
- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Para permitir que sus usuarios utilicen sesiones de consola con identidad mejorada, debe concederles el permiso `sts:setContext` en virtud de una política basada en la identidad. Para más información, consulte [Concesión de permisos para usar sesiones de consola con identidad mejorada](#).

## ¿Cómo habilitar las sesiones identity-enhanced-console

Puede activar las sesiones de consola con identidad mejorada en la consola de Kiro o en la consola de IAM Identity Center.

Habilite las sesiones de consola con identidad mejorada en la consola Kiro

Antes de habilitar sesiones de consola con identidad mejorada, debe tener una instancia de organización de IAM Identity Center con un origen de identidades conectado. Si ya ha configurado IAM Identity Center, vaya al paso 3.

1. Abra la consola del IAM Identity Center. Seleccione Activar y cree una instancia de organización de IAM Identity Center. Para obtener información, consulte [Activar IAM Identity Center](#).
2. Conecte su fuente de identidad a IAM Identity Center y aprovisiona usuarios a IAM Identity Center. Puede conectar su origen de identidad actual a IAM Identity Center o utilizar el directorio del Identity Center si aún no utiliza otro origen de identidad. Para obtener más información, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#).
3. Cuando termine de configurar el Centro de identidades de IAM, abra la consola de Kiro y siga los pasos que se indican en las [suscripciones](#) de la Guía del usuario de Kiro. Asegúrese de habilitar las sesiones de consola con identidad mejorada.

 Note

Si no tiene los permisos suficientes para habilitar las sesiones de consola con identidad mejorada, es posible que tenga que pedirle a un administrador de IAM Identity Center que realice esta tarea por usted en la consola de IAM Identity Center. Para obtener más información, consulte el siguiente procedimiento.

## Habilite sesiones de consola con identidad mejorada en la consola de IAM Identity Center

Si es administrador de IAM Identity Center, es posible que otro administrador le pida que habilite sesiones de consola con identidad mejorada en la consola de IAM Identity Center.

1. Abra la consola de IAM Identity Center.
2. En el panel de navegación, seleccione Configuración.
3. En Habilitar sesiones con identidad mejorada, seleccione Habilitar.
4. En el segundo mensaje, seleccione Activar.
5. Cuando termine de habilitar las sesiones de consola con identidad mejorada, aparecerá un mensaje de confirmación en la parte superior de la página Configuración.
6. En la sección Detalles, el estado de las Sesiones con identidad mejorada es Habilitado.

## Cómo funcionan las sesiones de consola con identidad mejorada

IAM Identity Center mejora la sesión de consola actual del usuario para incluir el ID de usuario activo de IAM Identity Center y el ID de sesión de IAM Identity Center.

Las sesiones de consola con identidad mejorada incluyen los tres valores siguientes:

- ID de usuario del almacén de identidades ([almacén de identidades: UserId](#)): este valor se utiliza para identificar de forma exclusiva a un usuario en la fuente de identidad que está conectada a IAM Identity Center.
- Directorio de almacenes de identidades ARN ([almacén de identidades: IdentityStoreArn](#)): este valor es el ARN del almacén de identidades que está conectado a IAM Identity Center y en el que puede buscar los atributos para `identitystore:UserId`.
- ID de sesión del IAM Identity Center: este valor indica si la sesión del usuario en IAM Identity Center sigue siendo válida.

Los valores son los mismos, pero se obtienen de formas distintas y se añaden en distintos puntos del proceso, en función de cómo inicie sesión el usuario:

- Centro de identidad de IAM (portal de AWS acceso): en este caso, los valores de ID de usuario y ARN del almacén de identidades del usuario ya se proporcionan en la sesión activa del Centro de identidades de IAM. IAM Identity Center mejora la sesión actual al añadir únicamente el ID de sesión.
- Otros métodos de inicio de sesión: si el usuario inicia sesión en AWS como usuario de IAM, con un rol de IAM o como usuario federado con IAM, no se proporciona ninguno de estos valores. IAM Identity Center mejora la sesión actual al añadir el ID de usuario del almacén de identidades, el ARN del directorio del almacén de identidades y el ID de sesión.

## Aplicaciones administradas por el cliente

IAM Identity Center actúa como un servicio de identidades central para los usuarios y grupos de su fuerza laboral. Si ya utiliza un proveedor de identidades (IdP), IAM Identity Center puede integrarse con su IdP para que pueda aprovisionar sus usuarios y grupos en IAM Identity Center y utilizar su IdP para la autenticación. Con una sola conexión, IAM Identity Center representa su IdP frente a Servicios de AWS varios y permite que OAuth sus aplicaciones 2.0 soliciten acceso a los datos de estos servicios en nombre de sus usuarios. También puede utilizar IAM Identity Center para asignar a sus usuarios el acceso a las aplicaciones de [SAML 2.0](#). Esto incluye AWS servicios como Amazon Connect y AWS Client VPN, que se integran con IAM Identity Center exclusivamente mediante SAML y, por lo tanto, se clasifican como aplicaciones gestionadas por el cliente.

- Si su aplicación es compatible con los JSON Web Tokens (JWTs), puede utilizar la fiable función de propagación de identidades del Centro de Identidad de IAM para permitir que la aplicación solicite acceso a los datos Servicios de AWS en nombre de sus usuarios. La propagación fiable de la identidad se basa en el marco de autorización OAuth 2.0 e incluye una opción para que las aplicaciones intercambien los identificadores de identidad procedentes de un servidor de autorización OAuth 2.0 externo por símbolos emitidos por el IAM Identity Center y reconocidos por. Servicios de AWS Para obtener más información, consulte [Casos de uso de propagación de identidades de confianza](#).
- Si su aplicación es compatible con SAML 2.0, puede conectarla a una instancia [organizativa de IAM Identity Center](#). Puede utilizar IAM Identity Center para asignar acceso a su aplicación SAML 2.0.

 Note

Al integrar aplicaciones gestionadas por el cliente con una instancia del Centro de Identidad de IAM que utilice una [clave de KMS gestionada por el cliente](#), compruebe si la aplicación invoca el servicio del Centro de Identidad de IAM APIs para confirmar si la aplicación necesita permisos de clave de KMS. Siga las instrucciones para conceder permisos de clave de KMS a flujos de trabajo personalizados que figuran en las políticas clave [básicas](#) de KMS de la Guía del usuario de IAM Identity Center.

## Temas

- [Acceso mediante inicio de sesión único a las aplicaciones SAML 2.0 y 2.0 OAuth](#)
- [Configuración de aplicaciones de SAML 2.0 administradas por el cliente](#)

## Acceso mediante inicio de sesión único a las aplicaciones SAML 2.0 y 2.0 OAuth

El Centro de identidades de IAM le permite ofrecer a sus usuarios un acceso de inicio de sesión único a las aplicaciones SAML 2.0 o 2.0. OAuth Los siguientes temas proporcionan una descripción general de alto nivel de SAML 2.0 y 2.0. OAuth

## Temas

- [SAML 2.0](#)
- [OAuth 2.0](#)

### SAML 2.0

SAML 2.0 es un estándar del sector utilizado para intercambiar de forma segura aserciones de SAML que transmiten información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML 2.0 (denominado proveedor de servicios o SP). El Centro de Identidad de IAM utiliza esta información para proporcionar un acceso de inicio de sesión único federado a los usuarios que están autorizados a utilizar las aplicaciones del portal de acceso.

AWS



 Note

IAM Identity Center no admite la validación de las firmas de las solicitudes de autenticación de SAML entrantes procedentes de aplicaciones de SAML.

## OAuth 2.0

OAuth 2.0 es un protocolo que permite a las aplicaciones acceder a los datos de los usuarios y compartirlos de forma segura sin compartir contraseñas. Esta capacidad proporciona a los usuarios una forma segura y estandarizada de permitir que las aplicaciones accedan a sus recursos. El acceso se ve facilitado por diferentes flujos de subvenciones OAuth 2.0.

El IAM Identity Center permite a las aplicaciones que se ejecutan en clientes públicos recuperar credenciales temporales de acceso Cuentas de AWS y servicios mediante programación en nombre de sus usuarios. Los clientes públicos suelen ser computadoras de escritorio, portátiles u otros dispositivos móviles que se utilizan para ejecutar aplicaciones de forma local. Algunos ejemplos de AWS aplicaciones que se ejecutan en clientes públicos son AWS Command Line Interface (AWS CLI) y los kits de desarrollo de AWS software (AWS SDKs). Para permitir que estas aplicaciones obtengan credenciales, IAM Identity Center admite partes de los siguientes flujos OAuth 2.0:

- Concesión de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE) ([RFC 6749](#) y [RFC 7636](#))
- Concesión de autorización de dispositivo ([RFC 8628](#))

 Note

Estos tipos de subvenciones solo se pueden utilizar si Servicios de AWS admiten esta capacidad. Es posible que estos servicios no admitan este tipo de concesión en todas Regiones de AWS. Consulte la documentación relevante Servicios de AWS para conocer las diferencias regionales.

OpenID Connect (OIDC) es un protocolo de autenticación que se basa en el marco 2.0. OAuth El OIDC especifica cómo utilizar la versión 2.0 para la autenticación. OAuth A través del [servicio OIDC del IAM Identity Center APIs](#), una aplicación registra un cliente OAuth 2.0 y utiliza uno de

estos flujos para obtener un token de acceso que permite proteger el IAM Identity Center. APIs Una aplicación específica los [ámbitos de acceso](#) para declarar el usuario de API al que va dirigido. Una vez que usted, como administrador de IAM Identity Center, haya configurado su fuente de identidad, los usuarios finales de la aplicación deberán completar un proceso de inicio de sesión, si aún no lo han hecho. A continuación, los usuarios finales deben dar su consentimiento para permitir que la aplicación realice llamadas a la API. Estas llamadas a la API se realizan con los permisos de los usuarios. En respuesta, IAM Identity Center devuelve un token de acceso a la aplicación que contiene los ámbitos de acceso a los que los usuarios dieron su consentimiento.

## Uso de un flujo de concesión 2.0 OAuth

OAuth Los flujos de subvenciones 2.0 solo están disponibles a través de aplicaciones AWS gestionadas que admiten los flujos. Para utilizar un flujo OAuth 2.0, su instancia de IAM Identity Center y cualquier aplicación AWS gestionada compatible que utilice deben desplegarse en una sola Región de AWS instancia. Consulte la documentación de cada una de ellas Servicio de AWS para determinar la disponibilidad regional de las aplicaciones AWS gestionadas y la instancia del IAM Identity Center que desea utilizar.

Para utilizar una aplicación que utilice un flujo OAuth 2.0, el usuario final debe introducir la URL a la que se conectará la aplicación y registrarse en su instancia de IAM Identity Center. En función de la aplicación, como administrador, debe proporcionar a sus usuarios la URL del portal de acceso AWS o la URL del emisor de su instancia de IAM Identity Center. Puede encontrar estos dos ajustes en la página de Configuración de la [consola de IAM Identity Center](#). Para obtener información adicional sobre la configuración de una aplicación cliente, consulte la documentación de esa aplicación.

La experiencia del usuario final a la hora de iniciar sesión en una aplicación y dar su consentimiento depende de si la aplicación utiliza [Concesión de código de autorización con PKCE](#) o [Concesión de autorización de dispositivo](#).

### Concesión de código de autorización con PKCE

Este flujo lo utilizan las aplicaciones que se ejecutan en un dispositivo que tiene un navegador.

1. Se abre una ventana del navegador.
2. Si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:

- El nombre de la aplicación
  - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

### Concesión de autorización de dispositivo

Las aplicaciones que se ejecutan en un dispositivo con o sin navegador pueden utilizar este flujo. Cuando la aplicación inicia el flujo, presenta una URL y un código de usuario que el usuario debe verificar más adelante en el flujo. El código de usuario es necesario porque la aplicación que inicia el flujo puede estar ejecutándose en un dispositivo diferente al dispositivo en el que el usuario da su consentimiento. El código garantiza que el usuario dé su consentimiento al flujo que inició en el otro dispositivo.

#### Note

Si tiene clientes que utilizan `device.sso.region.amazonaws.com`, debe actualizar su flujo de autorización para utilizar la clave de prueba para el intercambio de códigos (PKCE). Para obtener más información, consulte [Configuración de la autenticación de IAM Identity Center con la AWS CLI](#) en la Guía del usuario de AWS Command Line Interface .

1. Cuando el flujo se inicia desde un dispositivo con un navegador, se abre una ventana del navegador. Cuando el flujo se inicia desde un dispositivo sin navegador, el usuario debe abrir un navegador en un dispositivo diferente e ir a la URL que presentó la aplicación.
2. En cualquier caso, si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:
  - El nombre de la aplicación
  - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
  - El código de usuario que la aplicación presentó al usuario
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

## Ámbitos de acceso

Un ámbito define el acceso a un servicio al que se puede acceder a través de un flujo OAuth 2.0. Los ámbitos permiten al servicio, también denominado servidor de recursos, agrupar los permisos relacionados con las acciones y los recursos del servicio, y especifican las operaciones más generales que OAuth pueden solicitar los clientes de la versión 2.0. Cuando un cliente OAuth 2.0 se registra en el [servicio OIDC del IAM Identity Center](#), especifica los ámbitos para declarar las acciones que pretende realizar, para lo cual el usuario debe dar su consentimiento.

OAuth Los clientes 2.0 utilizan scope los valores definidos en la [sección 3.3 de la OAuth versión 2.0 \(RFC 6749\)](#) para especificar qué permisos se solicitan para un token de acceso. Los clientes pueden especificar un máximo de 25 ámbitos al solicitar un token de acceso. Cuando un usuario da su consentimiento durante una concesión de código de autorización con el PKCE o el flujo de concesión de autorización de un dispositivo, IAM Identity Center codifica los ámbitos en el token de acceso que devuelve.

AWS añade ámbitos al Centro de Identidad de IAM para que sean compatibles. Servicios de AWS En la siguiente tabla, se enumeran los ámbitos que admite el servicio OIDC de IAM Identity Center al registrar un cliente público.

Ámbitos de acceso compatibles con el servicio OIDC de IAM Identity Center al registrar a un cliente público

| Alcance                   | Description (Descripción)                                                                | Servicios admitidos por                              |
|---------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------|
| sso:account:access        | Acceda a las cuentas administradas y a los conjuntos de permisos de IAM Identity Center. | IAM Identity Center                                  |
| codewhisperer:analysis    | Habilite el acceso al análisis de código de Kiro.                                        | ID de creador de AWS y el Centro de Identidad de IAM |
| codewhisperer:completions | Habilite el acceso a las sugerencias de código en línea de Kiro.                         | ID de creador de AWS y el Centro de Identidad de IAM |

| Alcance                                          | Description (Descripción)                                                                                        | Servicios admitidos por                              |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <code>codewhisperer:conversations</code>         | Habilite el acceso al chat de Kiro.                                                                              | ID de creador de AWS y el Centro de Identidad de IAM |
| <code>codewhisperer:taskassist</code>            | Habilite el acceso a Kiro Agent para el desarrollo de software.                                                  | ID de creador de AWS y el Centro de Identidad de IAM |
| <code>codewhisperer:transformations</code>       | Habilite el acceso a Kiro Agent para la transformación del código.                                               | ID de creador de AWS y el Centro de Identidad de IAM |
| <code>codecatalyst:read_write</code>             | Lee y escribe en tus CodeCatalyst recursos de Amazon, lo que te permite acceder a todos tus recursos existentes. | ID de creador de AWS y IAM Identity Center           |
| <code>verified_access:application:connect</code> | Habilitar Acceso verificado de AWS                                                                               | Acceso verificado de AWS                             |
| <code>redshift:connect</code>                    | Conéctese a Amazon Redshift                                                                                      | Amazon Redshift                                      |
| <code>datazone:domain:access</code>              | Acceda a su función DataZone de ejecución de dominio                                                             | Amazon DataZone                                      |
| <code>nosqlworkbench:datamodeladviser</code>     | Cree y lea modelos de datos                                                                                      | NoSQL Workbench                                      |
| <code>transform:read_write</code>                | Habilite el acceso a AWS Transform Agent para la transformación del código                                       | AWS Transformación                                   |

## Configuración de aplicaciones de SAML 2.0 administradas por el cliente

Si usa aplicaciones administradas por el cliente que admiten [SAML 2.0](#), puede federar su IdP a IAM Identity Center mediante SAML 2.0 y usar IAM Identity Center para administrar el acceso de los usuarios a esas aplicaciones. Puede seleccionar una aplicación de SAML 2.0 de un catálogo de aplicaciones de uso frecuente en la consola de IAM Identity Center o puede configurar su propia aplicación de SAML 2.0.

### Note

Si tiene aplicaciones gestionadas por clientes compatibles con la OAuth versión 2.0 y sus usuarios necesitan acceder a ellas desde esas aplicaciones Servicios de AWS, puede utilizar la propagación de identidades fiable. Con la propagación de identidades de confianza, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir la identidad de los usuarios en las solicitudes de acceso a los datos de los Servicios de AWS.

### Temas

- [Configuración de una aplicación del catálogo de aplicaciones de IAM Identity Center](#)
- [Configuración de su propia aplicación de SAML 2.0](#)

## Configuración de una aplicación del catálogo de aplicaciones de IAM Identity Center

Puede utilizar el catálogo de aplicaciones de la consola de IAM Identity Center para agregar muchas aplicaciones de SAML 2.0 de uso común que funcionan con IAM Identity Center. Algunos ejemplos son Salesforce, Box y Microsoft 365.

La mayoría de aplicaciones proporcionan información detallada sobre cómo configurar la confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta información está disponible en la página de configuración de la aplicación, después de seleccionarla en el catálogo. Tras configurar la aplicación, puede asignar el acceso a los usuarios o grupos de IAM Identity Center según sea necesario.

Utilice este procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación.

Antes de comenzar este procedimiento, resulta útil disponer del archivo de intercambio de metadatos del proveedor de servicios para que pueda configurar la relación de confianza de manera más

eficiente. Aunque no disponga de este archivo, puede utilizar este procedimiento para configurar la confianza manualmente.

Para añadir y configurar una aplicación del catálogo de aplicaciones

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, elija Deseo seleccionar una aplicación del catálogo.
6. En Catálogo de aplicaciones, empiece a escribir el nombre de la aplicación que desea agregar en el cuadro de búsqueda.
7. Elija el nombre de la aplicación en la lista cuando aparezca en los resultados de la búsqueda y, a continuación, seleccione Siguiente.
8. En la página Configurar aplicación, los campos Nombre de visualización y Descripción se rellenan automáticamente con los detalles correspondientes de la aplicación. Puede modificar esta información.
9. En Metadatos de IAM Identity Center, haga lo siguiente:
  - a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.
  - b. En el a Certificado de IAM Identity Center, elija Descargar certificado para descargar el certificado del proveedor de identidad.

 Note

Necesitará estos archivos más tarde al configurar la aplicación desde el sitio web del proveedor de servicios. Siga las instrucciones de dicho proveedor.

10. (Opcional) En Propiedades de la aplicación, puede especificar URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#).
11. En Metadatos de la aplicación, realice una de las siguientes acciones:

- a. Si tiene un archivo de metadatos, seleccione Cargar archivo de metadatos de SAML de la aplicación. A continuación, seleccione Elegir archivo para buscar y seleccionar el archivo de metadatos.
  - b. Si no tiene un archivo de metadatos, elija Escribir manualmente los valores de los metadatos y, a continuación, proporcione la URL de ACS de la aplicación y los valores de audiencia de SAML de la aplicación.
12. Seleccione Enviar. Accederá a la página de detalles de la aplicación que acaba de añadir.

## Configuración de su propia aplicación de SAML 2.0

Puede configurar sus propias aplicaciones que permitan la federación de identidades mediante SAML 2.0 y agregarlas a IAM Identity Center. La mayoría de los pasos para configurar sus propias aplicaciones de SAML 2.0 son los mismos que para configurar una aplicación de SAML 2.0 desde el catálogo de aplicaciones de la consola de IAM Identity Center. Sin embargo, también debe proporcionar más asignaciones de atributos de SAML para sus aplicaciones de SAML 2.0. Estas asignaciones permiten que IAM Identity Center rellene correctamente la aserción de SAML 2.0 para su aplicación. Puede proporcionar esta asignación de atributos SAML adicionales cuando configure la aplicación por primera vez. También puede proporcionar asignaciones de atributos de SAML 2.0 en la página de detalles de la aplicación de la consola de IAM Identity Center.

Utilice el siguiente procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación de SAML 2.0. Antes de comenzar este procedimiento, asegúrese de que dispone del certificado y del archivo de intercambio de metadatos del proveedor de servicios para que pueda completar la configuración de la relación de confianza.

Para configurar su propia aplicación de SAML 2.0

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, seleccione SAML 2.0.
7. Elija Siguiente.



8. En la página Configurar aplicación, en Configurar aplicación, introduzca un nombre para mostrar para la aplicación, por ejemplo **MyApp**. Escriba una descripción en Descripción.
9. En Metadatos de IAM Identity Center, haga lo siguiente:
  - a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.
  - b. Junto a Certificado de IAM Identity Center, seleccione Descargar para descargar el certificado del proveedor de identidades.

 Note

Necesitará estos archivos más tarde al configurar la aplicación personalizada desde el sitio web del proveedor de servicios.

10. (Opcional) En Propiedades de la aplicación, también puede especificar los valores de URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#).
11. En Metadatos de la aplicación, elija Escribir manualmente los valores de los metadatos. A continuación, proporcione valores para la URL de ACS de la aplicación y la audiencia de SAML de la aplicación.
12. Seleccione Enviar. Accederá a la página de detalles de la aplicación que acaba de añadir.

## Descripción general de la propagación de identidades de confianza

La propagación de identidades de confianza es una característica de IAM Identity Center que permite a los administradores de Servicios de AWS conceder permisos en función de los atributos de los usuarios, como las asociaciones de grupos. Con la propagación de identidades confiable, el contexto de identidad se agrega a una función de IAM para identificar al usuario que solicita acceso a AWS los recursos. Este contexto se propaga a otros. Servicios de AWS

El contexto de identidad comprende la información que se Servicios de AWS utiliza para tomar decisiones de autorización cuando reciben solicitudes de acceso. Esta información incluye los metadatos que identifican al solicitante (por ejemplo, un usuario del Centro de Identidad de IAM), el lugar Servicio de AWS al que se solicita el acceso (por ejemplo, Amazon Redshift) y el ámbito del

acceso (por ejemplo, el acceso de solo lectura). El destinatario Servicio de AWS utiliza este contexto y cualquier permiso asignado al usuario para autorizar el acceso a sus recursos.

## Ventajas de la propagación de la identidad de confianza

La propagación fiable de la identidad permite Servicios de AWS a los administradores conceder permisos a los recursos, como los datos, utilizando las identidades corporativas de sus empleados. Además, pueden auditar quién accedió a qué datos consultando los registros de servicio o AWS CloudTrail. Si es administrador del IAM Identity Center, es posible que otros administradores de Servicio de AWS le pidan que habilite la propagación de identidades de confianza.

## Activación de la propagación de identidades de confianza

El proceso de habilitar la propagación de identidades de forma fiable consta de los dos pasos siguientes:

1. Activa el Centro de Identidad de IAM y conecta tu fuente de identidades actual al Centro de Identidad de IAM. Seguirás gestionando las identidades de tus empleados en tu fuente de identidades actual; al conectarlo al Centro de Identidad de IAM, se crea una referencia para tus empleados que todos los usuarios de tu Servicios de AWS caso práctico pueden compartir. También está disponible para que los propietarios de los datos lo utilicen en futuros casos de uso.
2. Conéctelo Servicios de AWS en su caso de uso al Centro de identidad de IAM: el administrador de cada uno Servicio de AWS de los casos de uso de propagación de identidad confiable sigue las instrucciones de la documentación de servicio correspondiente para conectar el servicio al Centro de identidad de IAM.

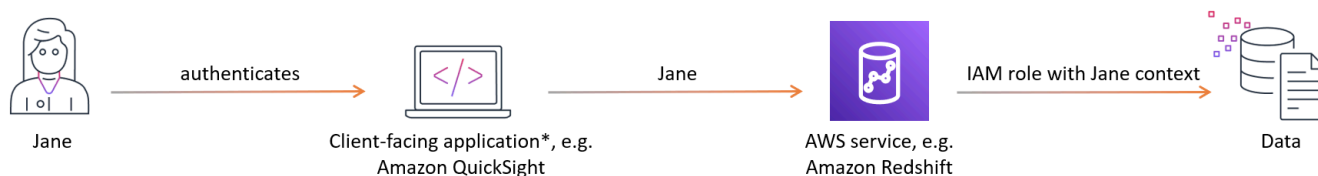
### Note

Si su caso de uso involucra una aplicación desarrollada por terceros o por un cliente, habilite la propagación de identidades de confianza configurando una relación de confianza entre el proveedor de identidades que autentica a los usuarios de la aplicación e IAM Identity Center. Esto permite que su aplicación aproveche el flujo de propagación de identidades de confianza descrito anteriormente.

Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

## Cómo funciona la propagación de identidades de confianza

En el diagrama a continuación se muestra el flujo de trabajo de alto nivel para la propagación de identidades de confianza:



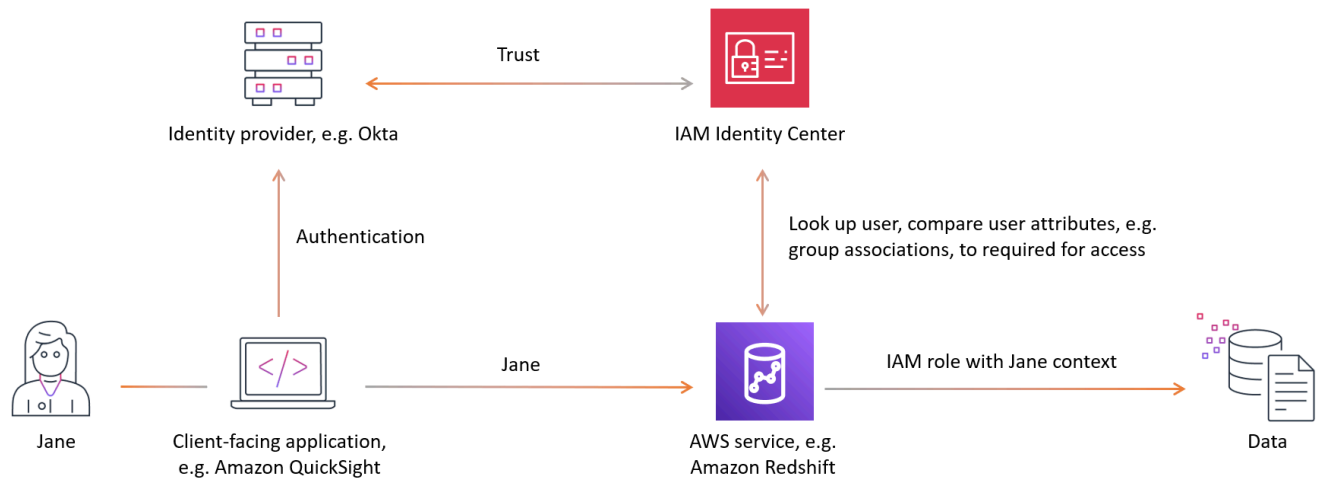
1. Los usuarios se autentican con una aplicación orientada al cliente, por ejemplo, Quick.
2. La aplicación orientada al cliente solicita acceso para usar y consultar datos e incluye información sobre el usuario. Servicio de AWS

### Note

Algunos casos de uso fiables de la propagación de identidades implican herramientas que interactúan con el Servicios de AWS uso de controladores de servicio. Puede averiguar si esto se aplica a su caso de uso en la [guía de casos de uso](#).

3. Servicio de AWS Verifica la identidad del usuario con el Centro de Identidad de IAM y compara los atributos del usuario, como sus asociaciones grupales, con los necesarios para el acceso. Servicio de AWS Autoriza el acceso siempre que el usuario o su grupo tengan los permisos necesarios.
4. Servicios de AWS puede registrar el identificador de usuario AWS CloudTrail y en sus registros de servicio. Para conocer detalles, consulte la documentación del servicio.

La siguiente imagen proporciona una descripción general de los pasos descritos anteriormente en el flujo de trabajo de propagación de identidades de confianza:



## Temas

- [Requisitos y consideraciones previos](#)
- [Casos de uso de propagación de identidades de confianza](#)
- [Autorización de servicios](#)

## Requisitos y consideraciones previos

Antes de configurar la propagación de identidades de confianza, revise los siguientes requisitos previos y consideraciones.

### Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Consideraciones para las aplicaciones administradas por el cliente](#)

## Requisitos previos

Para utilizar la propagación de identidades de confianza, asegúrese de que el entorno cumple los siguientes requisitos previos.

- Habilite y aprovisiona IAM Identity Center
  - Para utilizar una propagación de identidad fiable, debe habilitar el Centro de Identidad de IAM en el mismo Región de AWS lugar donde están habilitadas las AWS aplicaciones y los servicios a los que accederán sus usuarios. Para obtener información, consulte [Activar IAM Identity Center](#).

- Se recomienda la instancia de organización IAM Identity Center: le recomendamos que utilice una [instancia de organización](#) de IAM Identity Center que habilite en la cuenta de administración de AWS Organizations. Puede [delegar la administración](#) de una instancia de organización de IAM Identity Center a una cuenta de miembro. Si elige una [instancia de cuenta](#) de IAM Identity Center, todos los Servicios de AWS a los que desee que accedan los usuarios con la propagación de identidades de confianza deben residir en la misma Cuenta de AWS donde habilita IAM Identity Center. Para obtener más información, consulte [Instancias de cuenta de IAM Identity Center](#).
- Conecte su origen de identidad a IAM Identity Center y aprovisiona usuarios y grupos en IAM Identity Center. Para obtener más información, consulte [Tutoriales de orígenes de identidad de IAM Identity Center](#).
- Conecte las aplicaciones y los servicios AWS gestionados de su caso de uso de propagación de identidades de confianza al IAM Identity Center. Para utilizar una propagación de identidad fiable, las aplicaciones AWS gestionadas deben estar conectadas al Centro de identidades de IAM.

## Consideraciones

Tenga en cuenta las siguientes consideraciones cuando configure y utilice la propagación de identidades de confianza:

- Instancia de organización frente a instancia de cuenta de IAM Identity Center
  - Una [instancia de organización](#) de IAM Identity Center le proporcionará el mayor control y flexibilidad para ampliar sus casos de uso a varias Cuentas de AWS, usuarios y Servicios de AWS. Si no puede utilizar una instancia de organización, es posible que su caso de uso sea compatible con las instancias de cuentas de IAM Identity Center. Para obtener más información sobre qué Servicios de AWS en su caso de uso admiten instancias de cuenta de IAM Identity Center, consulte [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#).
- No se requieren permisos de varias cuentas (conjuntos de permisos)
  - La propagación de identidades de confianza no requiere que configure [permisos de varias cuentas](#) (conjuntos de permisos). Puede habilitar IAM Identity Center y utilizarlo únicamente para la propagación de identidades de confianza.

## Consideraciones para las aplicaciones administradas por el cliente

Sus empleados pueden beneficiarse de una propagación de identidad fiable incluso si sus usuarios interactúan con aplicaciones orientadas al cliente que no están gestionadas, por ejemplo AWS, por

sus aplicaciones desarrolladas a Tableau medida. Es posible que los usuarios de estas aplicaciones no estén aprovisionados en IAM Identity Center. Para permitir el reconocimiento y la autorización sin problemas del acceso de los usuarios a AWS los recursos, el Centro de identidad de IAM le permite configurar una relación de confianza entre el proveedor de identidad que autentica a sus usuarios y el Centro de identidad de IAM. Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

Además, configurar la propagación de identidades de confianza para su aplicación requerirá lo siguiente:

- La aplicación debe utilizar el marco OAuth 2.0 para la autenticación. La propagación de identidades de confianza no admite integraciones de SAML 2.0.
- IAM Identity Center debe reconocer su aplicación. Siga las instrucciones específicas para su [caso de uso](#).

## Casos de uso de propagación de identidades de confianza

Como administrador de IAM Identity Center, es posible que se le pida que ayude a configurar la propagación de identidades de confianza desde las aplicaciones orientadas a usuarios hasta los Servicios de AWS. Para respaldar esta solicitud, deberá tener la siguiente información:

- ¿Con qué aplicación orientada al cliente interactuarán sus usuarios?
- ¿Cuáles Servicios de AWS se utilizan para consultar los datos y autorizar el acceso a los datos?
- ¿ Servicio de AWS Quién autoriza el acceso a los datos?

Su rol a la hora de habilitar los casos de uso de la propagación de identidades de confianza que no impliquen aplicaciones de terceros o aplicaciones desarrolladas a medida consiste en:

1. [Habilite el centro de identidad de IAM](#).
2. [Conecte su origen de identidad existente a IAM Identity Center](#).

Los pasos restantes de la configuración de la identidad confiable para estos casos de uso se llevan a cabo dentro de las aplicaciones conectadas Servicios de AWS y. Los administradores de las aplicaciones conectadas Servicios de AWS o conectadas deben consultar las guías de usuario correspondientes para obtener una guía completa sobre los servicios específicos.

Su rol a la hora de habilitar los casos de uso de la propagación de identidades de confianza que implican aplicaciones de terceros o aplicaciones desarrolladas a medida incluye los pasos necesarios de [Activar IAM Identity Center](#) y [conectar su origen de identidades](#), así como:

1. Configurar la conexión de su proveedor de identidades (IdP) con la aplicación de terceros o desarrollada a medida.
2. Permitir que IAM Identity Center reconozca la aplicación de terceros o desarrollada a medida.
3. Configurar su IdP como emisor de tokens de confianza en IAM Identity Center Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

Los administradores de las aplicaciones conectadas Servicios de AWS deben consultar las guías de usuario correspondientes para obtener una guía completa sobre los servicios específicos.

## Casos de uso de análisis, machine learning y almacén de lago de datos

Puede habilitar casos de uso de propagación de confianza con los siguientes servicios de análisis y machine learning:

- Amazon Redshift: para obtener instrucciones, consulte [Propagación de identidades de confianza con Amazon Redshift](#).
- Amazon EMR: para obtener instrucciones, consulte [Propagación de identidades de confianza con Amazon EMR](#).
- Amazon Athena: para obtener instrucciones, consulte [Propagación de identidades de confianza con Amazon Athena](#).
- SageMaker Studio: para obtener orientación, consulte. [Propagación de identidad fiable con Amazon SageMaker Studio](#)

## Casos de uso adicionales

Puede habilitar IAM Identity Center y la propagación de identidades de confianza con los siguientes Servicios de AWS adicionales:

- Amazon Q Business: para obtener instrucciones, consulte:
  - [Flujo de trabajo del administrador para las aplicaciones que utilizan IAM Identity Center](#).
  - [Configuración de una aplicación Amazon Q Business mediante IAM Identity Center](#).

- [Cómo configurar Amazon Q Business con la propagación de identidades de confianza de IAM Identity Center.](#)
- Amazon OpenSearch Service: para obtener información, consulta:
  - [IAM Identity Center Trusted Identity Propagation Support for Amazon OpenSearch Service.](#)
  - [Interfaz OpenSearch de usuario centralizada \(paneles de control\) con Amazon OpenSearch Service.](#)
- AWS Transfer Family: para obtener instrucciones, consulte:
  - [Aplicaciones web Transfer Family.](#)

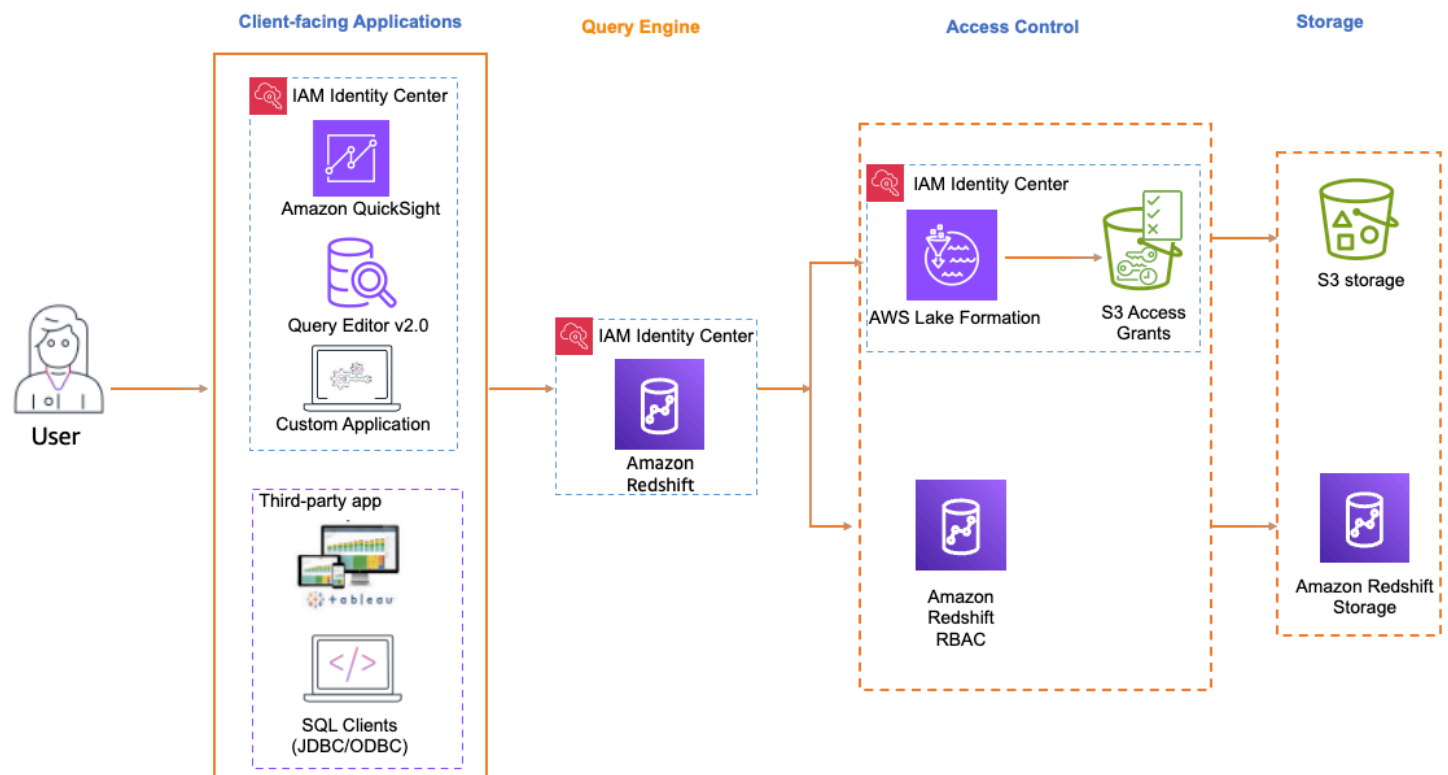
## Temas

- [Propagación de identidades de confianza con Amazon Redshift](#)
- [Propagación de identidades de confianza con Amazon EMR](#)
- [Propagación de identidades de confianza con Amazon Athena](#)
- [Propagación de identidad fiable con Amazon SageMaker Studio](#)

## Propagación de identidades de confianza con Amazon Redshift

Los pasos para permitir una propagación de identidad fiable dependen de si los usuarios interactúan con las aplicaciones AWS gestionadas o con las gestionadas por los clientes. El siguiente diagrama muestra una configuración de propagación de identidad confiable para aplicaciones orientadas al cliente, AWS administradas o externas, que consultan datos de Amazon Redshift con el control de acceso proporcionado por Amazon Redshift o por servicios de autorización, como Amazon S3. AWS Lake Formation Access Grants





Cuando la propagación de identidades de confianza a Amazon Redshift está habilitada, los administradores de Redshift pueden configurar Redshift para que [cree automáticamente funciones](#) para IAM Identity Center como proveedor de identidades, asignar las funciones de Redshift a los grupos de IAM Identity Center y utilizar el [control de acceso basado en funciones de Redshift para conceder el acceso](#).

Aplicaciones orientadas al cliente compatibles

AWS aplicaciones administradas

Las siguientes aplicaciones AWS gestionadas orientadas al cliente admiten la propagación de identidades de confianza en Amazon Redshift:

- [Amazon Redshift Query Editor V2](#)
- [Rápido](#)

 Note

Si utiliza Amazon Redshift Spectrum para acceder a bases de datos o tablas externas en AWS Glue Data Catalog, considere la posibilidad de configurar [Lake Formation](#) y [Access Grants de Amazon S3](#) para proporcionar un control de acceso detallado.

## Aplicaciones administradas por el cliente

Las siguientes aplicaciones orientadas al cliente administradas por el cliente admiten la propagación de identidades de confianza en Amazon Redshift:

- Tableau, incluidos Tableau Desktop, Tableau Server y Tableau Prep
  - Para habilitar la propagación de identidades de confianza para los usuarios de Tableau, consulte [Integrate Tableau and Okta with Amazon Redshift using IAM Identity Center](#) en el Blog de macrodatos de AWS .
- Clientes de SQL (DBeaver y DBVisualizer)
  - Para permitir la propagación de identidades de confianza para los usuarios de clientes de SQL (DBeaver y DBVisualizer), consulte [Integrate Identity Provider \(IdP\) with Amazon Redshift Query Editor V2 and SQL Client using IAM Identity Center for seamless Single Sign-On](#) en el Blog de macrodatos de AWS .

## Configuración de la propagación de identidades de confianza con el editor de consultas V2 de Amazon Redshift

El siguiente procedimiento explica cómo lograr una propagación de identidades de confianza desde el editor de consultas V2 de Amazon Redshift a Amazon Redshift.

### Requisitos previos

Antes de empezar con este tutorial, primero tendrá que configurar lo siguiente:

1. [Habilite el centro de identidad de IAM](#). Se recomienda la [instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisionar los usuarios y grupos de su origen de identidades en IAM Identity Center](#).

La activación de la propagación de identidades de confianza incluye las tareas realizadas por un administrador de IAM Identity Center en la consola de IAM Identity Center y las tareas realizadas por un administrador de Amazon Redshift en la consola de Amazon Redshift.

Tareas realizadas por el administrador de IAM Identity Center

El administrador de IAM Identity Center debía completar las siguientes tareas:

1. Crear un [rol de IAM](#) en la cuenta en la que se encuentre el clúster de Amazon Redshift o la instancia sin servidor con la siguiente política de permisos. Para obtener más información, consulte [Creación de roles de IAM](#).

  - Los siguientes ejemplos de políticas incluyen los permisos necesarios para completar este tutorial. Para usar esta política, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Creación de una política](#) o [Edición de una política](#).

Política de permisos:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
    }
  ]
}
```

```

        "Resource": [
            "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
ID",
            "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
        ]
    }
}

```

Política de confianza:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

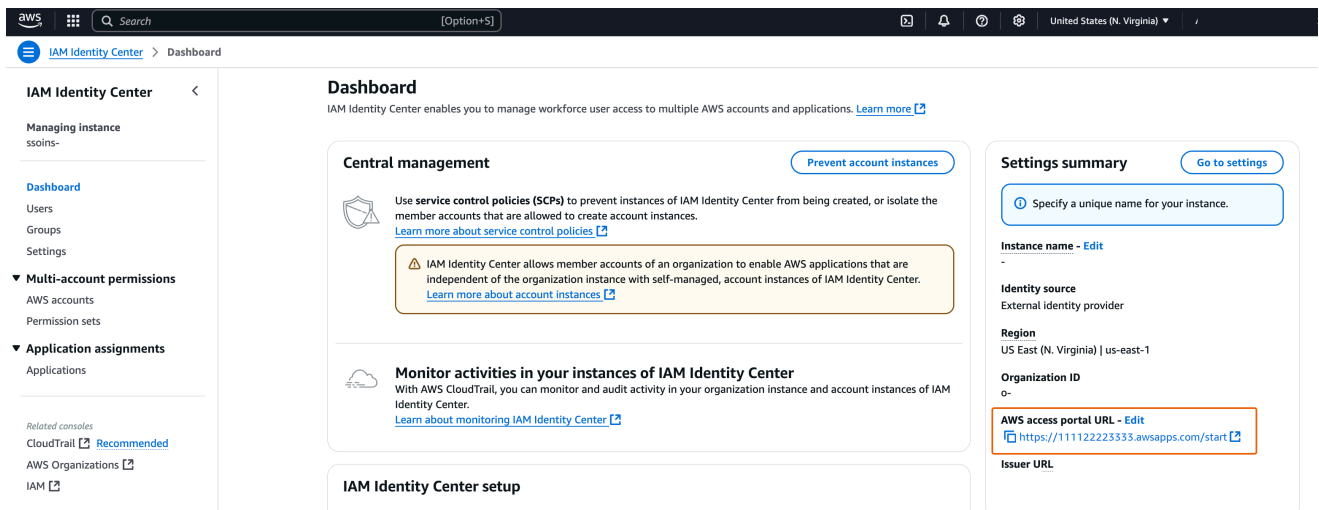
2. Cree un conjunto de permisos en la cuenta de administración de AWS Organizations en la que esté activado IAM Identity Center. Lo usará en el siguiente paso para permitir que los usuarios federados accedan al editor de consultas V2 de Redshift.
  - a. En la consola de IAM Identity Center, en Permisos multicuenta, seleccione Conjuntos de permisos.

- b. Elija Crear conjunto de permisos.
- c. Elija Conjunto de permisos personalizado y, a continuación, elija Siguiente.
- d. En Políticas administradas por AWS , seleccione **AmazonRedshiftQueryEditorV2ReadSharing**.
- e. En Política insertada, agregue la siguiente política:

JSON

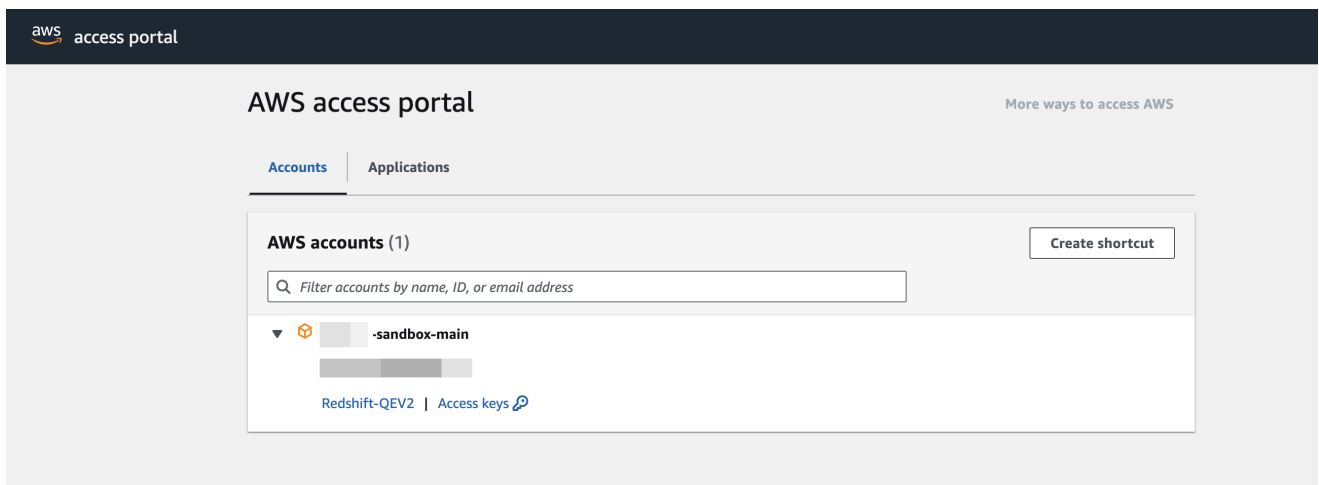
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}
```

- f. Seleccione Siguiente y, a continuación, proporcione un nombre para el nombre del conjunto de permisos. Por ejemplo, **Redshift-Query-Editor-V2**.
- g. En Estado de relé (opcional), defina el estado de relé predeterminado en la URL del editor de consultas V2, con el formato: `https://your-region.console.aws.amazon.com/sqlworkbench/home`.
- h. Revise la configuración y seleccione Crear.
- i. Diríjase al panel de control de IAM Identity Center y copie la URL del portal de acceso de AWS de la sección Resumen de la configuración.



- j. Abra una nueva ventana del navegador de incógnito y pegue la URL.

Esto lo llevará a su portal de AWS acceso, asegurándose de que está iniciando sesión con un usuario del Centro de Identidad de IAM.



Para obtener más información sobre el conjunto de permisos, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

3. Permita que los usuarios federados accedan al editor de consultas V2 de Redshift.
  - a. En la cuenta AWS Organizations de administración, abra la consola de IAM Identity Center.
  - b. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
  - c. En la Cuentas de AWS página, seleccione Cuenta de AWS aquella a la que desee asignar el acceso.
  - d. Seleccione Asignar usuarios o grupos.

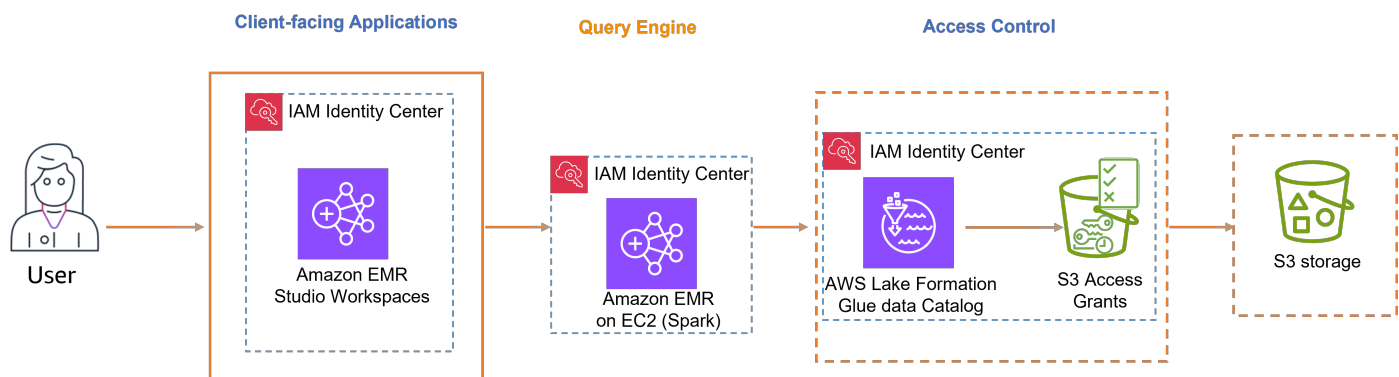
- e. En la página Asignar usuarios y grupos, seleccione los usuarios o grupos para los que desee crear permisos. A continuación, elija Siguiente.
- f. En la página Asignar conjuntos de permisos, elija el conjunto de permisos que creó en el paso anterior. A continuación, elija Siguiente.
- g. En la página Revisar y enviar asignaciones, revise la selección y elija Enviar.

## Tareas realizadas por un administrador de Amazon Redshift

Para habilitar la propagación de identidades de confianza en Amazon Redshift, es necesario que un administrador de clústeres de Amazon Redshift o un administrador de Amazon Redshift sin servidor realice una serie de tareas en la consola de Amazon Redshift. Para obtener más información, consulte [Integrate Identity Provider \(IdP\) with Amazon Redshift Query Editor V2 and SQL Client using IAM Identity Center for seamless Single Sign-On](#) en el Blog de macrodatos de AWS .

## Propagación de identidades de confianza con Amazon EMR

El siguiente diagrama muestra una configuración de propagación de identidad confiable para Amazon EMR Studio que utiliza Amazon EMR en Amazon EC2 con el control de acceso proporcionado por Amazon S3. AWS Lake Formation Access Grants



## Aplicaciones orientadas al cliente compatibles

- Amazon EMR Studio

Para habilitar la propagación de identidades de confianza, siga estos pasos:

- [Configure Amazon EMR Studio](#) como la aplicación orientada al cliente para el clúster de Amazon EMR.
- Configure el [clúster de Amazon EMR en Amazon EC2 con Apache Spark](#).

- Recomendado: [AWS Lake Formation](#) y [Amazon S3 Access Grants](#) para proporcionar un control de acceso detallado a las ubicaciones de datos subyacentes AWS Glue Data Catalog y a las ubicaciones de datos subyacentes en S3.

## Configuración de la propagación de identidades de confianza con Amazon EMR Studio

El siguiente procedimiento explica cómo configurar Amazon EMR Studio para la propagación de identidades de confianza en consultas realizadas en grupos de trabajo de Amazon Athena o clústeres de Amazon EMR que ejecutan Apache Spark.

### Requisitos previos

Antes de empezar con este tutorial, primero tendrá que configurar lo siguiente:

1. [Habilite el centro de identidad de IAM](#). Se recomienda la [instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisionar los usuarios y grupos de su origen de identidades en IAM Identity Center](#).

Para completar la configuración de la propagación de identidades de confianza desde Amazon EMR Studio, el administrador de EMR Studio debe realizar los siguientes pasos.

### Paso 1. Creación del rol de IAM requerido para EMR Studio

En este paso, el administrador de Amazon EMR Studio crea un rol de servicio de IAM y un rol de usuario de IAM para EMR Studio.

1. [Cree un rol de servicio de EMR Studio](#): EMR Studio asume este rol de IAM para gestionar de forma segura los espacios de trabajo y los blocs de notas, conectarse a clústeres y gestionar las interacciones de datos.
  - a. Navegue hasta la consola de IAM (<https://console.aws.amazon.com/iam/>) y cree un rol de IAM.
  - b. Seleccione Servicio de AWS como entidad de confianza y, a continuación, elija Amazon EMR. Adjunte las siguientes políticas para definir los permisos y la relación de confianza del rol.

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Creación de una política](#) o [Edición de una política](#).



## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    }
  ]
}
```

Para obtener una referencia de todos los permisos de rol de servicio, consulte [EMR Studio service role permissions](#).

2. [Cree un rol de usuario de EMR Studio para la autenticación de IAM Identity Center](#): EMR Studio asume este rol cuando un usuario inicia sesión a través de IAM Identity Center para administrar espacios de trabajo, clústeres de EMR, trabajos y repositorios de git. Este rol se utiliza para iniciar el flujo de trabajo de propagación de identidades de confianza.

 Note

El rol de usuario de EMR Studio no necesita incluir permisos para acceder a las ubicaciones de Amazon S3 de las tablas del catálogo. AWS Glue AWS Lake Formation los permisos y las ubicaciones de lagos registradas se utilizarán para recibir permisos temporales.

El siguiente ejemplo de política se puede utilizar en un rol que permita a un usuario de EMR Studio utilizar los grupos de trabajo de Athena para ejecutar consultas.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid": "AllowSecretManagerListSecrets",
      "Action": [
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:TagResource",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
    },
    {
      "Sid": "AllowPassingServiceRoleForWorkspaceCreation",

```

```

        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ReadOnlyAccessToLogs",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowAthenaQueryExecutions",
        "Effect": "Allow",
        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",
            "athena:CreatePreparedStatement",
            "athena:GetPreparedStatement",
            "athena>DeletePreparedStatement"
        ],

```

```

        "Resource": "*"
    },
    {
        "Sid": "AllowGlueSchemaManipulations",
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena:*:111122223333:workgroup*"
    },
    {
        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce>DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        }
    },
    {
        "Sid": "DescribeNetwork",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",

```

```
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListIAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "*"
    }
  ]
}
```

La siguiente política de confianza permite que EMR Studio asuma el rol:

 Note

Se necesitan permisos adicionales para aprovechar los espacios de trabajo de EMR Studio y los blocs de notas de EMR. Consulte [Creación de políticas de permisos para los usuarios de EMR Studio](#) para obtener más información.

Dispone de más información en los siguientes enlaces:

- [Defina los permisos de IAM personalizados con políticas administradas por el cliente](#)
- [Permisos de rol de servicio de EMR Studio](#)

## Paso 2. Creación y configuración de EMR Studio

En este paso, creará un Amazon EMR Studio en la consola de EMR Studio y utilizará los roles de IAM que creó en [Paso 1. Creación del rol de IAM requerido para EMR Studio](#).

1. Navegue hasta la consola de EMR Studio, seleccione Crear estudio y Configuración personalizada. Puede crear un nuevo bucket de S3 o utilizar un bucket existente. Puede marcar la casilla para Cifrar los archivos del espacio de trabajo con sus propias claves de KMS. Para obtener más información, consulte [AWS Key Management Service](#).

The screenshot shows the AWS EMR Studio console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a dropdown menu for the region (United States (N. Virginia)). Below the navigation bar, the breadcrumb trail reads: Amazon EMR > EMR Studio: Studios > Create Studio.

The main content area is titled "Create a Studio" with an "Info" link. It contains two main sections:

- Setup options** (with an "Info" link): This section has three radio buttons: "Interactive workloads", "Batch jobs", and "Custom". The "Custom" option is selected.
- Studio settings** (with an "Info" link): This section contains several fields and options:
  - Studio name**: A text input field containing "Studio\_1". Below it, a note says "Use up to 256 characters (alphanumeric, hyphens, or underscores)."
  - Description - optional**: A text area with the placeholder "Describe the Studio". Below it, a note says "The description below will be visible to your studio teams." and "256 characters maximum".
  - S3 location for Workspace storage**: A section with the instruction "Specify an Amazon S3 location where Workspace work will be saved." It has two radio buttons: "Create new bucket" (selected) and "Select existing location". Below this, it says "We'll create a new bucket and use the location s3://aws-emr-studio-225989353012-us-east-1/1735848818523."
  - Encrypt Workspace files with your own AWS KMS key**: A checkbox that is currently unchecked. Below it, a note says "EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation."

2. En Rol de servicio para permitir que Studio acceda a sus recursos, seleccione el rol de servicio creado en [Paso 1. Creación del rol de IAM requerido para EMR Studio](#) desde el menú.
3. En Autenticación, elija IAM Identity Center. Seleccione el rol de usuario creado en [Paso 1. Creación del rol de IAM requerido para EMR Studio](#).

Service role to let Studio access your AWS resources

AmazonEMRStudio\_ [View permission details](#)

**Authentication** [Info](#)

**Authentication**  
Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)  
Authenticate with single sign-on using IAM identity federation or IAM credentials.

☒ IAM Identity Center (AWS Single Sign-On)  
Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

**User role**  
Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#).

emrstudio-userrole-idc [Create IAM role](#)

**Connect EMR Studio to IAM Identity Center**  
instance of IAM Identity Center  
Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

[arn:aws:sso::instance/ssoin-](#)

4. Marque la casilla Propagación de identidades de confianza. Seleccione Solo usuarios y grupos asignados en la sección Acceso a la aplicación, lo que le permitirá conceder el acceso a este estudio únicamente a usuarios y grupos autorizados.
5. (Opcional): puede configurar la VPC y la subred si utiliza este estudio con clústeres de EMR.

**Trusted identity propagation** [Info](#)  
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**  
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

**The following features aren't supported from a Studio with trusted identity propagation:** creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.

**Application access** [Info](#)  
**Choose who can access your application**  
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**  
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ All users and groups  
Any user or group from your IAM Identity Center directory can access this application.

**Networking and security - optional**

**VPC** [Info](#)  
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the for-use-with-amazon-emr-managed-policies key and value true. To manage tags, use [VPC Dashboard](#).

Select a VPC

**Subnets** [Info](#)  
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the for-use-with-amazon-emr-managed-policies key and value true. To manage tags, use [VPC Dashboard](#).

6. Revise todos los detalles y seleccione Crear Studio.
7. Tras configurar un clúster de Athena WorkGroup o EMR, inicie sesión en la URL de Studio para:
  - a. Ejecutar consultas de Athena con el editor de consultas.
  - b. Ejecutar los trabajos de Spark en el espacio de trabajo con un bloc de notas Jupyter.

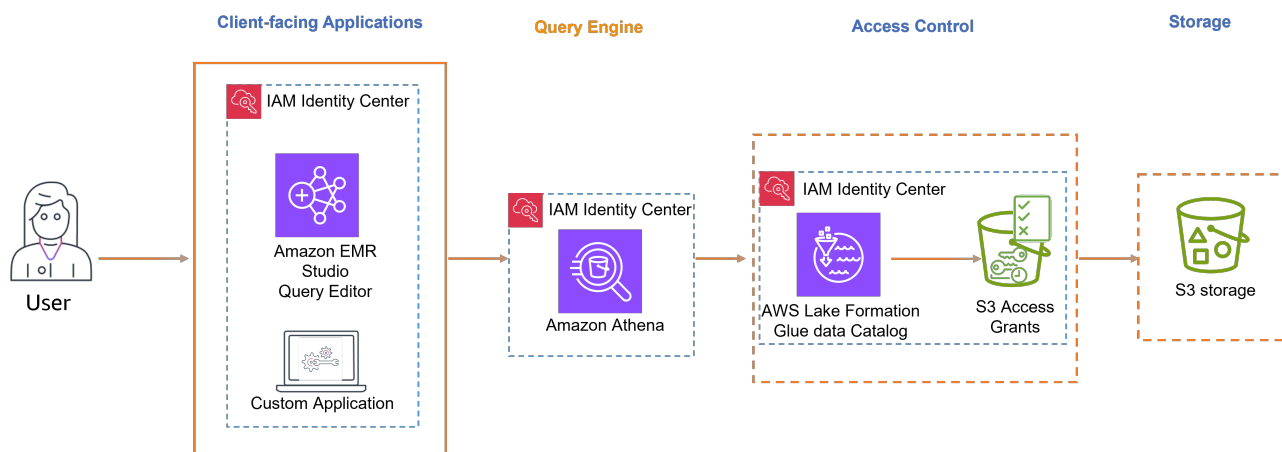


## Propagación de identidades de confianza con Amazon Athena

Los pasos para permitir una propagación de identidades fiable dependen de si los usuarios interactúan con las aplicaciones AWS gestionadas o con las gestionadas por los clientes. El siguiente diagrama muestra una configuración de propagación de identidad confiable para aplicaciones orientadas al cliente, AWS administradas o externas, que utilizan Amazon Athena para AWS consultar datos de Amazon S3 con el control de acceso proporcionado por AWS Lake Formation Amazon S3. Access Grants

### Note

- La propagación de identidades de confianza con Amazon Athena requiere el uso de Trino.
- No se admiten los clientes de SQL y Apache Spark conectados a Amazon Athena mediante controladores ODBC y JDBC.



### AWS aplicaciones administradas

La siguiente aplicación AWS gestionada orientada al cliente admite la propagación de identidades de confianza con Athena:

- Amazon EMR Studio

Para habilitar la propagación de identidades de confianza, siga estos pasos:

- [Configure Amazon EMR Studio](#) como la aplicación orientada al cliente para Athena. El editor de consultas de EMR Studio es necesario para ejecutar Athena Queries cuando la propagación de identidades de confianza está habilitada.
- [Configure Athena Workgroup](#).
- Se ha [configurado AWS Lake Formation](#) para permitir un control de acceso detallado para AWS Glue las tablas en función del usuario o grupo del IAM Identity Center.
- [Configure Amazon S3 Access Grants](#) para permitir el acceso temporal a las ubicaciones de datos subyacentes de S3.

 Note

Tanto Lake Formation como Amazon S3 Access Grants son necesarios para el control de acceso AWS Glue Data Catalog y para los resultados de las consultas de Athena en Amazon S3.

## Aplicaciones administradas por el cliente

Para permitir la propagación de identidades confiable para los usuarios de aplicaciones desarrolladas a medida, consulte [Acceder mediante Servicios de AWS programación mediante la propagación de identidades confiable en](#) el blog de seguridad.AWS

## Configuración de la propagación de identidades de confianza con grupos de trabajo de Amazon Athena

El siguiente procedimiento explica cómo configurar los grupos de trabajo de Amazon Athena para la propagación de identidades de confianza.

### Requisitos previos

Antes de empezar con este tutorial, primero tendrá que configurar lo siguiente:

1. [Habilite el Centro](#) de identidad de IAM. Se recomienda la [instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisionar los usuarios y grupos de su origen de identidades en IAM Identity Center](#).

3. Esta configuración requiere [Amazon EMR Studio](#), [AWS Lake Formation](#) y [Concesiones de acceso a Amazon S3](#).

## Configuración de la propagación de identidades de confianza con Athena

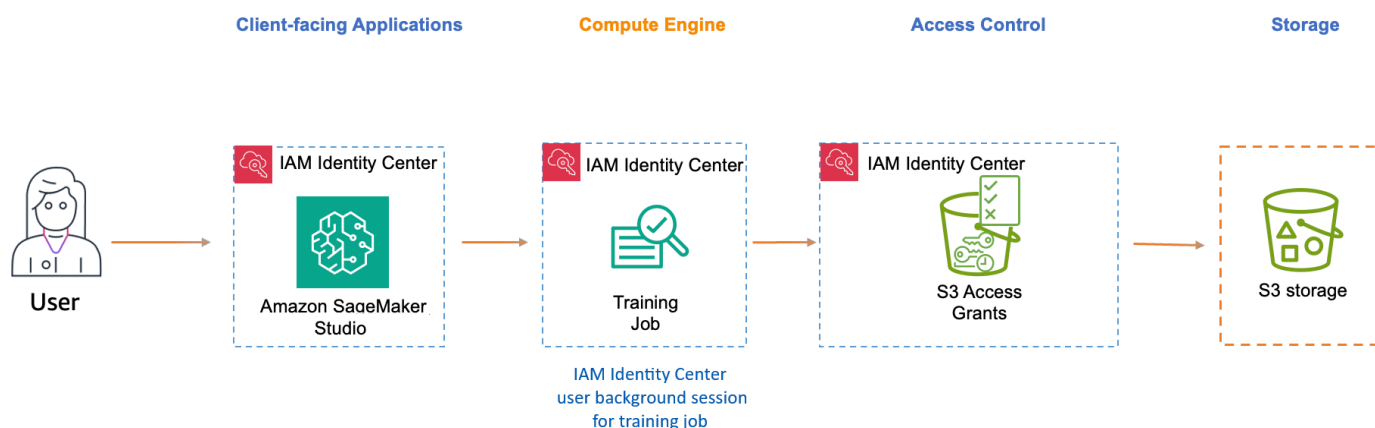
Para configurar la propagación de identidades de confianza con Athena, el administrador de Athena debe hacer lo siguiente:

1. Consultar [Consideraciones y limitaciones del uso de grupos de trabajo de Athena habilitados para IAM Identity Center](#).
2. [Crear un grupo de trabajo de Athena habilitado para IAM Identity Center](#).

## Propagación de identidad fiable con Amazon SageMaker Studio

[Amazon SageMaker Studio](#) se integra con el Centro de identidades de IAM y admite las [sesiones en segundo plano de los usuarios](#) y la propagación de identidades de confianza. Las sesiones de usuario en segundo plano permiten a un usuario iniciar un trabajo de larga duración en SageMaker Studio, sin que el usuario tenga que permanecer conectado mientras se ejecuta el trabajo. El trabajo se ejecuta inmediatamente y en segundo plano, utilizando los permisos del usuario que lo inició. El trabajo puede seguir ejecutándose aunque el usuario apague el ordenador, caduque su sesión de inicio de sesión en el IAM Identity Center o cierre sesión en el portal de acceso. AWS La duración de sesión predeterminada para las sesiones de usuario en segundo plano es de 7 días, pero puede especificar una duración máxima de 90 días. La propagación de identidades de confianza permite proporcionar un acceso detallado a recursos de AWS como los buckets de Amazon S3 en función de la identidad del usuario o de la membresía grupal.

El siguiente diagrama muestra una configuración de propagación de identidad confiable para SageMaker Studio, con acceso a los datos almacenados en un bucket de Amazon S3. Las sesiones de usuario en segundo plano están habilitadas para el IAM Identity Center, lo que permite que el trabajo de formación de SageMaker Studio se ejecute en segundo plano. Amazon S3 Access Grants proporciona el control de acceso a los datos de entrenamiento.



## AWS aplicación gestionada

La siguiente aplicación AWS gestionada orientada al cliente admite la propagación de identidades de forma fiable:

- [Amazon SageMaker Studio](#)

Para habilitar la propagación de identidades de confianza y sesiones de usuario en segundo plano, siga estos pasos:

- [Configure SageMaker Studio como la aplicación orientada al cliente.](#)
- [Configure Amazon S3 Access Grants](#) para permitir el acceso temporal a las ubicaciones de datos subyacentes de Amazon S3.

## Configuración de la propagación de identidades fiable con Studio SageMaker

El siguiente procedimiento explica cómo configurar SageMaker Studio para la propagación de identidades de confianza y las sesiones de usuario en segundo plano.

### Requisitos previos

Antes de empezar con este tutorial, primero tendrá que completar las siguientes tareas:

1. [Habilite el Centro de identidades de IAM.](#) Se requiere una instancia de organización. Para obtener más información, consulte [Requisitos y consideraciones previos.](#)
2. [Aprovisionar los usuarios y grupos de su origen de identidades en IAM Identity Center.](#)

3. [Confirmar que las sesiones de usuario en segundo plano estén habilitadas](#) en la consola de IAM Identity Center. De forma predeterminada, las sesiones de usuario en segundo plano están habilitadas y la duración de la sesión se establece en 7 días. Puede cambiar esta duración.

Para configurar la propagación de identidades de confianza desde SageMaker Studio, el administrador de SageMaker Studio debe realizar los siguientes pasos.

Paso 1: Habilitar la propagación de identidades de confianza en un dominio de SageMaker Studio nuevo o existente

SageMaker Studio usa los dominios para organizar los perfiles de usuario, las aplicaciones y sus recursos asociados. Para habilitar la propagación de identidades de forma fiable, debe crear un dominio de SageMaker Studio o modificar uno existente, tal y como se describe en el siguiente procedimiento.

1. Abra la consola de SageMaker IA, vaya a Dominios y realice una de las siguientes acciones.
  - Crea un nuevo dominio de SageMaker Studio mediante [la configuración para organizaciones](#).

Elija Configuración para organizaciones y, a continuación, haga lo siguiente:

- Elija AWS Identity Center como método de autenticación.
- Active la casilla Habilitar la propagación de identidad de confianza para todos los usuarios de este dominio.
- Modifica un dominio de SageMaker Studio existente.
  - Seleccione un dominio existente que utilice IAM Identity Center para la autenticación.

 Important

La propagación de identidades fiables solo se admite en los dominios de SageMaker Studio que utilizan el Centro de identidades de IAM para la autenticación. Si el dominio usa IAM para la autenticación, no puede cambiar el método de autenticación y, por lo tanto, no puede habilitar la propagación de identidades de confianza.

- [Edite la configuración del dominio](#) Edite la configuración Autenticación y permisos para activar la propagación de identidades de confianza.

2. Continúe con el [paso 2: configure el rol de ejecución de dominio predeterminado](#). Esta función es necesaria para que los usuarios de un dominio de SageMaker Studio puedan acceder a otros AWS servicios, como Amazon S3.

Paso 2: configure el rol de ejecución de dominio predeterminado y la política de confianza del rol

Una función de ejecución de dominio es una [función de IAM](#) que asume un dominio de SageMaker Studio en nombre de todos los usuarios del dominio. Los permisos que asigne a este rol determinan qué acciones puede realizar SageMaker Studio.

1. Para crear o seleccionar un rol de ejecución de dominio, realice una de las siguientes acciones:
  - Cree o seleccione un rol mediante la [configuración para organizaciones](#).
    - Abra la consola de SageMaker IA y siga las instrucciones de la consola del paso 2: Configure las funciones y las actividades de aprendizaje automático para crear una nueva función de ejecución de dominio o seleccione una función existente.
    - Complete el resto de los pasos de configuración para crear tu dominio de SageMaker Studio.
  - Cree un rol de ejecución manualmente.
    - Abra la consola de IAM y [cree el rol de ejecución usted mismo](#).
2. [Actualice la política de confianza](#) asociada al rol de ejecución del dominio para que incluya las dos acciones siguientes: [sts:AssumeRole](#) y [sts:SetContext](#). Para obtener información sobre cómo encontrar el rol de ejecución de tu dominio de SageMaker Studio, consulta [Obtener el rol de ejecución del dominio](#).

Una política de confianza especifica la identidad que pueda asumir un rol. Esta política es necesaria para permitir que el servicio de SageMaker Studio asuma la función de ejecución del dominio. Añada estas dos acciones para que aparezcan de la siguiente manera en su política.

```
{  
  
  "Version": "2012-10-17",  
  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {
```

```
        "Service": [
            "sagemaker.amazonaws.com"
        ],
    },
    "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
    ]
}
]
```

Paso 3: verifique los permisos de acceso a Concesiones de acceso a Amazon S3 necesarios para el rol de ejecución del dominio

Para utilizar Amazon S3 Access Grants, debe adjuntar una política de permisos (ya sea una política integrada o una política gestionada por el cliente) a su función de ejecución de dominios de SageMaker Studio que contenga los siguientes permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix"
            ],
            "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
        }
    ]
}
```

Si no tiene una política que contenga estos permisos, siga las instrucciones de la Guía del usuario de AWS Identity and Access Management para la [Adición y eliminación de permisos de identidad de IAM](#).

## Paso 4: asigne grupos y usuarios al dominio

Para asignar grupos y usuarios al dominio de SageMaker Studio, sigue los pasos que se indican en [Añadir grupos y usuarios](#).

## Paso 5: configure concesiones de acceso a Amazon S3

Para configurar las Concesiones de acceso a Amazon S3, siga los pasos que se indican en [Configuración de las Concesiones de acceso a Amazon S3 para una propagación de identidades de confianza a través de IAM Identity Center](#). Siga las step-by-step instrucciones para completar las siguientes tareas:

1. Cree una instancia de Concesiones de acceso a Amazon S3.
2. Registre una ubicación en esa instancia.
3. Cree concesiones para permitir que usuarios o grupos específicos de IAM Identity Center accedan a las ubicaciones o subconjuntos de Amazon S3 designados (por ejemplo, prefijos específicos) dentro de esas ubicaciones.

## Paso 6: Envíe un trabajo de SageMaker formación y consulte los detalles de la sesión de fondo del usuario

En SageMaker Studio, lanza un nuevo cuaderno de Jupyter y envía un trabajo de formación. Mientras se ejecuta el trabajo, complete los siguientes pasos para ver la información de la sesión y comprobar que el contexto de la sesión de usuario en segundo plano esté activo.

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. En la página Usuarios, elija el nombre de usuario cuyas sesiones desee administrar. Esto lo dirigirá a una página con la información del usuario.
4. En la página del usuario, elija la pestaña Sesiones activas. El número entre paréntesis junto a Sesiones activas indica el número de sesiones activas de este usuario.
5. Para buscar sesiones por el nombre de recurso de Amazon (ARN) del trabajo que utiliza la sesión, en la lista Tipo de sesión, elija Sesiones de usuario en segundo plano y, a continuación, introduzca el ARN del trabajo en el cuadro de búsqueda.

A continuación se muestra un ejemplo de cómo aparece un trabajo de entrenamiento que utiliza una sesión de usuario en segundo plano en la pestaña Sesiones activas de un usuario.



Profile
Groups (0)
AWS accounts
Applications
MFA devices (1)
Active sessions (5)

Active sessions (5)
End sessions

You can end any of the active sessions in this list. The list shows all active sessions initiated by wei\_zhang [Learn more](#)

Session type
All

< 1 >

| <input type="checkbox"/> | Client | Session type          | Used by                                                                            | IP address |
|--------------------------|--------|-----------------------|------------------------------------------------------------------------------------|------------|
| <input type="checkbox"/> | -      | User background se... | arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b | -          |

## Paso 7: Vea los CloudTrail registros para verificar la propagación de identidad confiable en CloudTrail

Cuando la propagación de identidad confiable está habilitada, las acciones aparecen en los registros de CloudTrail eventos debajo del `onBehalfOf` elemento. `userId` refleja el ID del usuario de IAM Identity Center que inició el trabajo de entrenamiento. El siguiente CloudTrail evento captura el proceso de propagación de identidades confiables.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        },
        "onBehalfOf": {
          "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",

```

```
"identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/d-1234567890"
  }
},
```

## Consideraciones sobre el tiempo de ejecución

Si un administrador decide realizar tareas `MaxRuntimeInSeconds` de formación o procesamiento de larga duración que sean inferiores a la duración de la sesión en segundo plano del usuario, SageMaker Studio ejecuta la tarea durante el tiempo mínimo de la sesión en segundo plano del usuario `MaxRuntimeInSeconds` o la duración mínima de la sesión en segundo plano.

Para obtener más información al respecto `MaxRuntimeInSeconds`, consulta la guía del `CreateTrainingJob` [StoppingCondition](#) parámetro en la Amazon SageMaker API Reference.

## Autorización de servicios

En todos los [casos de uso de análisis y almacén de lago de datos](#), puede lograr controles de acceso detallados mediante:

- AWS Lake Formation - para obtener orientación, consulte [Configuración AWS Lake Formation con IAM Identity Center](#).
- Amazon S3 Access Grants: para obtener instrucciones, consulte [Configuración de Concesiones de acceso a Amazon S3 con IAM Identity Center](#).

## Configuración AWS Lake Formation con IAM Identity Center

[AWS Lake Formation](#) es un servicio administrado que simplifica la creación y administración de lagos de datos en AWS. Automatiza la recopilación, la catalogación y la seguridad de los datos, y proporciona un repositorio centralizado para almacenar y analizar diversos tipos de datos. Lake Formation ofrece controles de acceso detallados y se integra con varios servicios de AWS análisis, lo que permite a las organizaciones configurar, proteger y obtener información de manera eficiente de sus lagos de datos.

Siga estos pasos para permitir que Lake Formation conceda permisos de datos en función de la identidad del usuario mediante IAM Identity Center y la propagación de identidades de confianza.

## Requisitos previos

Antes de empezar con este tutorial, primero tendrá que configurar lo siguiente:

- [Habilite el IAM Identity Center](#). Se recomienda la [instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).

## Pasos para configurar la propagación de identidades de confianza

1. Integre IAM Identity Center con AWS Lake Formation siguiendo las instrucciones de [Conexión de Lake Formation con IAM Identity Center](#).

### Important

Si no tiene tablas de AWS Glue Data Catalog, debe crearlas para poder utilizar AWS Lake Formation a fin de conceder acceso a los usuarios y grupos de IAM Identity Center. Consulte [Creación de objetos en AWS Glue Data Catalog](#) para obtener más información.

2. Registre las ubicaciones de los lagos de datos.

[Registre las ubicaciones de S3](#) donde se almacenan los datos de las tablas de Glue. De este modo, Lake Formation proporcionará acceso temporal a las ubicaciones de S3 requeridas cuando se consulten las tablas, lo que eliminará la necesidad de incluir permisos de S3 en la función de servicio (por ejemplo, la función de servicio de Athena configurada en WorkGroup).

- a. Diríjase a las ubicaciones de los lagos de datos en la sección Administración del panel de navegación de la AWS Lake Formation consola. Seleccione Registrar ubicación.

Esto permitirá a Lake Formation proporcionar credenciales de IAM temporales con los permisos necesarios para acceder a las ubicaciones de datos de S3.

**Register location**

**Amazon S3 location**  
Register an Amazon S3 path as the storage location for your data lake.

**Amazon S3 path**  
Choose an Amazon S3 path for your data lake.

**Review location permissions - strongly recommended**  
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

**IAM role**  
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

☐ **Enable Data Catalog Federation**  
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

**Permission mode**  
Select the permission mode you want to use to manage access.

☒ **Hybrid access mode**  
Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access.  
[Learn more](#)

☐ **Lake Formation**  
Only Lake Formation permissions are enforced.

- b. Introduzca la ruta de S3 de las ubicaciones de los datos de las tablas de AWS Glue en el campo Ruta de Amazon S3.
- c. En la sección Roles de IAM, no seleccione el rol vinculado al servicio si quiere utilizarlo con una propagación de identidades de confianza. Cree un rol con los siguientes permisos:

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Creación de una política](#) o [Edición de una política](#). La política de permisos debe permitir el acceso a la ubicación de S3 especificada en la ruta:

- i. Política de permisos

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
```

```

        "arn:aws:s3:::Your-S3-Bucket/*"
    ],
    },
    {
        "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket"
        ]
    },
    {
        "Sid": "LakeFormationDataAccessServiceRolePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
]
}

```

- ii. Relación de confianza: debe incluir `sts:SectContext`, lo cual es obligatorio para la propagación de identidades de confianza.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",

```

```
    "sts:SetContext"  
  ]  
}  
]
```

 Note

El rol de IAM creado por el asistente es un rol vinculado a un servicio y no incluye `sts:SetContext`.

- d. Tras crear el rol de IAM, seleccione Registrar ubicación.

## Propagación de identidad confiable con Lake Formation across Cuentas de AWS

AWS Lake Formation admite el uso de [AWS Resource Access Manager \(RAM\)](#) para compartir tablas Cuentas de AWS y funciona con la propagación de identidades confiable cuando la cuenta del otorgante y la cuenta del concesionario están en la misma Región de AWS, en la misma instancia de la organización y comparten la misma AWS Organizations instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Cross-account data sharing in Lake Formation](#).

## Configuración de Concesiones de acceso a Amazon S3 con IAM Identity Center

[Amazon S3 Access Grants](#) ofrece la flexibilidad necesaria para conceder un control de acceso detallado basado en la identidad a las ubicaciones de S3. Puede usar Amazon S3 Access Grants concede a los buckets de Amazon S3 acceso directo a los usuarios y grupos corporativos. Siga estos pasos para habilitar S3 Access Grants con IAM Identity Center y lograr una propagación de identidades de confianza.

### Requisitos previos

Antes de empezar con este tutorial, primero tendrá que configurar lo siguiente:

- [Habilite el Centro de identidades de IAM](#). Se recomienda la [instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).

## Configuración de Concesiones de acceso de S3 para una propagación de identidades de confianza a través de IAM Identity Center

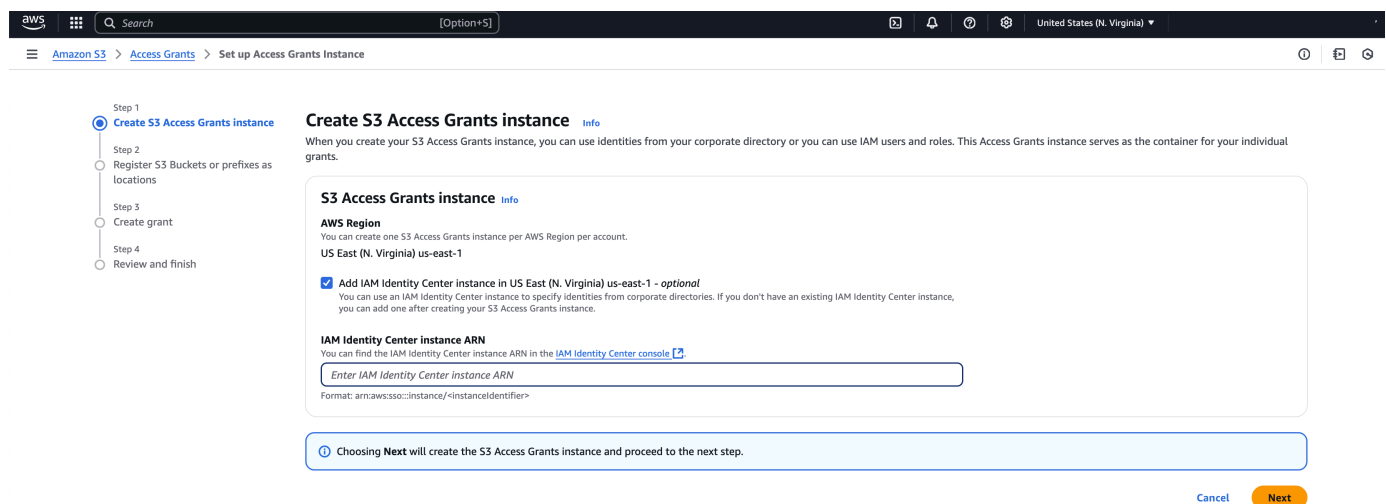
Si ya tiene una instancia de Amazon S3 Access Grants con una ubicación registrada, siga estos pasos:

1. [Asocie o desasocie su instancia de IAM Identity Center.](#)
2. [Cree una concesión](#)

Si aún no ha creado un Amazon S3 Access Grants, siga estos pasos:

1. [Crear una Access Grants instancia S3](#): puede crear una Access Grants instancia S3 por cada instancia. Región de AWS Al crear la instancia de S3 Access Grants, asegúrese de marcar la casilla Agregar una instancia de IAM Identity Center y de proporcionar el ARN de su instancia de IAM Identity Center. Seleccione Siguiente.

La siguiente imagen muestra la página Crear instancia de S3 Access Grants en la consola de Amazon S3 Access Grants:



2. Registrar una ubicación: después de crear y [crear una Access Grants instancia de Amazon S3](#) Región de AWS en una de su cuenta, [registra una ubicación S3](#) en esa instancia. Una ubicación de S3 Access Grants asigna la región predeterminada de S3 (S3://), un bucket o un prefijo a un rol de IAM. S3 Access Grants asume este rol de Amazon S3 para vender credenciales temporales al beneficiario que accede a esa ubicación en particular. En primer lugar, debe

registrar al menos una ubicación en su instancia de S3 Access Grants para poder crear una concesión de acceso.

Para el ámbito de ubicación, especifique `s3://`, que incluye todos los buckets de esa región. Este es el ámbito de ubicación recomendado para la mayoría de los casos de uso. Si tiene un caso de uso de administración de acceso avanzada, puede establecer el ámbito de ubicación en un bucket específico `s3://bucket` o en un prefijo dentro de un bucket `s3://bucket/prefix-with-path`. Para obtener más información, consulte [Registrar una ubicación](#) en la Guía del usuario de Amazon Simple Storage Service.

 Note

Asegúrese de que las ubicaciones S3 de las AWS Glue tablas a las que quiere conceder acceso estén incluidas en esta ruta.

El procedimiento requiere que configure un rol de IAM para la ubicación. Este rol debe incluir permisos para acceder al ámbito de la ubicación. Puede utilizar la consola de S3 para crear este rol. Deberá especificar el ARN de su instancia de S3 Access Grants en las políticas de este rol de IAM. El valor predeterminado del ARN de la instancia de S3 Access Grants es `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`.

En el siguiente ejemplo de política de permisos se otorgan permisos a Amazon S3 para el rol de IAM que ha creado. La política de confianza de ejemplo que le sigue permite a la entidad principal del servicio de S3 Access Grants asumir el rol de IAM.

a. Política de permisos

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Creación de una política](#) o [Edición de una política](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
```



```

    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    }
},
{
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    }
}

```

```

        }
    },
    {
        "Sid": "BucketLevelReadPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "111122223333"
            },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                ]
            }
        }
    },
    {
        "Sid": "OptionalKMSPermissionsForSSEEncryption",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

#### b. Política de confianza

En la política de confianza del rol de IAM, proporcione al servicio de Concesiones de acceso a Amazon S3 acceso de entidad principal (`access-grants.s3.amazonaws.com`) al rol de IAM que ha creado. Para ello, puede crear un archivo JSON que contenga las siguientes

instrucciones. Para agregar la política de confianza a su cuenta, consulte [Creación de un rol mediante políticas de confianza personalizadas](#).

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}
```

```
]
}
```

## Creación de una concesión de acceso de Amazon S3

Si tiene una instancia de Amazon S3 Access Grants con una ubicación registrada y ha asociado su instancia de IAM Identity Center a ella, puede [crear una concesión](#). En la página Crear concesión de la consola de S3, complete lo siguiente:

### Crear una concesión

1. Seleccione la ubicación que creó en el paso anterior. Puede reducir el ámbito de la concesión añadiendo un subprefijo. El subprefijo puede ser un bucket, bucket/prefix o un objeto del bucket. Para obtener más información, consulte [Subprefijo](#) en la Guía del usuario de Amazon Simple Storage Service.
2. En Permisos y acceso, seleccione Leer o Escribir según sus necesidades.
3. En Tipo de otorgante, elija Identidad de directorio en IAM Identity Center.
4. Proporcione el ID de usuario o grupo de IAM Identity Center. Puede encontrar el usuario y el grupo IDs en la consola del IAM Identity Center, en [las secciones Usuario y Grupo](#). Seleccione Siguiente.
5. En la página Revisar y finalizar, revise la configuración de S3 Access Grant y, a continuación, seleccione Crear concesión.

La siguiente imagen muestra la página Crear concesión en la consola de Amazon S3 Access Grants:

RWS

Search

[Option+]

United States (N. Virginia)

Create Grant

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://

Browse locations

Register location

Location ID

IAM role

sAccessGrants\_role\_for\_location\_for\_awsids-albi-sandbox-storage

Subprefix - optional

Further scope the grant to a bucket, prefix, or an individual object.  
Format for bucket: <bucket>  
Format for prefix: <bucket>/<prefix-with-path>\*  
Format for object: <bucket>/<prefix-with-path>/<object>

bucket-name/prefix\*

Grant scope

s3://

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read  
☐ Write

Grantee type

☒ Directory identity from IAM Identity Center  
☐ IAM principal

Directory identity type

☐ User  
☒ Group

IAM Identity Center group ID

The group that you want to grant this level of access to. You can find the ID in the IAM Identity Center console

Enter group ID

# Cómo configurar su propia aplicación OAuth 2.0

La propagación fiable de la identidad permite que una aplicación gestionada por el cliente solicite el acceso a los datos de AWS los servicios en nombre de un usuario. La administración del acceso a los datos se basa en la identidad del usuario, por lo que los administradores pueden conceder el acceso en función de la pertenencia actual de los usuarios a grupos y usuarios. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en registros y CloudTrail eventos específicos del servicio.

Con la propagación de identidades de confianza, un usuario puede iniciar sesión en una aplicación administrada por el cliente y esa aplicación puede transmitir la identidad del usuario en las solicitudes de acceso a los datos de los Servicios de AWS.

**⚠ Important**

Para acceder a una Servicio de AWS, las aplicaciones gestionadas por el cliente deben obtener un token de un emisor de token de confianza, que sea externo al Centro de Identidad de IAM. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan las aplicaciones que inician solicitudes de acceso a

Servicios de AWS (aplicaciones receptoras). Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

## Temas

- [Configure aplicaciones OAuth 2.0 administradas por el cliente para una propagación de identidad confiable](#)
- [Especificación de las aplicaciones de confianza](#)
- [Uso de aplicaciones con un emisor de tokens de confianza](#)

## Configure aplicaciones OAuth 2.0 administradas por el cliente para una propagación de identidad confiable

Para configurar una aplicación OAuth 2.0 gestionada por el cliente para la propagación de identidades de forma fiable, primero debe añadirla al Centro de identidades de IAM. Siga el procedimiento que se indica a continuación para agregar su aplicación a IAM Identity Center.

## Temas

- [Paso 1: selección del tipo de aplicación](#)
- [Paso 2: especificación de los detalles de la aplicación](#)
- [Paso 3: especificación de la configuración de autenticación](#)
- [Paso 4: especificación de las credenciales de la aplicación](#)
- [Paso 5: revisión y configuración](#)

## Paso 1: selección del tipo de aplicación

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, elija OAuth 2.0.

7. Seleccione Siguiente para continuar a la página siguiente, [Paso 2: especificación de los detalles de la aplicación](#).

## Paso 2: especificación de los detalles de la aplicación

1. En la página Especificar detalles de la aplicación, en Nombre y descripción de la aplicación, ingrese un Nombre de visualización para la aplicación, como **MyApp**. Escriba una descripción en Descripción.
2. En Método de asignación de usuarios y grupos, seleccione una de las siguientes opciones:
  - Requerir asignaciones: permita que solo los usuarios y grupos de IAM Identity Center que estén asignados a esta aplicación accedan a la aplicación.

Visibilidad del mosaico de la aplicación: solo los usuarios que estén asignados a la aplicación directamente o mediante una asignación grupal pueden ver el mosaico de la aplicación en el portal de AWS acceso, siempre que la visibilidad de la aplicación en el portal de AWS acceso esté establecida en Visible.

- No requerir asignaciones: permita que todos los usuarios y grupos autorizados de IAM Identity Center accedan a esta aplicación.

Visibilidad del mosaico de la aplicación: el mosaico de la aplicación es visible para todos los usuarios que inician sesión en el portal de AWS acceso, a menos que la visibilidad de la aplicación en el portal de AWS acceso esté configurada como No visible.

3. En el portal de AWS acceso, introduzca la URL desde la que los usuarios pueden acceder a la aplicación y especifique si el icono de la aplicación estará visible o no en el portal de AWS acceso. Si selecciona No visible, ni siquiera los usuarios asignados podrán ver el icono de la aplicación.
4. Expanda Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique los valores de Clave y Valor (opcional).

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

5. Seleccione Siguiente y pase a la página siguiente, [Paso 3: especificación de la configuración de autenticación](#).

## Paso 3: especificación de la configuración de autenticación

Para añadir una aplicación gestionada por el cliente que sea compatible con la OAuth versión 2.0 al IAM Identity Center, debe especificar un emisor de token de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes (aplicaciones solicitantes) de acceso a aplicaciones administradas por AWS (aplicaciones receptoras).

1. En la página Especificar configuración de autenticación, en Emisores de tokens de confianza, realice una de las siguientes acciones:

- Para usar un emisor de tokens de confianza existente:

Seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que desea usar.

- Para agregar un nuevo emisor de tokens de confianza:

1. Seleccione Crear emisor de tokens de confianza.
2. Se abrirá una nueva pestaña del navegador. Siga los pasos del 5 al 8 que se indican en [Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center](#).
3. Tras completar estos pasos, regrese a la ventana del navegador que está utilizando para configurar la aplicación y seleccione el emisor de tokens de confianza que acaba de agregar.
4. En la lista de emisores de tokens de confianza, seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que acaba de agregar.

Tras seleccionar un emisor de tokens de confianza, aparece la sección Configurar los emisores de tokens de confianza seleccionados.

2. En Configurar los emisores de tokens de confianza seleccionados, ingrese la notificación de audiencia. La notificación de audiencia identifica a la audiencia objetivo (destinatarios) del token que ha generado el emisor de tokens de confianza. Para obtener más información, consulte [Notificación de audiencia](#).
3. Para evitar que sus usuarios tengan que volver a autenticarse cuando utilicen esta aplicación, seleccione Habilitar la concesión de tokens de actualización. Si está seleccionada, esta opción actualiza el token de acceso de la sesión cada 60 minutos, hasta que la sesión caduque o el usuario la finalice.
4. Seleccione Siguiente y pase a la página siguiente, [Paso 4: especificación de las credenciales de la aplicación](#).



## Paso 4: especificación de las credenciales de la aplicación

Complete los pasos de este procedimiento para especificar las credenciales que la aplicación utilizará para realizar acciones de intercambio de tokens con aplicaciones de confianza. Estas credenciales se utilizan en una política basada en recursos. La política requiere que especifique una entidad principal que tenga permisos para realizar las acciones que se especifican en la política. Debe especificar una entidad principal, incluso si las aplicaciones de confianza se encuentran en la misma Cuenta de AWS.

### Note

Cuando establezca permisos con políticas, conceda solo los permisos necesarios para llevar a cabo una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos.

Esta política requiere la acción de la API [CreateTokenWithIAM](#). Para obtener más información sobre esta política y un ejemplo que pueda adaptar según sea necesario para su entorno, consulte [Ejemplos de política basada en recursos para IAM Identity Center](#).

1. En la página Especificar las credenciales de la aplicación, lleve a cabo una de las siguientes acciones:
  - Para especificar rápidamente uno o varios roles de IAM:
    1. Seleccione Ingresar uno o más roles de IAM.
    2. En Ingresar roles de IAM, especifique el nombre de recurso de Amazon (ARN) de un rol de IAM existente. Para especificar el ARN, utilice la siguiente sintaxis. La parte de la región del ARN está en blanco porque los recursos de IAM son globales.

```
arn:aws:iam::account:role/role-name-with-path
```

Para obtener más información, consulte el artículo [Acceso entre cuentas mediante políticas basadas en recursos](#) e [IAM ARNs](#) en la Guía del usuario.AWS Identity and Access Management

- Para editar la política manualmente (obligatorio si no especificas credenciales):AWS
  1. Seleccione Editar la política de la aplicación.

2. Para modificar la política, escriba o pegue texto en el cuadro de texto JSON.
  3. Resuelva las advertencias de seguridad, errores o advertencias generales que hayan surgido durante la validación de la política. Para obtener más información, consulte [Validación de políticas de IAM](#) en la Guía del usuario de AWS Identity and Access Management .
2. Seleccione Siguiente y pase a la página siguiente, [Paso 5: revisión y configuración](#).

## Paso 5: revisión y configuración

1. En la página Revisar y configurar, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar y, a continuación, realice los cambios necesarios.
2. Cuando haya terminado, seleccione Agregar aplicación.
3. La aplicación que ha agregado aparece en la lista Aplicaciones administradas por el cliente.
4. Tras configurar la aplicación gestionada por el cliente en el Centro de identidades de IAM, debe especificar una o más Servicios de AWS aplicaciones de confianza para la propagación de la identidad. Esto permite a los usuarios iniciar sesión en la aplicación administrada por el cliente y acceder a los datos de la aplicación de confianza.

Para obtener más información, consulte [Especificación de las aplicaciones de confianza](#).

## Especificación de las aplicaciones de confianza

Tras [configurar la aplicación gestionada por el cliente](#), debe especificar uno o más AWS servicios o aplicaciones de confianza para la propagación de la identidad. Especifique un AWS servicio que contenga datos a los que los usuarios de las aplicaciones gestionadas por el cliente necesiten acceder. Cuando los usuarios inicien sesión en la aplicación administrada por el cliente, esa aplicación transferirá la identidad de los usuarios a la aplicación de confianza.

Utilice el siguiente procedimiento para seleccionar un servicio y, a continuación, especifique las aplicaciones individuales que son de confianza para ese servicio.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.

4. En la lista de aplicaciones administradas por el cliente, seleccione la aplicación OAuth 2.0 a la que desee iniciar las solicitudes de acceso. Esta es la aplicación en la que inician sesión los usuarios.
5. En la página de detalles, en Aplicaciones de confianza para la propagación de identidades, seleccione Especificar aplicaciones de confianza.
6. En Tipo de configuración, seleccione Aplicaciones individuales y acceso específico y, a continuación, seleccione Siguiente.
7. En la página Seleccionar servicio, seleccione el servicio de AWS que tenga aplicaciones en las que la aplicación administrada por el cliente pueda confiar para propagar identidades y, a continuación, seleccione Siguiente.

El servicio que seleccione define las aplicaciones que son de confianza. Seleccionará las aplicaciones en el siguiente paso.

8. En la página Seleccionar aplicaciones, seleccione Aplicaciones individuales, active la casilla de verificación de cada aplicación que pueda recibir solicitudes de acceso y, a continuación, seleccione Siguiente.
9. En la página Configurar el acceso, en Método de configuración, realice una de las siguientes acciones:
  - Seleccionar el acceso por aplicación: seleccione esta opción para configurar diferentes niveles de acceso para cada aplicación. Seleccione la aplicación para la que desee configurar el nivel de acceso y, a continuación, seleccione Editar acceso. En Nivel de acceso que aplicar, cambie los niveles de acceso según sea necesario y, a continuación, seleccione Guardar cambios.
  - Aplicar el mismo nivel de acceso a todas las aplicaciones: seleccione esta opción si no tiene que configurar los niveles de acceso por aplicación.
10. Elija Siguiente.
11. En la página Revisar configuración, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar acceso y, a continuación, realice los cambios necesarios.
12. Cuando haya terminado, seleccione Aplicaciones de confianza.

## Uso de aplicaciones con un emisor de tokens de confianza

Los emisores de tokens confiables le permiten utilizar la propagación de identidades confiable con aplicaciones que se autentican fuera de ella. AWS Con los emisores de tokens de confianza, puede

autorizar a estas aplicaciones a realizar solicitudes en nombre de sus usuarios para acceder AWS a las aplicaciones gestionadas.

En los siguientes temas se describe cómo funcionan los emisores de tokens de confianza y se proporcionan instrucciones de configuración.

## Temas

- [Descripción general de los emisores de tokens de confianza](#)
- [Requisitos previos y consideraciones para los emisores de tokens de confianza](#)
- [Detalles de la notificación de JTI](#)
- [Ajustes de configuración de un emisor de tokens de confianza](#)
- [Configuración de un emisor de tokens de confianza](#)
- [Sesiones de rol de IAM con identidad mejorada](#)

## Descripción general de los emisores de tokens de confianza

La propagación de identidades fiable proporciona un mecanismo que permite a las aplicaciones que se autentican fuera del AWS sistema realizar solicitudes en nombre de sus usuarios mediante el uso de un emisor de token de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes (solicitudes de solicitudes) de acceso a Servicios de AWS (aplicaciones receptoras). Las aplicaciones solicitantes inician las solicitudes de acceso en nombre de los usuarios que el emisor de tokens de confianza autentica. Tanto el emisor de tokens de confianza como IAM Identity Center conocen a los usuarios.

**Servicios de AWS** Las personas que reciben solicitudes gestionan la autorización detallada de sus recursos en función de sus usuarios y de la pertenencia a grupos, tal y como se muestran en el directorio de Identity Center. Servicios de AWS no pueden usar directamente los tokens del emisor externo del token.

Para resolver este problema, IAM Identity Center proporciona una forma para que la aplicación solicitante, o un controlador de AWS que utilice la aplicación solicitante, intercambie el token que emite el emisor de tokens de confianza por un token generado por IAM Identity Center. El token que genera IAM Identity Center hace referencia al usuario correspondiente de IAM Identity Center. La aplicación solicitante, o el controlador, utiliza el nuevo token para iniciar una solicitud a la aplicación receptora. Como el nuevo token hace referencia al usuario correspondiente de IAM Identity Center,

la aplicación receptora puede autorizar el acceso solicitado en función del usuario o de su grupo, tal como se representa en IAM Identity Center.

#### Important

Elegir un servidor de autorización OAuth 2.0 para añadirlo como emisor de token de confianza es una decisión de seguridad que requiere una cuidadosa consideración. Seleccione únicamente emisores de tokens de confianza para realizar las siguientes tareas:

- Autenticar al usuario especificado en el token.
- Autorizar el acceso de ese usuario a la aplicación receptora.
- Generar un token que IAM Identity Center pueda intercambiar por un token creado por IAM Identity Center.

## Requisitos previos y consideraciones para los emisores de tokens de confianza

Antes de configurar un emisor de tokens de confianza, revise los siguientes requisitos previos y consideraciones.

- Configuración de un emisor de tokens de confianza

Debe configurar un servidor de autorización OAuth 2.0 (el emisor de token de confianza). Aunque el emisor del token de confianza suele ser el proveedor de identidad que utilizas como fuente de identidad para el IAM Identity Center, no tiene por qué serlo. Para ver instrucciones sobre cómo configurar el emisor de tokens de confianza, consulte la documentación del proveedor de identidades correspondiente.

#### Note

Puede configurar hasta 10 emisores de tokens de confianza para utilizarlos con IAM Identity Center, siempre que asigne la identidad de cada usuario del emisor de tokens de confianza a un usuario correspondiente de IAM Identity Center.

- El servidor de autorización OAuth 2.0 (el emisor del token de confianza) que crea el token debe tener un punto final de descubrimiento [OpenID Connect \(OIDC\)](#) que IAM Identity Center pueda utilizar para obtener claves públicas para verificar las firmas del token. Para obtener más información, consulte [URL del punto de conexión de detección de OIDC \(URL del emisor\)](#).

- Tokens emitidos por el emisor de tokens de confianza

Los tokens del emisor de tokens de confianza deben cumplir los siguientes requisitos:

- El token debe estar firmado y en [formato JSON Web Token \(JWT\)](#) mediante el algoritmo. RS256
- El token debe contener las siguientes afirmaciones:
  - [Emisor](#) (iss): la entidad que emitió el token. Este valor debe coincidir con el valor que está configurado en el punto de conexión de detección del OIDC (URL del emisor) en el emisor del token de confianza.
  - [Sujeto](#) (sub): el usuario autenticado.
  - [Público](#) (aud): el destinatario previsto del token. Este es el Servicio de AWS al que se accederá después de cambiarlo por un token de IAM Identity Center. Para obtener más información, consulte [Notificación de audiencia](#).
  - [Tiempo de caducidad](#) (exp): el tiempo después del cual caduca el token.
- El token puede ser un token de identidad o un token de acceso.
- El token debe tener un atributo que pueda asignarse de forma exclusiva a un usuario de IAM Identity Center.

 Note

No se admite el uso de una clave de firma personalizada para JWTs from Microsoft Entra ID. Para usar tokens de Microsoft Entra ID con un emisor de tokens de confianza, no puede usar una clave de firma personalizada.

- Notificaciones opcionales

IAM Identity Center admite todas las notificaciones opcionales que se definen en RFC 7523. Para obtener más información, consulte la [sección 3: JWT Format and Processing Requirements](#) de esta RFC.

Por ejemplo, el token puede contener una [notificación de JTI \(ID de JWT\)](#). Esta notificación, cuando está presente, impide que los tokens que tienen el mismo JTI se reutilicen para el intercambio de tokens. Para obtener más información acerca de las notificaciones de JTI, consulte [Detalles de la notificación de JTI](#).

- Configuración de IAM Identity Center para que funcione con un emisor de tokens de confianza

También debe habilitar IAM Identity Center, configurar el origen de identidad de IAM Identity Center y aprovisionar a los usuarios que correspondan a los usuarios del directorio del emisor de tokens de confianza.

Para ello, debe hacer una de las siguientes acciones:

- Sincronice los usuarios con IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) 2.0.
- Cree los usuarios directamente en IAM Identity Center.

## Detalles de la notificación de JTI

Si IAM Identity Center recibe una solicitud para intercambiar un token que IAM Identity Center ya ha intercambiado, se produce un error en la solicitud. Para detectar e impedir la reutilización de un token para los intercambios de tokens, puede incluir una notificación de JTI. IAM Identity Center protege contra la repetición de tokens en función de las notificaciones que figuran en el token.

No todos los servidores de autorización OAuth 2.0 añaden una declaración de JTI a los tokens. Es posible que algunos servidores de autorización OAuth 2.0 no te permitan añadir una JTI como afirmación personalizada. OAuth Los servidores de autorización 2.0 que admiten el uso de una declaración de JTI pueden añadir esta afirmación únicamente a los tokens de identidad, solo a los de acceso o a ambos. Para obtener más información, consulte la documentación de su servidor de autorización OAuth 2.0.

Para obtener información sobre cómo crear aplicaciones que intercambien tokens, consulte la documentación de la API de IAM Identity Center. Para obtener información sobre cómo configurar una aplicación administrada por el cliente para obtener e intercambiar los tokens correctos, consulte la documentación de la aplicación.

## Ajustes de configuración de un emisor de tokens de confianza

En las siguientes secciones se describen los ajustes necesarios para configurar y utilizar un emisor de tokens de confianza.

### Temas

- [URL del punto de conexión de detección de OIDC \(URL del emisor\)](#)
- [Mapeo de atributos](#)
- [Notificación de audiencia](#)

## URL del punto de conexión de detección de OIDC (URL del emisor)

Al agregar un emisor de tokens de confianza a la consola de IAM Identity Center, debe especificar la URL del punto de conexión de detección de OIDC. Se suele hacer referencia a esta URL por su URL relativa, `/.well-known/openid-configuration`. En la consola de IAM Identity Center, esta URL se denomina URL del emisor.

### Note

Debe pegar la URL del punto de conexión de detección hasta que no aparezca `.well-known/openid-configuration`. Si `.well-known/openid-configuration` se incluye en la URL, la configuración del emisor del token de confianza no funcionará. Como el IAM Identity Center no valida esta URL, si la URL no está formada correctamente, la configuración del emisor de token de confianza fallará sin notificación.

Solo se debe poder acceder a la URL del punto de conexión de detección del OIDC a través de los puertos 80 y 443.

IAM Identity Center utiliza esta URL para obtener información adicional sobre el emisor de tokens de confianza. Por ejemplo, IAM Identity Center utiliza esta URL para obtener la información necesaria para verificar los tokens que genera el emisor de tokens de confianza. Al agregar un emisor de tokens de confianza a IAM Identity Center, debe especificar esta URL. Para encontrar la URL, consulte la documentación del proveedor del servidor de autorización OAuth 2.0 que utilice para generar los tokens para su aplicación o póngase en contacto directamente con el proveedor para obtener ayuda.

## Mapeo de atributos

Las asignaciones de atributos permiten que IAM Identity Center vincule el usuario representado en un token emitido por un emisor de tokens de confianza con un único usuario de IAM Identity Center. Debe especificar la asignación de atributos al agregar el emisor de tokens de confianza a IAM Identity Center. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario de IAM Identity Center, que se utilizará como el usuario de AWS. La notificación que elija debe asignarse a un atributo de una lista fija de atributos disponibles en el almacén de identidades de IAM Identity Center. Puede elegir uno de los siguientes atributos del almacén de identidades de IAM Identity



Center: nombre de usuario, correo electrónico e ID externo. El valor del atributo que especifique en IAM Identity Center debe ser único para cada usuario.

## Notificación de audiencia

Las notificaciones de audiencia identifican a la audiencia (destinatarios) a la que se destina un token. Cuando la aplicación que solicita el acceso se autentica a través de un proveedor de identidades que no está federado en IAM Identity Center, dicho proveedor de identidades debe configurarse como un emisor de tokens de confianza. La aplicación que recibe la solicitud de acceso (la aplicación receptora) debe cambiar el token que ha generado el emisor de tokens de confianza por un token que haya generado IAM Identity Center.

Para obtener información sobre cómo obtener los valores de la notificación de audiencia para la aplicación receptora tal como están registrados en el emisor de tokens de confianza, consulte la documentación del emisor de tokens de confianza o póngase en contacto con el administrador del emisor de tokens de confianza para obtener ayuda.

## Configuración de un emisor de tokens de confianza

Para habilitar la propagación de identidades de confianza en una aplicación que se autentica externamente en IAM Identity Center, uno o más administradores deben configurar un emisor de tokens de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que emite tokens a las aplicaciones que inician solicitudes (solicitudes de solicitudes). Los tokens autorizan a estas aplicaciones a iniciar solicitudes en nombre de sus usuarios a una aplicación o aplicaciones receptoras Servicio de AWS.

### Temas

- [Coordinación de los roles y responsabilidades de administración](#)
- [Tareas para configurar un emisor de tokens de confianza](#)
- [Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center](#)
- [Cómo ver o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center](#)
- [Proceso de configuración y flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza](#)

## Coordinación de los roles y responsabilidades de administración

En algunos casos, un único administrador puede realizar todas las tareas necesarias para configurar un emisor de tokens de confianza. Si varios administradores realizan estas tareas, es necesario que haya una estrecha coordinación. En la siguiente tabla se describe cómo varios administradores pueden coordinarse para configurar un emisor de token de confianza y configurar el AWS servicio para usarlo.

### Note

La aplicación puede ser cualquier AWS servicio que esté integrado con el Centro de Identidad de IAM y permita la propagación de identidades de forma fiable.

Para obtener más información, consulte [Tareas para configurar un emisor de tokens de confianza](#).

| Rol                                                           | Realiza estas tareas                                                                                                                                                                                                                                                                                                                                    | Se coordina con                                                                                            |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Administrador del IAM Identity Center                         | <p>Agrega el IdP externo como emisor de tokens de confianza a la consola de IAM Identity Center.</p> <p>Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo.</p> <p>Notifica al administrador del AWS servicio cuando el emisor del token de confianza se añade a la consola del IAM Identity Center.</p> | <p>Administrador del IdP externo (emisor de tokens de confianza)</p> <p>AWS administrador del servicio</p> |
| Administrador del IdP externo (emisor de tokens de confianza) | <p>Configura el IdP externo para emitir los tokens.</p> <p>Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo.</p>                                                                                                                                                                                       | <p>Administrador del IAM Identity Center</p> <p>AWS administrador de servicios</p>                         |

| Rol                            | Realiza estas tareas                                                                                                                                                                                                                                                                                                                                  | Se coordina con                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
|                                | Proporciona el nombre de la audiencia (notificación de audiencia ) al administrador del servicio de AWS .                                                                                                                                                                                                                                             |                                                                                                                   |
| AWS administrador de servicios | <p>Busca en la consola AWS de servicio el emisor del token de confianza. El emisor del token de confianza estará visible en la consola de AWS servicio después de que el administrador del IAM Identity Center lo añada a la consola del IAM Identity Center.</p> <p>Configura el AWS servicio para que utilice el emisor del token de confianza.</p> | <p>Administrador del IAM Identity Center</p> <p>Administrador del IdP externo (emisor de tokens de confianza)</p> |

## Tareas para configurar un emisor de tokens de confianza

Para configurar un emisor de tokens de confianza, un administrador de IAM Identity Center, un administrador del IdP externo (emisor de tokens de confianza) y un administrador de aplicaciones deben realizar las siguientes tareas.

### Note

La aplicación puede ser cualquier AWS servicio que esté integrado con el IAM Identity Center y permita la propagación de identidades de forma fiable.

1. Agregue el emisor de token de confianza al Centro de Identidad de IAM: el administrador del Centro de Identidad de IAM [agrega el emisor de token de confianza mediante la consola del Centro de Identidad de IAM](#) o. [APIs](#) Esta configuración requiere especificar lo siguiente:
  - El nombre del emisor de tokens de confianza.

- La URL del punto de conexión de detección de OIDC (en la consola de IAM Identity Center, esta URL se denomina URL del emisor). Solo se debe poder acceder al punto de conexión de detección a través de los puertos 80 y 443.
  - Asignación de atributos para la búsqueda de usuarios. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario en IAM Identity Center.
2. Conectar el AWS servicio al IAM Identity Center: el administrador del AWS servicio debe conectar la aplicación al IAM Identity Center mediante la consola de la aplicación o la aplicación. APIs

Una vez que el emisor del token de confianza se haya añadido a la consola del IAM Identity Center, también estará visible en la consola de AWS servicio y estará disponible para que el administrador del AWS servicio lo seleccione.

3. Configure el uso del intercambio de tokens: en la consola de AWS servicio, el administrador del AWS servicio configura el AWS servicio para que acepte los tokens emitidos por el emisor de token de confianza. Estos tokens se intercambian por tokens que ha generado IAM Identity Center. Para ello, es necesario especificar el nombre del emisor de los tokens de confianza del paso 1 y el valor de reclamación en AUD que corresponde al servicio. AWS

El emisor del token de confianza coloca el valor reclamado en AUD en el token que emite para indicar que el token está destinado a ser utilizado por el AWS servicio. Para obtener este valor, póngase en contacto con el administrador del emisor de tokens de confianza.

## Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center

En una organización que tiene varios administradores, esta tarea la realiza un administrador de IAM Identity Center. Si es el administrador de IAM Identity Center, debe elegir qué IdP externo desea utilizar como emisor de tokens de confianza.

Para agregar un emisor de tokens de confianza a la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione Crear emisor de tokens de confianza.

5. En la página Configurar un IdP externo para emitir tokens de confianza, en Detalles del emisor del token de confianza, haga lo siguiente:
  - En URL del emisor, escriba la [URL de detección de OIDC](#) del IdP externo que emitirá los tokens para la propagación de identidades de confianza. Debe especificar la URL del punto de conexión de detección hasta el momento sin `.well-known/openid-configuration`. El administrador del IdP externo puede proporcionar esta URL.

 Note

Nota: Esta URL debe coincidir con la URL de la afirmación del emisor (iss) en los tokens que se emiten para la propagación de identidades confiables.

- En Nombre del emisor de tokens de confianza, ingrese un nombre para identificar a este emisor de tokens de confianza en IAM Identity Center y en la consola de la aplicación.
6. En Asignar atributos, haga lo siguiente:
    - En Atributo de proveedor de identidad, seleccione un atributo de la lista para asignarlo a un atributo del almacén de identidades de IAM Identity Center.
    - En Atributo de IAM Identity Center, seleccione el atributo correspondiente para la asignación de atributos.
  7. En Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique un valor para Clave y, si lo desea, para Valor.

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

8. Seleccione Crear emisor de tokens de confianza.
9. Cuando termine de crear el emisor de tokens de confianza, póngase en contacto con el administrador de la aplicación para que sepa el nombre del emisor de tokens de confianza y así pueda confirmar que está visible en la consola correspondiente.
10. El administrador de la aplicación debe seleccionar este emisor de tokens de confianza en la consola correspondiente para permitir que los usuarios accedan a la aplicación desde las aplicaciones que están configuradas para la propagación de identidades de confianza.

## Cómo ver o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

Tras agregar un emisor de tokens de confianza a la consola de IAM Identity Center, podrá ver y editar la configuración correspondiente.

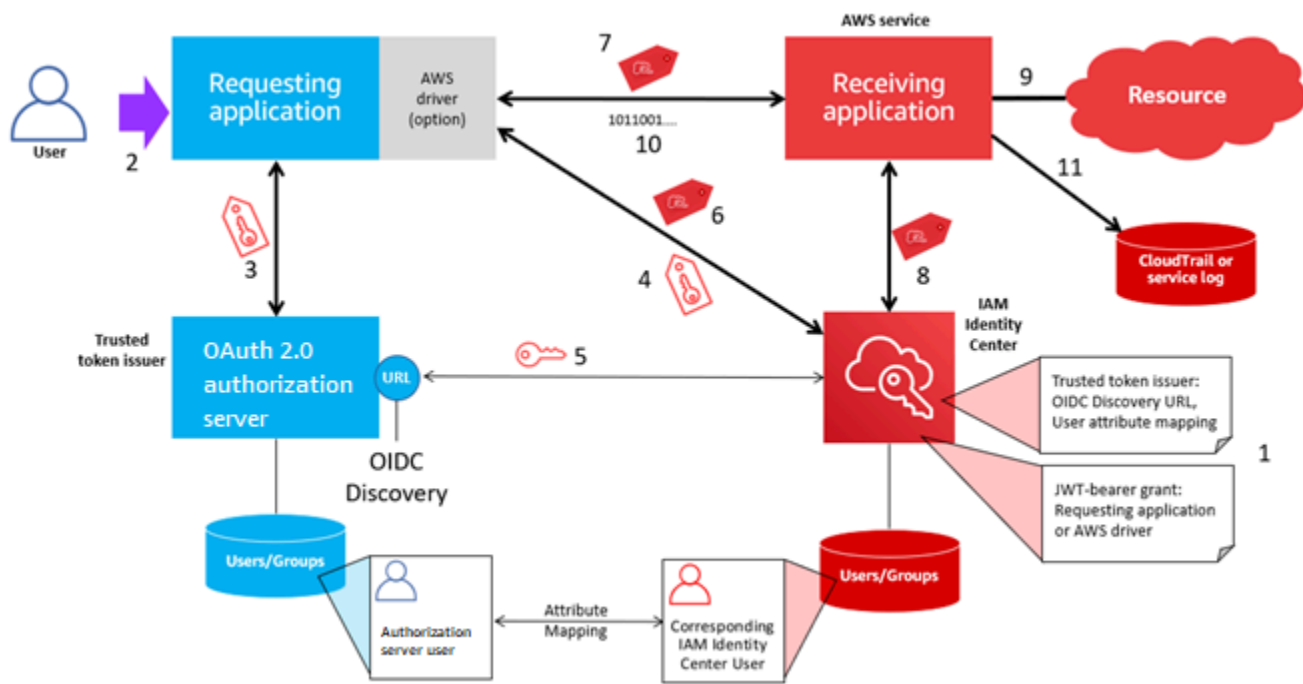
Si tiene previsto editar la configuración del emisor de tokens de confianza, tenga en cuenta que si lo hace, los usuarios podrían perder el acceso a cualquier aplicación que esté configurada para utilizar el emisor de tokens de confianza. Para evitar interrumpir el acceso de los usuarios, le recomendamos que se ponga en contacto con los administradores de cualquier aplicación que esté configurada para usar el emisor de tokens de confianza antes de editar la configuración.

Para visualizar o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione el emisor de tokens de confianza que desee ver o editar.
5. Seleccione Acciones y, a continuación, Editar.
6. En la página Editar emisor de tokens de confianza, consulte o edite la configuración según sea necesario. Puede editar el nombre del emisor de tokens de confianza, las asignaciones de atributos y las etiquetas.
7. Seleccione Save changes (Guardar cambios).
8. En el cuadro de diálogo Editar emisor de tokens de confianza, se le pedirá que confirme que desea realizar cambios. Elija Confirmar.

## Proceso de configuración y flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza

En esta sección se describe el proceso de configuración y el flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza para la propagación de identidades de confianza. En el diagrama siguiente se proporciona una descripción general de este proceso.



En los pasos siguientes tiene más información sobre este proceso.

1. Configure el IAM Identity Center y la aplicación AWS gestionada de recepción para utilizar un emisor de token de confianza. Para obtener información, consulte [Tareas para configurar un emisor de tokens de confianza](#).
2. El flujo de solicitud comienza cuando un usuario abre la aplicación solicitante.
3. La aplicación solicitante solicita un token al emisor del token de confianza para iniciar las solicitudes a la aplicación gestionada receptora AWS. Si el usuario aún no se ha autenticado, este proceso desencadena un flujo de autenticación. El token contiene la siguiente información:
  - El asunto del usuario.
  - El atributo que IAM Identity Center utiliza para buscar al usuario correspondiente en IAM Identity Center.
  - Una notificación de audiencia que contiene un valor que el emisor de tokens de confianza asocia a la aplicación administrada por AWS receptora. Si hay otras notificaciones, IAM Identity Center no las utiliza.
4. La aplicación solicitante, o el AWS controlador que utiliza, pasa el token al Centro de Identidad de IAM y solicita que se cambie por un token generado por el Centro de Identidad de IAM. Si utiliza un controlador de AWS, es posible que tenga que configurarlo para este caso de uso. Para obtener más información, consulte la documentación de la aplicación AWS gestionada correspondiente.

5. IAM Identity Center utiliza el punto de conexión de detección de OIDC para obtener la clave pública que puede utilizar para verificar la autenticidad del token. A continuación, IAM Identity Center hace lo siguiente:
    - Verifica el token.
    - Busca en el directorio de Identity Center. Para ello, IAM Identity Center utiliza el atributo asignado que se especifica en el token.
    - Verifica que el usuario está autorizado para acceder a la aplicación receptora. Si la aplicación AWS gestionada está configurada para requerir asignaciones a usuarios y grupos, el usuario debe tener una asignación directa o basada en grupos a la aplicación; de lo contrario, se deniega la solicitud. Si la aplicación AWS administrada está configurada para no requerir asignaciones de usuarios y grupos, el procesamiento continúa.
-  **Note**

AWS los servicios tienen una configuración predeterminada que determina si las asignaciones son necesarias para los usuarios y los grupos. Le recomendamos que no modifique la configuración Requerir asignaciones de estas aplicaciones si tiene previsto utilizarlas con la propagación de identidades de confianza. Incluso si ha configurado permisos detallados que permiten a los usuarios acceder a recursos de la aplicación específica, la modificación de la configuración Requerir asignaciones puede provocar un comportamiento inesperado, como la interrupción del acceso de los usuarios a estos recursos.
- Comprueba que la aplicación solicitante esté configurada para utilizar ámbitos válidos para la aplicación AWS gestionada receptora.
6. Si los pasos de verificación anteriores se realizan correctamente, IAM Identity Center creará un nuevo token. El nuevo token es un token opaco (cifrado) que incluye la identidad del usuario correspondiente en el Centro de Identidad de IAM, la audiencia (AUD) de la aplicación AWS gestionada receptora y los ámbitos que la aplicación solicitante puede utilizar al realizar solicitudes a la aplicación gestionada receptora. AWS
  7. La aplicación solicitante, o el controlador que utiliza, inicia una solicitud de recursos a la aplicación receptora y pasa el token que IAM Identity Center generó a la aplicación receptora.
  8. La aplicación receptora realiza llamadas a IAM Identity Center para obtener la identidad del usuario y los ámbitos codificados en el token. También puede realizar solicitudes para obtener los atributos del usuario o la pertenencia del usuario a grupos desde el directorio de Identity Center.



9. La aplicación receptora utiliza su configuración de autorización para determinar si el usuario está autorizado a acceder al recurso de la aplicación solicitado.
10. Si el usuario está autorizado a acceder al recurso de la aplicación solicitado, la aplicación receptora responde a la solicitud.
11. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en los registros y CloudTrail eventos de la aplicación receptora. La forma específica en que se registra esta información varía en función de la aplicación.

## Sesiones de rol de IAM con identidad mejorada

[AWS Security Token Service](#) (STS) permite que una aplicación obtenga una sesión de rol de IAM con identidad mejorada. Las sesiones de rol con identidad mejorada tienen un contexto de identidad adicional que incluye un identificador de usuario al Servicio de AWS que llaman. Servicios de AWS puede buscar las pertenencias a los grupos y los atributos del usuario en el Centro de Identidad de IAM y utilizarlos para autorizar el acceso del usuario a los recursos.

AWS las aplicaciones obtienen sesiones de roles con una identidad mejorada realizando solicitudes a la acción de la AWS STS [AssumeRole](#) API y pasando una afirmación de contexto con el identificador del usuario (`userId`) en el `ProvidedContexts` parámetro de la solicitud a. `AssumeRole` La afirmación de contexto se obtiene de la reclamación `idToken` recibida en respuesta a una solicitud dirigida a SSO OIDC para [CreateTokenWithIAM](#). Cuando una AWS aplicación utiliza una sesión de rol con identidad mejorada para acceder a un recurso, CloudTrail registra la `userId` sesión de inicio y la acción realizada. Para obtener más información, consulte [Registro de sesiones de rol de IAM con identidad mejorada](#).

### Temas

- [Tipos de sesiones de rol de IAM con identidad mejorada](#)
- [Registro de sesiones de rol de IAM con identidad mejorada](#)

### Tipos de sesiones de rol de IAM con identidad mejorada

AWS STS puede crear dos tipos diferentes de sesiones de rol de IAM con identidad mejorada, en función de la afirmación de contexto proporcionada a la solicitud. `AssumeRole` Las aplicaciones que hayan obtenido tokens de identificación de IAM Identity Center pueden añadir `sts:identity_context` (recomendado) o `sts:audit_context` (admitido por compatibilidad con versiones anteriores) a las sesiones de rol de IAM. Una sesión de roles de IAM con identidad mejorada solo puede tener una de estas aserciones de contexto, no ambas.

## Sesiones de rol de IAM con identidad mejorada creadas mediante **sts:identity\_context**

Cuando una sesión de rol con identidad mejorada contiene `sts:identity_context`, el Servicio de AWS llamado determina si la autorización de recursos se basa en el usuario que está representado en la sesión de rol o si se basa en el rol. Los Servicios de AWS que admiten la autorización basada en el usuario proporcionan al administrador de la aplicación controles para asignar el acceso al usuario o a los grupos de los que el usuario es miembro.

Servicios de AWS que no admitan la autorización basada en el usuario ignoran la.

`sts:identity_context` CloudTrail registra el USERID del usuario del Centro de Identidad de IAM con todas las acciones realizadas por el rol. Para obtener más información, consulte [Registro de sesiones de rol de IAM con identidad mejorada](#).

Para obtener este tipo de sesión de rol con identidad mejorada AWS STS, las aplicaciones proporcionan el valor del `sts:identity_context` campo de la solicitud mediante el parámetro de [AssumeRoles](#)solicitud. `ProvidedContexts` Utilice `arn:aws:iam::aws:contextProvider/IdentityCenter` como valor para `ProviderArn`.

Para obtener más información sobre el comportamiento de la autorización, consulte la documentación relativa a la recepción. Servicio de AWS

## Sesiones de rol de IAM con identidad mejorada creadas mediante **sts:audit\_context**

En el pasado, se `sts:audit_context` utilizaba Servicios de AWS para permitir el registro de la identidad del usuario sin utilizarla para tomar una decisión de autorización. Servicios de AWS ahora pueden usar un único contexto: `sts:identity_context` - para lograrlo y para tomar decisiones de autorización. Recomendamos utilizar `sts:identity_context` en todas las nuevas implementaciones de propagación de identidades de confianza.

### Registro de sesiones de rol de IAM con identidad mejorada

Cuando se realiza una solicitud a una Servicio de AWS sesión de rol de IAM con identidad mejorada, se inicia sesión en el elemento en el centro `userId` de identidad de IAM del usuario. CloudTrail `OnBehalfOf` La forma en que se registran los eventos CloudTrail varía en función del. Servicio de AWS No todos los Servicios de AWS registran el elemento `onBehalfOf`.

A continuación se muestra un ejemplo de cómo se inicia sesión en una sesión de rol con identidad mejorada. Servicio de AWS CloudTrail

```
"userIdentity": {  
  "type": "AssumedRole",
```

```

    "principalId": "AROEXAMPLE:MyRole",
    "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
    "accountId": "111111111111",
    "accessKeyId": "ASIAEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLE",
        "arn": "arn:aws:iam::111111111111:role/MyRole",
        "accountId": "111111111111",
        "userName": "MyRole"
      },
      "attributes": {
        "creationDate": "2023-12-12T13:55:22Z",
        "mfaAuthenticated": "false"
      }
    },
    "onBehalfOf": {
      "userId": "11111111-1111-1111-1111-111111111111",
      "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
    }
  }
}

```

## Rotación de certificados de IAM Identity Center

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y el proveedor de servicios de la aplicación. Al añadir una aplicación al IAM Identity Center, se crea automáticamente un certificado de IAM Identity Center para usarlo con esa aplicación durante el proceso de configuración. De forma predeterminada, este certificado de IAM Identity Center generado automáticamente es válido durante un período de 5 años.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados antiguos de una aplicación por otros más nuevos. Por ejemplo, puede que tenga que sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

## Consideraciones antes de rotar un certificado

Antes de iniciar el proceso de rotación de un certificado en IAM Identity Center, tenga en cuenta lo siguiente:

- El proceso de rotación de certificaciones requiere que se restablezca la relación de confianza entre IAM Identity Center y el proveedor de servicios. Para restablecer la relación de confianza, utilice los procedimientos que se proporcionan en [Rotación de un certificado de IAM Identity Center](#).
- La actualización del certificado con el proveedor de servicios puede provocar una interrupción temporal del servicio para los usuarios hasta que la relación de confianza se restablezca correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

## Rotación de un certificado de IAM Identity Center

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Generación de un nuevo certificado
- Adición del nuevo certificado al sitio web del proveedor de servicios
- Configuración del nuevo certificado como activo
- Eliminación del certificado inactivo

Utilice todos los procedimientos siguientes en el orden que se indica a continuación para completar el proceso de rotación de certificados para una solicitud determinada:

### Paso 1: generar un nuevo certificado

Los nuevos certificados de IAM Identity Center que genere se pueden configurar para que utilicen las siguientes propiedades:

- **Período de validez:** especifica el tiempo asignado (en meses) antes de que caduque un nuevo certificado de IAM Identity Center.
- **Tamaño de la clave:** determina el número de bits que debe utilizar una clave con su algoritmo criptográfico. Puede establecer este valor en RSA de 1024 bits o RSA de 2048 bits. Para obtener información general sobre cómo funcionan los tamaños de clave en criptografía, consulte [Tamaño de clave](#).
- **Algoritmo:** especifica el algoritmo que IAM Identity Center utiliza al firmar la aserción/respuesta de SAML. Puede establecer este valor en SHA-1 o SHA-256. AWS recomienda utilizar el SHA-256 siempre que sea posible, a menos que su proveedor de servicios requiera el SHA-1. Para obtener

información general sobre cómo funcionan los algoritmos de criptografía, consulte [Criptografía de clave pública](#).

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija la aplicación para la que desee generar un nuevo certificado.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los metadatos de IAM Identity Center, seleccione Administrar certificado. Si no tiene una pestaña de Configuración o el ajuste de configuración no está disponible, no necesita rotar el certificado de esta aplicación.
5. En la página de certificados de IAM Identity Center, seleccione Generar un certificado nuevo.
6. En el cuadro de diálogo Generar un nuevo certificado de IAM Identity Center, especifique los valores adecuados para el período de validez, el algoritmo y el tamaño de clave. A continuación, elija Generar.

## Paso 2: actualizar el sitio web del proveedor de servicios

Utilice el siguiente procedimiento para restablecer la relación de confianza con el proveedor de servicios de la aplicación.

### Important

Al cargar el nuevo certificado al proveedor de servicios, es posible que los usuarios no puedan autenticarse. Para corregir esta situación, configure el nuevo certificado como activo como se describe en el paso siguiente.

1. En la [consola de IAM Identity Center](#), elija la aplicación para la que acaba de generar un nuevo certificado.
2. En la página de detalles de la aplicación, elija la pestaña Configuración.
3. Seleccione Ver instrucciones y, a continuación, siga las instrucciones del sitio web específico del proveedor de servicios de aplicaciones para añadir el certificado recién generado.

## Paso 3: configurar el nuevo certificado como activo

Una aplicación puede tener asignados hasta dos certificados. IAM Identity Center utilizará el certificado que esté establecido como activo para firmar todas las aserciones de SAML.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.
5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee configurar como activo, elija Acciones y, a continuación, Establecer como activo.
6. En el cuadro de diálogo Establecer el certificado seleccionado como activo, confirme que comprende que configurar un certificado como activo puede requerir que restablezca la relación confianza y, a continuación, seleccione Activar.

## Paso 4: eliminación del certificado anterior

Use el siguiente procedimiento para completar el proceso de rotación de certificados para su aplicación. Solo puede eliminar un certificado que esté en estado inactivo.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.
5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee eliminar. Elija Acciones y, a continuación, elija Eliminar.
6. En el cuadro de diálogo Eliminar certificado, elija Eliminar.

## Indicadores de estado de caducidad de certificados

En la consola del IAM Identity Center, la página de aplicaciones muestra los iconos indicadores de estado en las propiedades de cada aplicación. Estos iconos aparecen en la columna Caduca el

situada junto a cada certificado de la lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado actualmente.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido actualmente y seguirá siendo válido durante al menos 90 días más.

Cómo comprobar el estado de un certificado:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de solicitudes, revise el estado de los certificados de la lista, tal y como se indica en la columna Caduca el.

## Entender las propiedades de la aplicación en la consola de IAM Identity Center

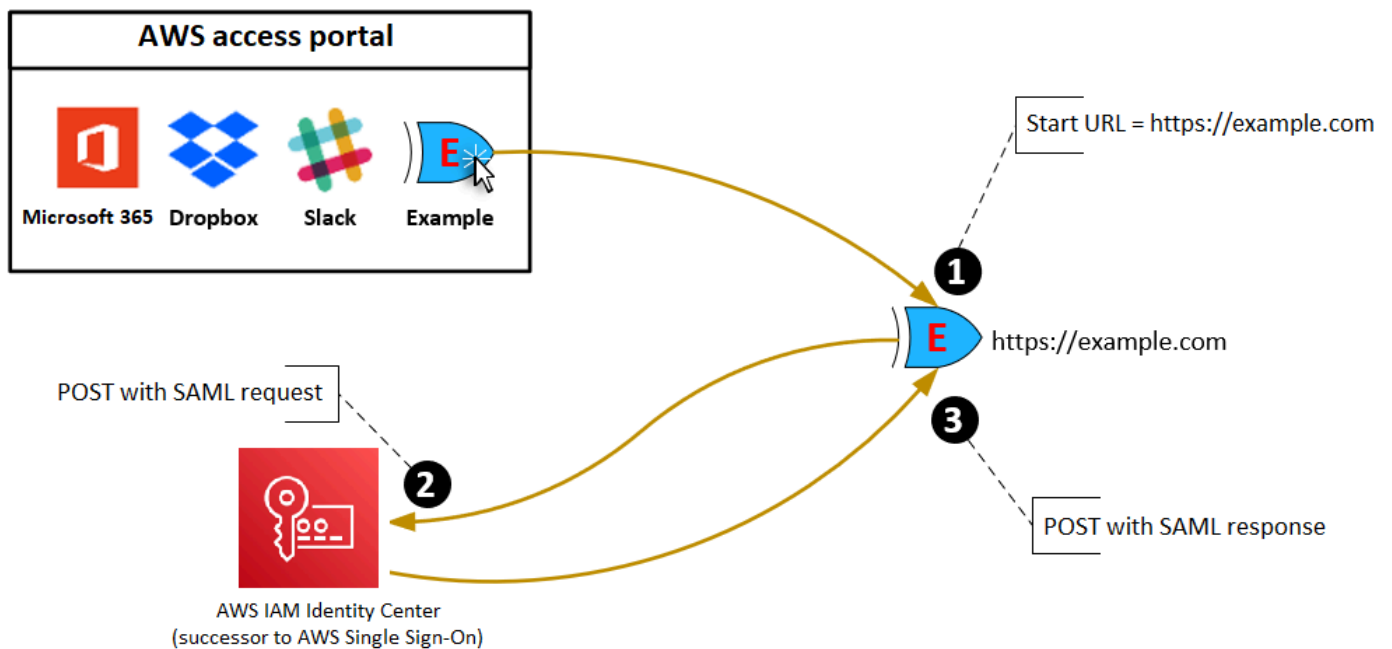
Configure la URL de inicio de la aplicación, el estado de retransmisión y la duración de la sesión en IAM Identity Center para optimizar la experiencia del usuario.

### URL de inicio de la aplicación

Utilice una URL de inicio de la aplicación para iniciar el proceso de federación con la aplicación. El uso típico es para una aplicación que solo admite una conexión iniciada por el proveedor de servicio (SP).

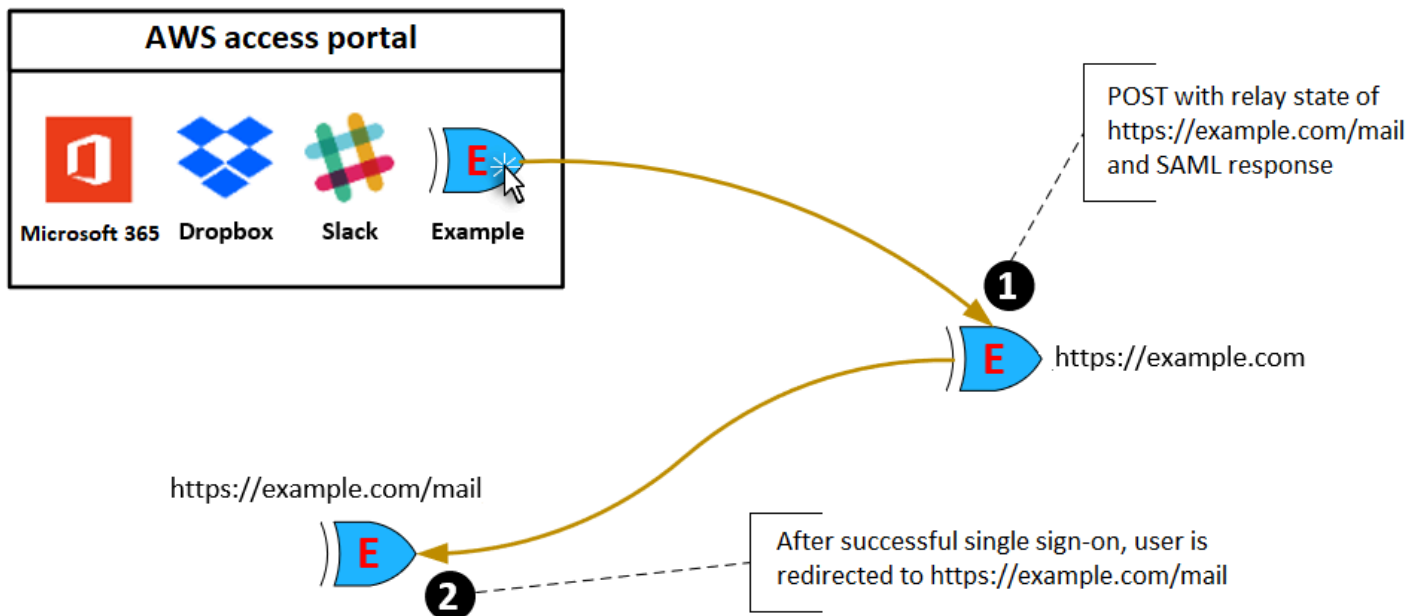
Los siguientes pasos y diagrama ilustran el flujo de trabajo de autenticación de la URL de inicio de la aplicación cuando un usuario elige una aplicación en el portal de acceso AWS :

1. El navegador del usuario redirige la solicitud de autenticación mediante el valor de la URL de inicio de la aplicación (en este caso <https://example.com>).
2. La aplicación envía un HTML POST con SAMLRequest a IAM Identity Center.
3. IAM Identity Center envía después una instrucción HTML POST con un elemento SAMLResponse a la aplicación.



## Estado de retransmisión

Durante el proceso de autenticación de la federación, el estado de retransmisión redirige a los usuarios dentro de la aplicación. Para SAML 2.0, este valor se pasa sin modificar a la aplicación. Una vez configuradas las propiedades de la aplicación, IAM Identity Center envía el valor de estado de retransmisión junto con una respuesta SAML a la aplicación.





## Duración de la sesión

La duración de la sesión es el tiempo durante el que la sesión de un usuario de la aplicación es válida. En el caso de SAML 2.0, esta duración se utiliza para definir la fecha `SessionNotOnOrAfter` del elemento de aserción de SAML `saml2:AuthNStatement`.

Las aplicaciones pueden interpretar la duración de la sesión de las siguientes formas:

- Las aplicaciones pueden utilizarla para determinar el tiempo máximo permitido para la sesión del usuario. Las aplicaciones pueden generar una sesión de usuario con una duración más corta. Esto puede ocurrir cuando la aplicación solo admite sesiones de usuario con una duración menor que la duración de la sesión configurada.
- Las aplicaciones pueden utilizarla como la duración exacta y podrían no permitir que los administradores configuren el valor. Esto puede ocurrir cuando la aplicación solo admite una duración de la sesión específica.

Para obtener más información acerca de cómo se utiliza la duración de la sesión, consulte la documentación de su aplicación específica.

## Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center

Puede asignar a los usuarios acceso mediante inicio de sesión único a las aplicaciones de SAML 2.0 del catálogo de aplicaciones o a las aplicaciones de SAML 2.0 personalizadas.

Consideraciones para las asignaciones de grupos:

- Asigne el acceso directamente a los grupos. Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se muda a una organización diferente, simplemente muévelo a un grupo diferente. Así el usuario recibirá automáticamente los permisos necesarios para la nueva organización.
- No se admiten grupos anidados. Al asignar el acceso de los usuarios a las aplicaciones, IAM Identity Center no permite añadir usuarios a grupos anidados. Si añade un usuario a un grupo anidado, es posible que reciba el mensaje “No tiene ninguna aplicación” al iniciar sesión. Las asignaciones deben realizarse en función del grupo inmediato del que el usuario es miembro.

## Cómo dar acceso a una aplicación a un usuario o grupo:

### Important

En el AWS caso de las aplicaciones gestionadas, debe añadir usuarios directamente desde las consolas de aplicaciones correspondientes o a través de APIs.

1. Abra la [consola de IAM Identity Center](#).

### Note

Si administra los usuarios en AWS Managed Microsoft AD, asegúrese de que la consola del IAM Identity Center utilice la AWS región en la que se encuentra su AWS Managed Microsoft AD directorio antes de dar el siguiente paso.

2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione el nombre de la aplicación a la que quiere asignar acceso.
4. En la página de detalles de la aplicación, en la sección Usuarios asignados, elija Asignar usuarios.
5. En el cuadro de diálogo Asignar usuarios, escriba un nombre de usuario o de grupo. Puede especificar varios usuarios o grupos seleccionando las cuentas aplicables tal y como aparecen en los resultados de búsqueda.
6. Elija Assign users (Asignar usuarios).

## Eliminar el acceso de los usuarios a las aplicaciones de SAML 2.0

Utilice este procedimiento para eliminar el acceso de los usuarios a aplicaciones de SAML 2.0 del catálogo de aplicaciones o a aplicaciones de SAML 2.0 personalizadas. Para obtener más información sobre las sesiones de autenticación y su duración, consulte [Descripción de las sesiones de autenticación en IAM Identity Center](#).

Para eliminar el acceso de los usuarios a una aplicación

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación cuyo acceso de usuario desea eliminar.

4. En la página de detalles de la aplicación, seleccione la pestaña Usuarios asignados, elija el usuario o grupo que desee eliminar y, a continuación, seleccione Eliminar acceso.
5. En el cuadro de diálogo Remove access (Eliminar acceso), compruebe el nombre del usuario o del grupo. A continuación, elija Remove access (Eliminar acceso).

## Asignación de atributos de su aplicación con atributos de IAM Identity Center

Algunos proveedores de servicios requieren aserciones SAML personalizadas para transferir datos adicionales acerca de los inicios de sesión de los usuarios. En ese caso, puede seguir el siguiente procedimiento para especificar cómo deben asignarse los atributos de usuarios de sus aplicaciones con los atributos correspondientes en IAM Identity Center.

Cómo asignar los atributos de la aplicación con atributos de IAM Identity Center:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación en la que desea mapear atributos.
4. En la página de detalles de la aplicación, seleccione Acciones y, a continuación, seleccione Editar asignación de atributos.
5. Seleccione Agregar nueva asignación de atributos.
6. En el primer cuadro de texto, escriba el atributo de la aplicación.
7. En el segundo cuadro de texto, escriba el atributo de IAM Identity Center que desea asignar con el atributo de la aplicación. Por ejemplo, es posible que desee asignar el atributo de la aplicación **Username** al atributo del usuario **email** de IAM Identity Center. Para ver la lista de los atributos de usuario permitidos en IAM Identity Center, consulte la tabla que encontrará en [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos](#).
8. En la tercera columna de la tabla, seleccione el formato adecuado del atributo en el menú.
9. Seleccione Save changes (Guardar cambios).

# Configurar el acceso a Cuentas de AWS

AWS IAM Identity Center está integrado con AWS Organizations, lo que le permite gestionar de forma centralizada los permisos de varias cuentas Cuentas de AWS sin necesidad de configurar cada una de sus cuentas de forma manual. Puede definir los permisos y asignarlos a los usuarios de la fuerza laboral para controlar su acceso a determinados recursos Cuentas de AWS mediante una [instancia organizativa](#) de IAM Identity Center. [Las instancias de cuentas](#) de IAM Identity Center no admiten el acceso a las cuentas.

## Cuenta de AWS tipos

Existen dos tipos de Cuentas de AWS entradas AWS Organizations:

- Cuenta de administración: la Cuenta de AWS que se utiliza para crear la organización.
- Cuentas de miembros: el resto Cuentas de AWS que pertenecen a una organización.

Para obtener más información sobre Cuenta de AWS los tipos, consulte [AWS Organizations Terminología y conceptos](#) en la Guía del AWS Organizations usuario.

También puede optar por registrar una cuenta de miembro como administrador delegado de IAM Identity Center. Los usuarios de esta cuenta pueden realizar la mayoría de las tareas administrativas de IAM Identity Center. Para obtener más información, consulte [Administración delegada](#).

La siguiente tabla indica si los usuarios de la cuenta pueden realizar la tarea administrativa de IAM Identity Center para cada tipo de tarea y cuenta.

| Tareas administrativas de IAM Identity Center                     | Cuenta de miembro                                                                         | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Lectura de usuarios o grupos (leer el grupo en sí y sus miembros) | <br>Sí | <br>Sí | <br>Sí |

| Tareas administrativas de IAM Identity Center                                | Cuenta de miembro                                                                         | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Cómo agregar, editar o eliminar usuarios o grupos                            | <br>No   | <br>Sí   | <br>Sí   |
| Cómo habilitar o deshabilitar el acceso de usuarios                          | <br>No   | <br>Sí   | <br>Sí   |
| Cómo habilitar, deshabilitar o administrar los atributos entrantes           | <br>No   | <br>Sí   | <br>Sí   |
| Cambio o administración de las fuentes de identidad                          | <br>No | <br>Sí | <br>Sí |
| Creación, edición o eliminación de aplicaciones administradas por el cliente | <br>No | <br>Sí | <br>Sí |
| Crear, editar o eliminar aplicaciones AWS gestionadas                        | <br>Sí | <br>Sí | <br>Sí |

| Tareas administrativas de IAM Identity Center                                            | Cuenta de miembro                                                                         | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Configuración de MFA                                                                     | <br>No   | <br>Sí   | <br>Sí   |
| Administración de conjuntos de permisos no aprovisionados en la cuenta de administración | <br>No   | <br>Sí   | <br>Sí   |
| Administración de conjuntos de permisos aprovisionados en la cuenta de administración    | <br>No   | <br>No   | <br>Sí   |
| Activar IAM Identity Center                                                              | <br>No | <br>No | <br>Sí |
| Eliminación de la configuración de IAM Identity Center                                   | <br>No | <br>No | <br>Sí |
| Cómo habilitar o deshabilitar el acceso de los usuarios en la cuenta de administración   | <br>No | <br>No | <br>Sí |

| Tareas administrativas de IAM Identity Center                               | Cuenta de miembro                                                                       | Cuenta de administrador delegado                                                        | Cuenta de administración                                                                  |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Registro o cancelación de una cuenta de miembro como administrador delegado | <br>No | <br>No | <br>Sí |

\* Consulte las prácticas recomendadas para la administración delegada en relación con las asignaciones de usuarios y grupos a la cuenta de administración.

## Asignación Cuenta de AWS de acceso

Puede usar los conjuntos de permisos para simplificar la forma en que asigna el acceso a los usuarios, grupos y Cuentas de AWS de su organización. Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta de AWS. Puede crear un único conjunto de permisos y asignarlo a varias Cuentas de AWS de su organización. También puede asignar varios conjuntos de permisos al mismo usuario.

Para obtener más información sobre los conjuntos de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

### Note

También puede asignar a sus usuarios acceso de inicio de sesión único a las aplicaciones. Para obtener información, consulte [Configuración del acceso a las aplicaciones](#).

## La experiencia del usuario final

El portal de AWS acceso proporciona a los usuarios del IAM Identity Center un acceso de inicio de sesión único a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas a través de un portal web. El portal de AWS acceso es diferente del [Consola de administración de AWS](#), que es un conjunto de consolas de servicio para administrar los recursos. AWS

Al crear un conjunto de permisos, el nombre que especifique para el conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol. Tras elegir el rol, pueden acceder a los AWS servicios mediante el uso de las credenciales temporales Consola de administración de AWS o recuperar las credenciales temporales para acceder a AWS los servicios mediante programación.

Para abrir Consola de administración de AWS o recuperar las credenciales temporales y acceder a ellas AWS mediante programación, los usuarios siguen estos pasos:

1. Los usuarios abren una ventana del navegador y utilizan la URL de inicio de sesión que usted proporciona para ir al AWS portal de acceso.
2. Con sus credenciales de directorio, inician sesión en el portal de AWS acceso.
3. Tras la autenticación, en la página del portal de AWS acceso, eligen la pestaña Cuentas para ver la lista Cuentas de AWS a la que tienen acceso.
4. A continuación, los usuarios eligen lo Cuenta de AWS que quieren usar.
5. Debajo del nombre del Cuenta de AWS, todos los conjuntos de permisos a los que estén asignados los usuarios aparecen como roles disponibles. Por ejemplo, si asignó un usuario `john_stiles` al conjunto de `PowerUser` permisos, el rol se mostrará en el portal de AWS acceso como `PowerUser/john_stiles`. Los usuarios que tienen asignados varios conjuntos de permisos eligen el rol de que quieren utilizar. Los usuarios pueden elegir su rol para acceder a Consola de administración de AWS.
6. Además del rol, los usuarios del portal de AWS acceso pueden recuperar credenciales temporales para el acceso mediante línea de comandos o mediante programación seleccionando las teclas de acceso.

Para step-by-step obtener información que puede proporcionar a los usuarios de su plantilla, consulte [Configuración y uso del portal de AWS acceso](#) y [Obtener las credenciales de usuario del IAM Identity Center para o AWS CLI AWS SDKs](#).

## Aplicación y limitación del acceso

Al habilitar IAM Identity Center, este crea un rol vinculado a un servicio. También puede utilizar las políticas de control de servicios (SCPs).



## Delegación y aplicación del acceso

Un rol vinculado a un servicio es un tipo de rol de IAM que está vinculado directamente a un servicio. AWS Tras activar el Centro de identidad de IAM, el Centro de identidades de IAM puede crear un rol vinculado a un servicio en cada uno de los componentes de la organización. Cuenta de AWS Esta función proporciona permisos predefinidos que permiten al Centro de Identidad de IAM delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a determinados miembros de su organización. Cuentas de AWS AWS Organizations Para utilizar esta característica, debe asignar a uno o más usuarios el acceso a una cuenta. Para obtener más información, consulte [Entender los roles vinculados a servicios en IAM Identity Center](#) y [Uso de roles vinculados a servicios para IAM Identity Center](#).

## Límite de acceso al almacén de identidades desde las cuentas de los miembros

En el caso del servicio de almacén de identidades utilizado por IAM Identity Center, los usuarios que tienen acceso a una cuenta de miembro pueden utilizar acciones de la API que requieren permisos de lectura. Las cuentas de los miembros tienen acceso a las acciones de lectura en los espacios de nombres sso-directory e identitystore. Para obtener más información, consulte [Acciones, recursos y claves de condición del AWS IAM Identity Center directorio](#) y [Acciones, recursos y claves de condición de AWS Identity Store](#) en la Referencia de autorización de servicios.

Para evitar que los usuarios de las cuentas de los miembros utilicen las operaciones de la API en el almacén de identidades, puede [asociar una política de control de servicio \(SCP\)](#). Un SCP es un tipo de política de organización que puede utilizar para administrar permisos en su organización. El siguiente ejemplo de SCP impide que los usuarios de las cuentas de los miembros accedan a cualquier operación de la API del almacén de identidades.

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

 Note

Para garantizar que sus aplicaciones AWS gestionadas funcionen correctamente en su centro de identidad de IAM, debe evitar aplicar este SCP al Cuentas de AWS lugar en el que desplegó esas aplicaciones. Además, si utiliza la administración delegada, debe evitar aplicar este SCP a la cuenta de administración delegada. Para obtener más información, consulte [Prácticas recomendadas](#).

Para obtener más información, consulte [las políticas de control de servicios \(SCPs\)](#) en la Guía del AWS Organizations usuario.

## Administración delegada

La administración delegada proporciona una forma cómoda para que los usuarios asignados a una cuenta de miembro registrada realicen la mayoría de las tareas administrativas de IAM Identity Center. Al activar el Centro de Identidad de IAM, su instancia del Centro de Identidad de IAM se crea en la cuenta de administración de forma AWS Organizations predeterminada. Se diseñó originalmente de esta manera para que IAM Identity Center pudiera aprovisionar, desaproveionar y actualizar las características en todas las cuentas de los miembros de su organización. Aunque su instancia del IAM Identity Center debe residir siempre en la cuenta de administración, puede delegar la administración del Centro de Identidad de IAM a una cuenta de miembro en AWS Organizations, lo que amplía la capacidad de administrar el Centro de Identidad de IAM desde fuera de la cuenta de administración.

Habilitar la administración delegada proporciona los siguientes beneficios:

- Minimiza la cantidad de personas que necesitan acceder a la cuenta de administración para ayudar a mitigar los problemas de seguridad
- Permite a determinados administradores asignar usuarios y grupos a las aplicaciones y a las cuentas de los miembros de su organización

Para obtener más información sobre cómo funciona el Centro de Identidad de IAM, consulte. AWS Organizations [Configurar el acceso a Cuentas de AWS](#) Para obtener información adicional y revisar un ejemplo de escenario empresarial que muestre cómo configurar la administración delegada, consulte [Getting started with IAM Identity Center delegated administration](#) en el blog de seguridad de AWS .

## Temas

- [Prácticas recomendadas](#)
- [Requisitos previos](#)
- [Registro de una cuenta de miembro](#)
- [Anulación del registro de una cuenta de miembro](#)
- [Consulte qué cuenta de miembro se ha registrado como administrador delegado](#)

## Prácticas recomendadas

Estas son algunas prácticas recomendadas antes de configurar la administración delegada:

- Otorgue el mínimo privilegio a la cuenta de administración: dado que la cuenta de administración es una cuenta con muchos privilegios y para cumplir con el principio de privilegios mínimos, le recomendamos encarecidamente que restrinja el acceso a la cuenta de administración al menor número posible de personas. La característica de administrador delegado tiene por objeto minimizar el número de personas que necesitan acceder a la cuenta de administración. También puede considerar la posibilidad de utilizar un [acceso elevado temporal](#) para conceder este acceso solo cuando sea necesario.
- Conjuntos de permisos dedicados para la cuenta de administración: utilice conjuntos de permisos dedicados para la cuenta de administración. Por motivos de seguridad, un conjunto de permisos utilizado para acceder a la cuenta de administración solo puede modificarlo un administrador de IAM Identity Center desde la cuenta de administración. El administrador delegado no puede modificar los conjuntos de permisos aprovisionados en la cuenta de administración.
- Asigne solo usuarios (no grupos) a los conjuntos de permisos de la cuenta de administración: dado que la cuenta de administración tiene privilegios especiales, debe tener cuidado al asignar el acceso a esta cuenta en la consola o AWS Command Line Interface (CLI). Si asigna grupos a conjuntos de permisos con acceso a la cuenta de administración, cualquier persona que tenga permisos para modificar la pertenencia a esos grupos podrá ser add/remove usuario to/from de esos grupos y, por lo tanto, determinar quién tiene acceso a la cuenta de administración. Se trata de cualquier administrador de grupo con control sobre su origen de identidad, incluido el administrador del proveedor de identidades (IdP), el administrador del Servicio de dominio de Microsoft Active Directory (AD DS) o el administrador de IAM Identity Center. Por lo tanto, debe asignar los usuarios directamente a los conjuntos de permisos que otorgan acceso a la cuenta de administración y evitar los grupos. Si usa grupos para administrar el acceso a la cuenta de administración, asegúrese de que haya controles adecuados en el IdP para limitar quién tiene

la capacidad de modificar esos grupos, y asegúrese de que los cambios en esos grupos (o los cambios en las credenciales de los usuarios de la cuenta de administración) se registren y revisen según sea necesario.

- Tenga en cuenta su ubicación de Active Directory: si piensa utilizar Active Directory como fuente de identidad de IAM Identity Center, localice el directorio en la cuenta del miembro en la que haya activado la característica de administrador delegado de IAM Identity Center. Si decide cambiar el origen de identidad de IAM Identity Center de cualquier otro origen a Active Directory, o cambiarlo de Active Directory a cualquier otro origen, el directorio debe residir en la cuenta de miembro administrador delegado de IAM Identity Center. Si desea que Active Directory esté en la cuenta de administración, debe realizar la configuración en la cuenta de administración, ya que el administrador delegado no tendrá los permisos necesarios para completarla.

## Limite las acciones del almacén de identidades de IAM Identity Center en la cuenta de administración delegada con orígenes de identidad externos

Si utiliza una fuente de identidad externa, como un IdP Directory Service, debe implementar políticas que limiten las acciones del almacén de identidades que un administrador del Centro de identidades de IAM puede realizar desde la cuenta de administración delegada. Las operaciones de escritura y eliminación deben considerarse detenidamente. Por lo general, el origen de identidad externo es la fuente veraz de los usuarios y sus atributos, así como de las membresías grupales. Si las modifica mediante el almacén de identidades APIs o la consola, los cambios se sobrescribirán durante los ciclos de sincronización normales. Es mejor dejar estas operaciones al control exclusivo del origen veraz de tu identidad. Esto también evita que un administrador de IAM Identity Center modifique la membresía grupal para conceder acceso a un conjunto de permisos o una aplicación asignados a un grupo, en lugar de dejar el control de la membresía grupal en manos del administrador del IdP. También debe asegurarse de quién puede crear los tokens portadores del SCIM desde la cuenta de administración delegada, ya que podrían permitir al administrador de la cuenta de miembro modificar grupos y usuarios a través de un cliente de SCIM.

Puede haber ocasiones en las que sea necesario realizar operaciones de escritura o eliminación desde la cuenta de administrador delegado. Por ejemplo, puede crear un grupo sin añadir miembros y, a continuación, realizar asignaciones a un conjunto de permisos sin tener que esperar a que el administrador del IdP cree el grupo. Nadie tendrá acceso a esa asignación hasta que el administrador del IdP aprovisiona el grupo y el proceso de sincronización del IdP establezca los miembros del grupo. También puede ser adecuado eliminar un usuario o un grupo para impedir el inicio de sesión o la autorización en un momento en el que no pueda esperar al proceso de sincronización del IdP para eliminar el acceso del usuario o el grupo. Sin embargo, el uso indebido

de este permiso puede ser perjudicial para los usuarios. Debe utilizar el principio de privilegio mínimo al asignar permisos de almacén de identidades. Puede controlar qué acciones de almacén de identidades permiten los administradores de su cuenta de administración delegada mediante una política de control de servicio (SCP).

El ejemplo de SCP que aparece a continuación impide asignar usuarios a grupos a través de la API Identity Store y el Consola de administración de AWS, lo cual se recomienda cuando la fuente de identidad es externa. Esto no afecta a la sincronización de usuarios desde Directory Service o desde un IdP externo (a través de SCIM).

#### Note

Es posible que, aunque utilice una fuente de identidad externa, su organización dependa, total o parcialmente, del almacén de identidades APIs para el aprovisionamiento de usuarios y grupos. Por lo tanto, antes de activar esta SCP, debe confirmar que su proceso de aprovisionamiento de usuarios no utiliza esta operación de la API del almacén de identidades. Consulte también la siguiente sección para obtener información sobre cómo limitar la administración de la membresía grupal a grupos específicos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

Si desea evitar agregar usuarios solo a los grupos que otorgan acceso a la cuenta de administración, puede hacer referencia a esos grupos específicos utilizando el ARN del grupo en el siguiente formato: `arn:${Partition}:identitystore:::group/${GroupId}`. Este y otros tipos de recursos disponibles en el almacén de identidades están documentados en la sección [Tipos de recursos definidos por el almacén de AWS identidades](#) en la Referencia de autorización de servicios. También puede considerar la posibilidad de incluir un almacén de identidades adicional APIs en el SCP. Para obtener más información, consulte [Actions](#) en la Referencia de la API del almacén de identidades.

Al añadir la siguiente declaración de política a su SCP, puede impedir que el administrador delegado cree los tokens portadores del SCIM. Puede aplicar esto a ambas fuentes de identidad externas.

 Note

Si tu administrador delegado necesita configurar el aprovisionamiento de usuarios con SCIM o realizar la rotación periódica del token portador del SCIM, tendrá que permitir temporalmente el acceso a esta API para que el administrador delegado pueda completar esas tareas.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

## Limite las acciones del almacén de identidades de IAM Identity Center en la cuenta de administración delegada para los usuarios gestionados localmente

Si crea sus usuarios y grupos directamente en el Centro de identidades de IAM, en lugar de utilizar un IdP Directory Service externo, debe tomar precauciones para determinar quién puede crear usuarios, restablecer las contraseñas y controlar la pertenencia a los grupos. Estas acciones otorgan al administrador un gran control sobre quién puede iniciar sesión y quién puede acceder a ellos mediante la pertenencia a grupos. Lo mejor es implementar estas políticas como políticas integradas dentro de los conjuntos de permisos que utilice para los administradores del Centro de Identidad de IAM, en lugar de implementarlas como políticas integradas. SCPs La siguiente política insertada de ejemplo tiene dos objetivos. En primer lugar, impide añadir usuarios a grupos específicos. Puede usarlo para evitar que los administradores delegados agreguen usuarios a los grupos que otorgan acceso a la cuenta de administración. En segundo lugar, impide la emisión de tokens portadores del SCIM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},
```

```
        arn:${Partition}:identitystore:::group/${GroupId2}
      ]
    }
  ],
  { "Effect": "Deny",
    "Action": ["sso-directory:CreateBearerToken"],
    "Resource": [ "*" ] }
  ]
}
```

## Separe la gestión de la configuración del IAM Identity Center de la administración PermissionSet

Separe las tareas administrativas, como la modificación del origen de identidad externo, la administración de los tokens del SCIM y la configuración del tiempo de espera de la sesión de las tareas de crear, modificar y asignar conjuntos de permisos creando conjuntos de permisos de administrador distintos desde su cuenta de administración.

### Limitación de la emisión de tokens portadores del SCIM

Los tokens portadores del SCIM permiten que un origen de identidad externo aprovisiona usuarios, grupos y membresías grupales mediante el protocolo SCIM cuando el origen de identidad de su IAM Identity Center es un IdP externo, como Okta o Entra ID. Puede configurar la siguiente SCP para impedir que los administradores delegados creen los tokens portadores del SCIM. Si su administrador delegado necesita configurar el aprovisionamiento de usuarios con SCIM o realizar la rotación periódica del token portador del SCIM, tendrá que permitir temporalmente el acceso a esta API para que el administrador delegado pueda completar esas tareas.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

## Uso de las etiquetas de los conjuntos de permisos y las listas de cuentas para delegar la administración de cuentas específicas

Puede crear conjuntos de permisos que asigne a los administradores de IAM Identity Center para delegar quién puede crear conjuntos de permisos y quién puede asignar qué conjuntos de permisos

en qué cuentas. Para ello, se etiquetan los conjuntos de permisos y se utilizan las condiciones de política en los conjuntos de permisos que se asignan a los administradores. Por ejemplo, puede crear conjuntos de permisos que permitan a un usuario crear conjuntos de permisos siempre que estén etiquetados de una forma determinada. Puede crear políticas que permitan a un administrador asignar conjuntos de permisos con etiquetas específicas en cuentas especificadas. Esto puede ayudarle a delegar la administración de las cuentas sin conceder al administrador los privilegios para modificar su acceso ni los privilegios sobre la cuenta de administración delegada. Por ejemplo, al etiquetar los conjuntos de permisos que utiliza únicamente en la cuenta de administración delegada, puede especificar una política que conceda únicamente a determinadas personas los permisos para modificar los conjuntos de permisos y las asignaciones que afectan a la cuenta de administración delegada. También puede conceder permisos a otras personas para que administren una lista de cuentas ajenas a la cuenta de administración delegada. Para obtener más información, consulte [Delegating permission set management and account assignment in AWS IAM Identity Center](#) el Blog de seguridad de AWS .

## Requisitos previos

Antes de poder registrar una cuenta como administrador delegado, primero debe configurar el siguiente entorno implementado:

- AWS Organizations debe estar habilitado y configurado con al menos una cuenta de miembro además de la cuenta de administración predeterminada.
- Si su fuente de identidad está configurada en Active Directory, la característica [Centro de identidades de IAM y sincronización de AD configurable](#) debe estar habilitada.

## Registro de una cuenta de miembro

Para configurar una administración delegada, primero debe registrar una cuenta de miembro en su organización como administrador delegado. Los usuarios de la cuenta de ese miembro que tengan permisos suficientes tendrán acceso administrativo a IAM Identity Center. Una vez que la cuenta de miembro se registra correctamente para la administración delegada, se denomina una cuenta de administrador delegado. Para obtener más información sobre las tareas que puede realizar la cuenta de administrador delegado, consulte [Cuenta de AWS tipos](#).

IAM Identity Center solo permite registrar una cuenta de miembro como administrador delegado a la vez. Solo puede registrar una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.



Utilice el siguiente procedimiento para conceder acceso administrativo al Centro de identidad de IAM registrando una cuenta de miembro específica en su AWS organización como administrador delegado.

 Important

Esta operación delega el acceso administrativo de IAM Identity Center a los usuarios administradores de esta cuenta de miembro. Todos los usuarios que dispongan de permisos suficientes para acceder a esta cuenta de administrador delegado pueden realizar todas las tareas administrativas de IAM Identity Center desde la cuenta, excepto:

- Habilitación de IAM Identity Center
- Eliminación de las configuraciones de IAM Identity Center
- Administración de conjuntos de permisos aprovisionados en la cuenta de administración
- Registro o cancelación del registro de otras cuentas de miembros como administradores delegados
- Habilitación o deshabilitación del acceso de usuarios en la cuenta de administración

El administrador delegado puede editar la pertenencia al grupo.

## Registro de una cuenta de miembro

1. Inicie sesión Consola de administración de AWS con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la [RegisterDelegatedAdministrator](#) API.
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra [la consola de IAM Identity Center](#).
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.
4. En la sección Administrador delegado, elija Registro de cuenta.
5. En la página Registrar un administrador delegado, selecciona el Cuenta de AWS que desees registrar y, a continuación, selecciona Registrar cuenta.

## Anulación del registro de una cuenta de miembro

Solo puede cancelar el registro de una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.

Utilice el siguiente procedimiento para eliminar el acceso administrativo al Centro de identidad de IAM anulando el registro de una cuenta de miembro de su AWS organización que anteriormente había sido designada como administrador delegado.

### Important

Al anular el registro de una cuenta, se elimina de forma efectiva la posibilidad de que todos los usuarios administradores administren IAM Identity Center desde esa cuenta. Como resultado, ya no pueden administrar las identidades de IAM Identity Center, la gestión del acceso, la autenticación o el acceso a las aplicaciones desde esta cuenta. Esta operación no afectará a ningún permiso o asignación configurados en el Centro de Identidad de IAM y, por lo tanto, no afectará a los usuarios finales, ya que seguirán teniendo acceso a sus aplicaciones y Cuentas de AWS desde el portal de acceso. AWS

### Anulación del registro de una cuenta de miembro

1. Inicie sesión Consola de administración de AWS con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la [DeregisterDelegatedAdministratorAPI](#).
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra [la consola de IAM Identity Center](#).
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.
4. En la sección Administrador delegado, elija Anular el registro de cuenta.
5. En el cuadro de diálogo Anular el registro de cuenta, revise las implicaciones de seguridad y, a continuación, escriba el nombre de la cuenta de miembro para confirmar que lo entiende.
6. Elija Anular el registro de la cuenta.

## Consulte qué cuenta de miembro se ha registrado como administrador delegado

Utilice el siguiente procedimiento para averiguar qué cuenta de miembro de su cuenta se AWS Organizations ha configurado como administrador delegado del Centro de Identidad de IAM.

Cómo ver su cuenta de miembro registrado

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la sección Detalles, busque el nombre de la cuenta registrada en Administrador delegado. También puede encontrar esta información seleccionando la pestaña Administración y consultándola en la sección Administrador delegado.

## Acceso elevado temporal para Cuentas de AWS

Todo acceso al suyo Cuenta de AWS implica algún nivel de privilegio. Las operaciones delicadas, como cambiar la configuración de un entorno de producción, requieren un tratamiento especial debido al alcance y al impacto potencial. El acceso elevado temporal (también conocido como just-in-time acceso) es una forma de solicitar, aprobar y realizar un seguimiento del uso de un permiso para realizar una tarea específica durante un tiempo específico. El acceso elevado temporal complementa otras formas de control de acceso, como los conjuntos de permisos y la autenticación multifactorial.

### Note

Para garantizar la continuidad del negocio, le recomendamos que [configure el acceso de emergencia a la Consola de administración de AWS](#).

Para abordar una variedad de necesidades de los clientes, AWS IAM Identity Center se integra con las soluciones de los socios con competencias en AWS seguridad. AWS valida que estas soluciones abordan un conjunto común de requisitos de acceso elevado temporal. Le recomendamos que revise detenidamente las soluciones de cada socio para que pueda elegir la que mejor se adapte a sus necesidades y preferencias, incluidos su negocio, la arquitectura de su entorno de nube y su presupuesto.

Las soluciones validadas incluyen la [plataforma de gestión de acceso Apongo](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#) y [Tenable](#) (anteriormente Ermetic).

Los socios pueden nominar soluciones mediante la aplicación AWS Security Competency del Partner Center. Para obtener más información, consulte [AWS Security Competency Partners](#).

 Note

Si utiliza Amazon Elastic AWS Key Management Service Kubernetes Service basado en recursos [o consulte Referenciar conjuntos de permisos en las políticas de recursos, los mapas de AWS KMS configuración de clústeres de Amazon EKS y las políticas](#) clave antes de elegir la solución. just-in-time

## Acceso mediante inicio de sesión único a Cuentas de AWS

Puede asignar permisos a los usuarios de su directorio conectado a la cuenta de administración o a las cuentas de los miembros de su organización en AWS Organizations función de las funciones [laborales más comunes](#). También puede utilizar permisos personalizados para satisfacer sus requisitos de seguridad específicos. Por ejemplo, puede conceder a los administradores de bases de datos permisos amplios a Amazon RDS en las cuentas de desarrollo pero limitar sus permisos en las cuentas de producción. IAM Identity Center configura todos los permisos de usuario necesarios en sus cuentas de Cuentas de AWS de forma automática.

 Note

Puede que tengas que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la política de [IAMFullacceso](#) o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

### Temas

- [Asigne el acceso de usuario o grupo a Cuentas de AWS](#)
- [Elimina el acceso de usuarios y grupos a un Cuenta de AWS](#)

- [Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos](#)
- [Delegue quién puede asignar el acceso de inicio de sesión único a los usuarios y grupos de la cuenta de administración](#)

## Asigne el acceso de usuario o grupo a Cuentas de AWS

Utilice el siguiente procedimiento para asignar el acceso de inicio de sesión único a usuarios y grupos del directorio conectado y para utilizar conjuntos de permisos para determinar su nivel de acceso.

Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

### Note

Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se va a otra organización, basta con cambiarlo a un grupo diferente y automáticamente recibirá los permisos necesarios para la nueva organización.

Para asignar el acceso de usuario o grupo a Cuentas de AWS

1. Abra la [consola de IAM Identity Center](#)

### Note

Antes de continuar con el paso siguiente, compruebe que la consola de IAM Identity Center utiliza alguna de las regiones donde se encuentra su directorio AWS Managed Microsoft AD .

2. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página de Cuentas de AWS, se muestra una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a la casilla Cuenta de AWS a la que desee asignar el acceso. Si desea configurar el acceso administrativo para IAM Identity Center, seleccione la casilla de verificación situada junto a la cuenta de administración.

 Note

Puedes seleccionar hasta 10 Cuentas de AWS a la vez por conjunto de permisos al asignar el acceso de inicio de sesión único a usuarios y grupos. Para asignar más de 10 Cuentas de AWS al mismo conjunto de usuarios y grupos, repita este procedimiento según sea necesario para las cuentas adicionales. Cuando se le solicite, seleccione los mismos usuarios, grupos y conjunto de permisos.

4. Seleccione Asignar usuarios o grupos.
5. Para el paso 1: seleccionar usuarios y grupos, en la página Asignar usuarios y grupos a **AWS-account-name** «», haga lo siguiente:
  1. En la pestaña Usuarios, seleccione uno o más usuarios a los que desee conceder el acceso de inicio de sesión único.

Para filtrar los resultados, escriba el nombre del usuario que desea en el cuadro de búsqueda.
  2. En la pestaña Grupos, seleccione uno o más grupos a los que desee conceder el acceso de inicio de sesión único.

Para filtrar los resultados, escriba el nombre del grupo que desea en el cuadro de búsqueda.
  3. Para mostrar los usuarios y grupos que ha seleccionado, elija el triángulo lateral situado junto a Usuarios y grupos seleccionados.
  4. Tras confirmar que se haya seleccionado los usuarios y grupos correctos, seleccione Siguiente.
6. Para el paso 2: seleccionar conjuntos de permisos, en la página Asignar conjuntos de permisos a **AWS-account-name** «», haga lo siguiente:
  1. Seleccione uno o varios conjuntos de permisos. Si es necesario, puede crear y seleccionar nuevos conjuntos de permisos.
    - Para seleccionar uno o más conjuntos de permisos existentes, en Conjuntos de permisos, seleccione los conjuntos de permisos que desee aplicar a los usuarios y grupos que seleccionó en el paso anterior.
    - Para crear uno o más conjuntos de permisos nuevos, elija Crear conjunto de permisos y siga los pasos que se indican en [Crea un conjunto de permisos](#). Tras crear los conjuntos de permisos que desea aplicar, en la consola de IAM Identity Center, vuelva a las Cuentas de AWS y siga las instrucciones hasta llegar al paso 2: seleccionar conjuntos de permisos.

Cuando llegue a este paso, seleccione los nuevos conjuntos de permisos que ha creado y continúe con el siguiente paso de este procedimiento.

2. Tras confirmar que se haya seleccionado los conjuntos de permisos correctos, seleccione Siguiente.
7. Para el paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a **AWS-account-name** «», haga lo siguiente:
  1. Revise los usuarios, grupos y los conjuntos de permisos seleccionados.
  2. Tras confirmar que se haya seleccionado los usuarios, grupos y los conjuntos de permisos correctos, seleccione Enviar.

### Consideraciones

- El proceso de asignación de usuarios y grupos puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

#### Note

Puede que tengas que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la política de [IAMFullacceso](#) o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

8. Si se aplica alguna de las siguientes condiciones, siga los pasos que se indican en [Solicitar MFA a los usuarios](#) para habilitar la MFA en IAM Identity Center:
  - Está utilizando el directorio predeterminado del Identity Center como origen e de identidad.
  - Utiliza un AWS Managed Microsoft AD directorio o un directorio autogestionado en Active Directory como fuente de identidad y no utiliza RADIUS AWS Directory Service MFA con.

**Note**

Si utiliza un proveedor de identidades externo, tenga en cuenta que el IdP externo, no IAM Identity Center, administra la configuración de MFA. No se admite el uso de MFA en el Centro de identidad de IAM para uso externo. IdPs

Al configurar el acceso a la cuenta para el usuario administrativo, del IAM Identity Center crea el rol de IAM correspondiente. Esta función, controlada por el Centro de Identidad de IAM, se crea en el lugar correspondiente Cuenta de AWS y las políticas especificadas en el conjunto de permisos se adjuntan a la función.

Como alternativa, puede utilizar [AWS CloudFormation](#) para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos. A continuación, los usuarios pueden [iniciar sesión en el portal de acceso de AWS](#) o utilizar los comandos de la [AWS Command Line Interface \(AWS CLI\)](#).

## Elimina el acceso de usuarios y grupos a un Cuenta de AWS

Utilice este procedimiento para quitar el acceso de inicio de sesión único a uno o varios usuarios y grupos del directorio conectado. Cuenta de AWS También puede utilizar la [delete-account-assignment](#) AWS CLI.

**Note**

Cuando necesite desaproveccionar usuarios o grupos de IAM Identity Center, primero debe [eliminar cualquier asignación de conjuntos de permisos](#) de sus usuarios y grupos antes de eliminarlos.

Para eliminar el acceso de usuarios y grupos a un Cuenta de AWS

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre Cuenta de AWS que contiene los usuarios y grupos a los que desea eliminar el acceso de inicio de sesión único.



4. En la página de información general de Cuenta de AWS, en Usuarios y grupos asignados, seleccione el nombre de uno o más usuarios o grupos y elija Eliminar el acceso.
5. En el cuadro de diálogo Eliminar el acceso, confirme que los nombres de los usuarios o grupos son correctos y elija Eliminar el acceso.

## Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos

El siguiente es un procedimiento general para revocar una sesión de conjunto de permisos activa para un usuario del IAM Identity Center. El procedimiento parte del supuesto de que se desea eliminar todos los accesos de un usuario cuyas credenciales estén comprometidas o de un usuario fraudulento que se encuentre en el sistema. El requisito previo es haber seguido las instrucciones que figuran en [Prepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos](#). Suponemos que la política de denegación de todo está presente en una política de control de servicio (SCP).

### Note

AWS recomienda crear una automatización para gestionar todos los pasos, excepto las operaciones que solo se realizan en la consola.

1. Obtenga el ID de la persona cuyo acceso debe revocar. Puede usar el almacén de identidades APIs para buscar al usuario por su nombre de usuario.
2. Actualice la política de denegación para agregar el ID de usuario del paso 1 de su política de control de servicio (SCP). Tras completar este paso, el usuario objetivo pierde el acceso y no puede realizar acciones con ninguna de las funciones a las que afecte la política.
3. Elimine todas las asignaciones de conjuntos de permisos para el usuario. Si el acceso se asigna mediante la pertenencia a un grupo, elimine al usuario de todos los grupos y de todas las asignaciones directas de conjuntos de permisos. Este paso impide que el usuario asuma roles de IAM adicionales. Si un usuario tiene una sesión activa en el portal de AWS acceso y usted lo desactiva, podrá seguir asumiendo nuevas funciones hasta que le quite el acceso.
4. Si usa un proveedor de identidades (IdP) o Microsoft Active Directory como fuente de identidad, deshabilite al usuario en la fuente de identidad. La desactivación del usuario impide la creación de sesiones adicionales en el portal de acceso AWS. Utilice su IdP o la documentación de la

API de Microsoft Active Directory para obtener información sobre cómo automatizar este paso. Si utiliza el directorio de IAM Identity Center como origen de identidad, no desactive todavía el acceso de los usuarios. Inhabilitará el acceso de usuarios en el paso 6.

5. En la consola del IAM Identity Center, busque al usuario y elimine su sesión activa.
  - a. Seleccione Usuarios.
  - b. Elija el usuario cuya sesión activa desea eliminar.
  - c. En la página de detalles del usuario, elija la pestaña Sesiones activas.
  - d. Seleccione las casillas de verificación situadas junto a las identidades que desea eliminar y elija Eliminar sesión.

Tras eliminar una sesión de usuario, el usuario perderá inmediatamente el acceso al portal de AWS acceso. Obtenga información sobre la [duración de la sesión](#).

6. En la consola del IAM Identity Center, deshabilite el acceso de los usuarios.
  - a. Seleccione Usuarios.
  - b. Seleccione el usuario cuyo acceso desea desactivar.
  - c. En la página de detalles del usuario, expanda Información general y pulse el botón Desactivar el acceso del usuario para evitar que el usuario vuelva a iniciar sesión.
7. Deje en vigor la política de denegación durante al menos 12 horas. De lo contrario, el usuario con una sesión de rol de IAM activa habrá restablecido las acciones con el rol de IAM. Si espera 12 horas, las sesiones activas caducan y el usuario no podrá volver a acceder al rol de IAM.

#### Important

Si deshabilita el acceso de un usuario antes de detener la sesión de usuario (completó el paso 6 sin completar el paso 5), ya no podrá detener la sesión del usuario a través de la consola del IAM Identity Center. Si inhabilita el acceso del usuario sin darse cuenta antes de detener la sesión, puede volver a habilitar al usuario, detener su sesión y, a continuación, volver a deshabilitar su acceso.

[Ahora puede cambiar las credenciales del usuario si su contraseña está comprometida y restaurar sus asignaciones.](#)

## Delegue quién puede asignar el acceso de inicio de sesión único a los usuarios y grupos de la cuenta de administración

La concesión de acceso de inicio de sesión único a la cuenta de administración utilizando la consola de IAM Identity Center es una acción que requiere privilegios. De forma predeterminada, solo un usuario Usuario raíz de la cuenta de AWS o un usuario que tenga asociadas las políticas IAMFullAccess AWS administradas AWSSSOMasterAccountAdministratory las políticas administradas puede asignar el acceso de inicio de sesión único a la cuenta de administración. Las IAMFullAccesspolíticas AWSSSOMasterAccountAdministratory gestionan el acceso mediante inicio de sesión único a la cuenta de administración de una organización. AWS Organizations

Como alternativa, puede utilizarlas AWS CLI para crear conjuntos de permisos, adjuntar políticas y asignarlos. A continuación se enumeran los comandos de cada paso:

- Para crear un conjunto de permisos: [create-permission-set](#)
- Para adjuntarlo AWS Managed Policy a un conjunto de permisos: [attach-managed-policy-to-permission-set](#)
- [Para adjuntar una política gestionada por el cliente a un conjunto de permisos: - attach-customer-managed-policy to-permission-set](#)
- Para asignar un conjunto de permisos a un director: [create-account-assignment](#)

Siga los pasos que se describen a continuación para delegar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos en su directorio.

Para otorgar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos del directorio

1. Inicie sesión en la consola de IAM Identity Center como usuario raíz de la cuenta de administración o con otro usuario que tenga permisos de administrador en la cuenta de administración.
2. Siga los pasos que se indican en [Crea un conjunto de permisos](#). para crear un conjunto de permisos y, a continuación, haga lo siguiente:
  1. En la página Crear un conjunto de permisos nuevo, active la casilla Crear un conjunto de permisos personalizado y, a continuación, elija Siguiente: Detalles.

2. En la página Crear un nuevo conjunto de permisos, especifique un nombre para el conjunto de permisos personalizado y, si lo desea, una descripción. Si es necesario, modifique la duración de la sesión y especifique una URL de estado de retransmisión.

 Note

Para la URL del estado de retransmisión, debe especificar una URL que esté en la Consola de administración de AWS. Por ejemplo:

**`https://console.aws.amazon.com/ec2/`**

Para obtener más información, consulte [Configure el estado de la retransmisión para acceder rápidamente a Consola de administración de AWS](#).

3. En ¿Qué políticas desea incluir en su conjunto de permisos?, active la casilla Adjuntar políticas administradas de AWS .
  4. En la lista de políticas de IAM, elija tanto la política como AWSSSOMasterAccountAdministratorla IAMFullAccess AWS gestionada. Estas políticas conceden permisos a todos los usuarios a los que se les asigne acceso a este conjunto de permisos en el futuro.
  5. Elija Siguiente: etiquetas.
  6. En Añadir etiquetas (opcional), especifique los valores de clave y valor (opcional) y, a continuación, seleccione Siguiente: revisar. Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).
  7. Revise las selecciones y, a continuación, elija Crear.
3. Siga los pasos que se indican en [Asigne el acceso de usuario o grupo a Cuentas de AWS](#) para asignar los usuarios y grupos adecuados al conjunto de permisos que acaba de crear.
  4. Informe a los usuarios asignados de que, cuando inicien sesión en el portal de acceso AWS y seleccionen la pestaña Cuentas, deberán elegir el nombre de característica adecuado para autenticarse con los permisos que usted acaba de delegar.

## Administre Cuentas de AWS con conjuntos de permisos

Un conjunto de permisos es una plantilla que usted crea y mantiene, y que define un conjunto de una o más [políticas de IAM](#). Los conjuntos de permisos simplifican la asignación del Cuenta de AWS acceso a los usuarios y grupos de su organización. Por ejemplo, puede crear un conjunto de permisos de administrador de bases de datos que incluya políticas para administrar los servicios de

AWS RDS, DynamoDB y Aurora, y usar ese conjunto de permisos único para conceder acceso a una lista de objetivos Cuentas de AWS de su organización a los administradores de [AWS bases de datos](#).

El Centro de identidad de IAM asigna el acceso a un usuario o grupo de uno o más con conjuntos de permisos. Cuentas de AWS Cuando asigna un conjunto de permisos, IAM Identity Center crea los roles de IAM controlados por IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de identidad de IAM administra la función y permite que los usuarios autorizados que haya definido asuman la función mediante el portal de usuarios de IAM Identity Center o la CLI AWS . A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia.

Puede agregar [políticas administradas por AWS](#), [políticas administradas por los clientes](#), [políticas insertadas](#) y [políticas administradas por AWS para las funciones de trabajo](#) a sus conjuntos de permisos. También puede asignar una política administrada por AWS o una política administrada por el cliente como [límite de permisos](#).

Para crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

## Creación de un conjunto de permisos que aplique los permisos de privilegio mínimo

Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo a uno o más usuarios. Los conjuntos de permisos creados en el procedimiento anterior proporcionan un punto de partida para evaluar la cantidad de acceso a los recursos que necesitan los usuarios. Para cambiar a los permisos con privilegios mínimos, puede ejecutar IAM Access Analyzer para supervisar a los directores con políticas gestionadas. AWS Después de saber qué permisos están utilizando, puede escribir una política personalizada o generar una política con solo los permisos necesarios para su equipo.

Con IAM Identity Center, puede asignar varios conjuntos de permisos al mismo usuario. A su usuario administrativo también se le deben asignar conjuntos de permisos adicionales y más restrictivos. De esta forma, pueden acceder a usted solo Cuenta de AWS con los permisos necesarios, en lugar de utilizar siempre sus permisos administrativos.

Por ejemplo, si es desarrollador, después de crear su usuario administrativo en IAM Identity Center, puede crear un nuevo conjunto de permisos que conceda permisos de `PowerUserAccess` y, a continuación, asignarse ese conjunto de permisos a usted. A diferencia del conjunto de permisos administrativos, que utiliza permisos de `AdministratorAccess`, el conjunto de permisos de `PowerUserAccess` no permite la administración de usuarios de IAM y grupos. Al iniciar sesión en el AWS portal de acceso para acceder a su AWS cuenta, puede `PowerUserAccess` elegir no `AdministratorAccess` realizar las tareas de desarrollo en la cuenta.

Tenga en cuenta las siguientes consideraciones:

- Para empezar rápidamente a crear un conjunto de permisos más restrictivo, utilice un conjunto de permisos predefinido en lugar de uno personalizado.

Con un conjunto de permisos predefinido, que utiliza [permisos predefinidos](#), puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel específico de acceso a AWS los servicios y recursos o permisos para una función laboral común. Para obtener información sobre cada una de estas políticas, consulte [Políticas administradas de AWS para funciones de trabajo](#).

- Puede configurar la duración de la sesión de un conjunto de permisos para controlar el tiempo que un usuario permanece registrado en una Cuenta de AWS.

Cuando los usuarios se federan Cuenta de AWS y utilizan la consola de AWS gestión o la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, el valor de Duración de la sesión, que determina el tiempo que un usuario puede iniciar sesión Cuenta de AWS antes de AWS cerrar la sesión del usuario, se establece en una hora. Puede especificar un valor máximo de 12 horas. Para obtener más información, consulte [Establezca la duración de la sesión para Cuentas de AWS](#).

- También puede configurar la duración de la sesión del portal de AWS acceso para controlar el tiempo que un usuario de la fuerza laboral permanece conectado al portal.

De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de Workforce puede iniciar sesión en el portal de AWS acceso antes de tener que volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte [Configuración de la duración de la sesión en IAM Identity Center](#).

- Cuando inicie sesión en el portal de AWS acceso, elija el rol que proporciona los permisos con privilegios mínimos.

Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el AWS portal de acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de `AdministratorAccess`.

- Puede agregar otros usuarios a IAM Identity Center y asignar conjuntos de permisos nuevos o existentes a esos usuarios.

Para obtener información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

## Temas

- [Permisos predefinidos para las políticas AWS administradas](#)
- [Permisos personalizados para las políticas AWS administradas y administradas por los clientes](#)
- [Creación, administración y eliminación de conjuntos de permisos](#)
- [Configure las propiedades del conjunto de permisos](#)

## Permisos predefinidos para las políticas AWS administradas

Puede crear un conjunto de permisos predefinido con políticas AWS administradas.

Cuando crea un conjunto de permisos con permisos predefinidos, elige una política de una lista de políticas AWS administradas. Dentro de las políticas disponibles, puede elegir entre políticas de permisos comunes y políticas de funciones de trabajo.

### Políticas de permisos comunes

Elija de una lista de políticas AWS administradas que le permitan acceder a los recursos en su totalidad Cuenta de AWS. Puede agregar una de las siguientes políticas:

- `AdministratorAccess`
- `PowerUserAccess`
- `ReadOnlyAccess`
- `ViewOnlyAccess`

## Políticas de funciones de trabajo

Elija de una lista de políticas AWS administradas que le permitan acceder a sus recursos Cuenta de AWS que puedan ser relevantes para un puesto en su organización. Puede agregar una de las siguientes políticas:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Para obtener una descripción detallada de las políticas de permisos y las políticas de funciones de trabajo comunes disponibles, consulte [políticas administradas de AWS para las funciones de trabajo](#) en la Guía del usuario de AWS Identity and Access Management .

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

## Permisos personalizados para las políticas AWS administradas y administradas por los clientes

Puede crear un conjunto de permisos con permisos personalizados y combinar cualquiera de las políticas AWS administradas y administradas por los clientes que tenga en AWS Identity and Access Management (IAM) con las políticas integradas. También puede incluir el límite de permisos al establecer el máximo de permisos posibles que otras políticas pueden conceder a los usuarios de su conjunto de permisos.

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

Tipos de políticas que puede adjuntar a su conjunto de permisos

### Temas

- [Políticas insertadas](#)
- [AWS políticas gestionadas](#)



- [Políticas administradas por el cliente](#)
- [Límites de permisos](#)

## Políticas insertadas

Puede adjuntar una política insertada a un conjunto de permisos. Una política insertada es un bloque de texto con el formato de una política de IAM que se añade directamente al conjunto de permisos. Al crear un conjunto de permisos nuevo, puede pegar una política o generar una nueva con la herramienta de creación de políticas de la consola de IAM Identity Center. También puede crear políticas de IAM con el [generador de políticas de AWS](#).

Al implementar un conjunto de permisos con una política integrada, el Centro de Identidad de IAM crea una política de IAM en la que Cuentas de AWS se asigna el conjunto de permisos. IAM Identity Center crea la política al asignar el conjunto de permisos definido en la cuenta. A continuación, la política se adjunta a la función de IAM Cuenta de AWS que asuma su usuario.

Cuando crea una política en línea y asigna su conjunto de permisos, IAM Identity Center configura las políticas propias por usted. Cuentas de AWS Al crear su conjunto de permisos [Políticas administradas por el cliente](#), debe crear las políticas usted Cuentas de AWS mismo antes de asignarlo.

## AWS políticas gestionadas

Puede adjuntar políticas AWS administradas a su conjunto de permisos. AWS las políticas gestionadas son políticas de IAM que AWS mantiene. Por el contrario, [Políticas administradas por el cliente](#) son las políticas de IAM de su cuenta las que usted crea y mantiene. AWS las políticas gestionadas abordan los casos de uso más comunes con privilegios mínimos en su Cuenta de AWS. Puede asignar una política AWS gestionada como permisos para la función que crea IAM Identity Center o como [límite de permisos](#).

AWS mantiene [políticas AWS gestionadas para las funciones laborales](#) que asignan permisos de acceso a sus recursos específicos para cada trabajo. AWS Puede agregar una política de función de trabajo si decide utilizar permisos predefinidos con su conjunto de permisos. Al elegir permisos personalizados, puede agregar más de una política de función de trabajo.

Cuenta de AWS También contiene una gran cantidad de políticas de IAM AWS gestionadas para aplicaciones específicas Servicios de AWS y combinaciones de ellas. Servicios de AWS Al crear un conjunto de permisos con permisos personalizados, puede elegir entre muchas políticas AWS gestionadas adicionales para asignarlas a su conjunto de permisos.

AWS rellena cada una de ellas Cuenta de AWS con políticas AWS administradas. Para implementar un conjunto de permisos con políticas AWS administradas, no necesita crear primero una política en su Cuentas de AWS. Al crear su conjunto de permisos [Políticas administradas por el cliente](#), debe crear las políticas usted Cuentas de AWS mismo antes de asignar el conjunto de permisos.

Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

## Políticas administradas por el cliente

Puede adjuntar políticas administradas por el cliente a su conjunto de permisos. Las políticas administradas por el cliente son políticas de IAM de su cuenta que usted crea y mantiene. Por el contrario, [AWS políticas gestionadas](#) son las políticas de IAM de su cuenta las que se AWS mantienen. Puede asignar una política administrada por el cliente como permisos para el rol que crea IAM Identity Center o como [límite de permisos](#).

Al crear un conjunto de permisos con una política gestionada por el cliente, debe crear una política de IAM con el mismo nombre y la misma ruta en cada uno de los Cuenta de AWS lugares en los que IAM Identity Center asigne el conjunto de permisos. Si va a especificar una ruta personalizada, asegúrese de especificar la misma ruta en cada una de Cuenta de AWS. Para obtener más información, consulte [Nombres fáciles de recordar y rutas](#) en la Guía del usuario de IAM. IAM Identity Center adjunta la política de IAM al rol de IAM que crea en su Cuenta de AWS. Como práctica recomendada, aplique los mismos permisos a la política en cada cuenta a la que asigne el conjunto de permisos. Para obtener más información, consulte [Utilice las políticas de IAM en los conjuntos de permisos](#).

### Note

Cuando una política administrada por el cliente se adjunta a un conjunto de permisos, el nombre de la política no distingue entre mayúsculas y minúsculas.

Para obtener más información, consulte [Políticas administradas por el cliente](#) en la Guía del usuario de IAM.

## Límites de permisos

Puede adjuntar un límite de permisos a su conjunto de permisos. Un límite de permisos es una política de IAM AWS gestionada o gestionada por el cliente que establece los permisos máximos

que una política basada en la identidad puede conceder a un responsable de IAM. Cuando aplica un límite de permisos, su [Políticas insertadas](#), [Políticas administradas por el cliente](#) y [AWS políticas gestionadas](#) no pueden conceder ningún permiso que exceda los permisos que concede su límite de permisos. Un límite de permisos no concede ningún permiso, sino que hace que IAM ignore todos los permisos que exceden límite.

Al crear un conjunto de permisos con una política administrada por el cliente como límite de permisos, debe crear una política de IAM con el mismo nombre en cada Cuenta de AWS donde IAM Identity Center asigne el conjunto de permisos. IAM Identity Center adjunta la política de IAM como límite de permisos al rol de IAM que usted crea en su Cuenta de AWS .

Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.

## Creación, administración y eliminación de conjuntos de permisos

Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

### Note

Puede buscar y ordenar los conjuntos de permisos en la consola de IAM Identity Center.

Tenga en cuenta las siguientes consideraciones al crear conjuntos de permisos:

- Instancia de organización

Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

- Comience con un conjunto de permisos predefinido

Con un conjunto de permisos predefinido, que utiliza [permisos predefinidos](#), puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel específico de acceso a AWS los servicios y recursos o permisos para una función laboral común.

Para obtener información sobre cada una de estas políticas, consulte [Políticas administradas de AWS para funciones de trabajo](#). Una vez recopilados los datos de uso, puede refinar el conjunto de permisos para que sea más restrictivo.

- Limite la duración de las sesiones de administración a periodos de trabajo razonables

Cuando los usuarios se federan en su Cuenta de AWS Consola de administración de AWS o utilizan la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. Cuando la sesión del usuario alcance la duración de la sesión, se cerrará la sesión de la consola y se le pedirá que vuelva a iniciar sesión. Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol. De forma predeterminada, el valor de Duración de la sesión es de una hora. Puede especificar un valor máximo de 12 horas. Para obtener más información, consulte [Establezca la duración de la sesión para Cuentas de AWS](#).

- Limite la duración de las sesiones en el portal de usuarios de la plantilla

Los usuarios de la plantilla utilizan las sesiones del portal para elegir los roles y acceder a las aplicaciones. De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de la fuerza laboral puede iniciar sesión en el portal de AWS acceso antes de volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte [Configuración de la duración de la sesión en IAM Identity Center](#).

- Utilice el rol que proporcione permisos con privilegios mínimos

Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el portal de AWS acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de AdministratorAccess. Pruebe sus conjuntos de permisos para comprobar que proporcionan el acceso necesario antes de enviar la invitación al usuario.

#### Note

También puede utilizar [AWS CloudFormation](#) para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos.

## Temas

- [Crea un conjunto de permisos.](#)
- [Ver y cambiar un conjunto de permisos](#)
- [Delegue la administración del conjunto de permisos](#)
- [Utilice las políticas de IAM en los conjuntos de permisos](#)
- [Eliminación de conjuntos de permisos de IAM Identity Center](#)
- [Eliminación de conjuntos de permisos de IAM Identity Center](#)

## Crea un conjunto de permisos.

Utilice este procedimiento para crear un conjunto de permisos predefinido que utilice una única política administrada o un conjunto de permisos personalizado de AWS que utilice hasta 10 políticas de AWS administradas o administradas por el cliente y una política integrada. Puede solicitar un ajuste en el número máximo de 10 políticas en la [consola Service Quotas](#) para IAM. Puede crear un conjunto de permisos en la consola de IAM Identity Center.

### Note

Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Creación de un conjunto de permisos

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija Crear conjunto de permisos.
4. En la página Seleccione el tipo de conjunto de permisos, en Tipo de conjunto de permisos, seleccione un tipo.
5. Elija una o más políticas que desee usar para el conjunto de permisos, en característica del tipo de conjunto de permisos:
  - Conjunto de permisos predefinido
    1. En Política para el conjunto de permisos predefinido, seleccione una de las políticas de característica de trabajo o de permisos comunes de IAM de la lista y, a continuación, elija Siguiente. Con el fin de obtener más información, consulte las [políticas administradas](#)

[por AWS](#) o las [políticas características de trabajo administradas por AWS](#) en la Guía del usuario de AWS Identity and Access Management IAM.

2. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.

- Conjunto de permisos personalizado

1. Elija Siguiente.

2. En la página Especificar políticas y límite de permisos, elija los tipos de políticas de IAM que desee aplicar a su nuevo conjunto de permisos. De forma predeterminada, puede añadir cualquier combinación de hasta 10 políticas administradas de AWS y políticas administradas por el cliente a su conjunto de permisos. Esta cuota la establece IAM. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas administradas asociadas a un rol de IAM en la consola de Service Quotas para cada Cuenta de AWS en la que desee asignar el conjunto de permisos.

- Amplíe las políticas AWS gestionadas para añadir políticas de IAM que AWS creen y mantengan. Para obtener más información, consulte [AWS políticas gestionadas](#).

- a. Busque y elija las políticas administradas de AWS que desee aplicar a sus usuarios en el conjunto de permisos.

- b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.

- Amplíe las políticas administradas por el cliente para añadir políticas de IAM que usted cree y mantiene. Para obtener más información, consulte [Políticas administradas por el cliente](#).

- a. Elija Adjuntar políticas e introduzca el nombre de la política que desee añadir a su conjunto de permisos. En cada cuenta a la que desee asignar el conjunto de permisos, cree una política con el nombre que ingresó. Como práctica recomendada, asigne los mismos permisos a la política en cada cuenta.

- b. Seleccione Adjuntar más para añadir otra política.

- c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.

- Amplíe Política integrada para agregar un texto de política personalizado con formato JSON. Las políticas insertadas no se corresponden con los recursos de IAM existentes. Para crear una política en línea, introduce un lenguaje de política personalizado en el formulario proporcionado. IAM Identity Center añade la política a los recursos de IAM que crea en las cuentas de sus miembros. Para obtener más información, consulte [Políticas insertadas](#).
    - a. Agregue las acciones y los recursos que desee en el editor interactivo a su política integrada. Se pueden agregar declaraciones adicionales con Agregar nueva declaración.
    - b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
  - Amplíe el límite de permisos para añadir una AWS política de IAM gestionada o gestionada por el cliente como máximo de permisos que pueden asignar las demás políticas del conjunto de permisos. Para obtener más información, consulte [Límites de permisos](#).
    - a. Elija Utilizar un límite de permisos para controlar los permisos máximos.
    - b. Elija una política administrada por AWS para establecer una política de IAM que AWS cree y mantenga como sus límites de permisos. Elija políticas administradas por el cliente para establecer una política de IAM que usted cree y mantenga como sus límites de permisos.
    - c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
6. En la página Especificar detalles de conjunto de permisos, haga lo siguiente:
1. En Nombre del conjunto de permisos, escriba un nombre para identificar este conjunto de permisos en IAM Identity Center. El nombre que especifique para este conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol.

 Note

Los nombres de conjuntos de permisos deben ser únicos en la instancia de IAM Identity Center.

2. (Opcional) También puede introducir una descripción. La descripción solo aparece en la consola del IAM Identity Center, no en el portal de AWS acceso.
3. (Opcional) Especifique el valor de la duración de la sesión. Este valor determina el tiempo que un usuario puede iniciar sesión antes de que la consola cierre su sesión. Para obtener más información, consulte [Establezca la duración de la sesión para Cuentas de AWS](#).
4. (Opcional) Especifique el valor del estado de retransmisión. Este valor se utiliza en el proceso de federación para redirigir a los usuarios dentro de la cuenta. Para obtener más información, consulte [Configure el estado de la retransmisión para acceder rápidamente a Consola de administración de AWS](#).

 Note

La URL del estado de retransmisión debe estar dentro de la Consola de administración de AWS. Por ejemplo:

**<https://console.aws.amazon.com/ec2/>**

5. Expanda Etiquetas (opcional), elija Añadir etiqueta, y especifique los valores de Clave y valor (opcional).

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

6. Elija Siguiente.
7. En la página Revisar y crear, revise las selecciones que ha realizado y, a continuación, elija Crear.
8. De forma predeterminada, al crear un conjunto de permisos, el conjunto de permisos no se aprovisiona (se usa en ninguno Cuentas de AWS). Para aprovisionar un conjunto de permisos en una Cuenta de AWS, debe asignar el acceso al Centro de Identidad de IAM a los usuarios y grupos de la cuenta y, a continuación, aplicar el conjunto de permisos a esos usuarios y grupos. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).



## Ver y cambiar un conjunto de permisos

Puede utilizar conjuntos de permisos para conceder acceso a los usuarios a las Cuentas de AWS. Puede ver y cambiar un conjunto de permisos con la AWS IAM Identity Center consola. Puede buscar y ordenar los conjuntos de permisos en la consola de IAM Identity Center. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [the section called “Conjuntos de permisos”](#).

No se requieren conjuntos de permisos para administrar el acceso de los usuarios a las aplicaciones.

### Note

Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Vista de asignaciones de conjuntos de permisos

Utilice este procedimiento para ver un conjunto de permisos con la consola AWS IAM Identity Center .

All Cuentas de AWS where a permission set is provisioned

Para ver todas las asignaciones de un conjunto de permisos, utilice el siguiente procedimiento:

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Conjuntos de permisos.
3. En la página Conjuntos de permisos, seleccione el conjunto de permisos que desee ver.
4. Una vez en la página de conjuntos de permisos seleccionados, en la pestaña Cuentas, podrá ver las cuentas en las que se utiliza el conjunto de permisos. Puede seleccionar la cuenta para ver cómo se aprovisiona el conjunto de permisos en la cuenta. Puede [eliminar](#), editar y adjuntar políticas al conjunto de permisos.

## All permission sets for an Cuenta de AWS

Para ver todas las asignaciones de un conjunto de permisos, utilice el siguiente procedimiento:

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Cuentas de AWS. Seleccione la cuenta de la que desee ver los conjuntos de permisos aprovisionados.
3. Una vez en la Cuenta de AWS página seleccionada, en la pestaña Conjuntos de permisos, puede ver los diferentes conjuntos de permisos asignados al seleccionado Cuenta de AWS. Puede seleccionar el hipervínculo del conjunto de permisos para obtener más información sobre el conjunto de permisos.

## All applied permission sets to users and groups

Para ver todos los conjuntos de permisos asignados a usuarios o grupos, utilice el siguiente procedimiento:

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. Seleccione Usuarios o Grupos en el Panel para ver los usuarios o grupos de IAM Identity Center.
  - a. Una vez en la página Usuarios, seleccione el usuario al que desee ver los conjuntos de permisos aplicados. A continuación, seleccione la pestaña Cuentas de AWS y la Cuenta de AWS en la sección acceso a la cuenta de AWS . Podrá ver los conjuntos de permisos aplicados y Cuenta de AWS para el usuario seleccionado.
  - b. Una vez en la página Grupos, seleccione el grupo en el que desee ver los conjuntos de permisos aplicados. A continuación, seleccione la pestaña Cuentas de AWS y la Cuenta de AWS en la sección acceso a la Cuenta de AWS . Podrá ver los conjuntos de permisos aplicados y Cuenta de AWS para el grupo seleccionado.

## Cambiar un conjunto de permisos

Utilice este procedimiento para cambiar un [conjunto de permisos](#) con la consola de IAM Identity Center. Puede agregar o eliminar conjuntos de permisos de los usuarios o los grupos.

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Cuentas de AWS.

3. En la página Cuenta de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre de la Cuenta de AWS de la que desea cambiar el conjunto de permisos.
4. En la página Descripción general de la Cuenta de AWS, en Usuarios y grupos asignados, seleccione el nombre de usuario o el nombre del grupo del conjunto de permisos que desee cambiar. A continuación, elija Cambiar conjuntos de permisos.
5. Realice los cambios que desee en el conjunto de permisos y, a continuación, seleccione Guardar cambios.
6. Vaya a la pestaña Conjuntos de permisos, seleccione el conjunto de permisos modificado recientemente y elija Actualizar.
7. En la página Actualizar permisos, seleccione Actualizar.

## Delegue la administración del conjunto de permisos

El Centro de Identidad de IAM le permite delegar la administración de los conjuntos de permisos y las asignaciones en las cuentas mediante la creación de [políticas de IAM](#) que hacen referencia a los [nombres de recursos de Amazon \(ARNs\) de los recursos](#) del Centro de Identidad de IAM. Por ejemplo, puede crear políticas que permitan a distintos administradores administrar las asignaciones en cuentas específicas para conjuntos de permisos con etiquetas específicas.

### Note

Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Puede utilizar uno de los siguientes métodos para crear este tipo de políticas.

- (Recomendado) Cree [conjuntos de permisos](#) en IAM Identity Center, cada uno con una política diferente, y asigne los conjuntos de permisos a distintos usuarios o grupos. Esto le permite administrar permisos administrativos de los usuarios que inician sesión en el [origen de identidad de IAM Identity Center](#) que haya elegido.
- Cree políticas personalizadas en IAM y, a continuación, adjúntelas a los roles de IAM que asuman sus administradores. Para obtener información sobre las características, consulte [roles de IAM](#) para obtener los permisos administrativos que se les han asignado en IAM Identity Center.

**⚠ Important**

Los recursos del IAM Identity Center distinguen mayúsculas de minúsculas ARNs .

A continuación, se muestra el caso adecuado para hacer referencia al conjunto de permisos y los tipos de recursos de la cuenta de IAM Identity Center.

| Tipos de recursos | ARN                                                                     | Claves de contexto         |
|-------------------|-------------------------------------------------------------------------|----------------------------|
| PermissionSet     | arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId} | aws:ResourceTag/\${TagKey} |
| Cuenta            | arn:\${Partition}:sso::account/\${AccountId}                            | No aplicable               |

## Utilice las políticas de IAM en los conjuntos de permisos

En [Crea un conjunto de permisos](#), aprendió a añadir políticas, incluidas las políticas administradas por el cliente y los límites de permisos, a un conjunto de permisos. Al añadir políticas y permisos administrados por el cliente a un conjunto de permisos, IAM Identity Center no crea ninguna política en Cuentas de AWS. En su lugar, debe crear esas políticas por adelantado en cada cuenta a la que desee asignar su conjunto de permisos y hacerlas coincidir con las especificaciones de nombre y ruta de su conjunto de permisos. Cuando asignas un conjunto de permisos a un Cuenta de AWS miembro de tu organización, el Centro de Identidad de IAM crea un [rol AWS Identity and Access Management \(IAM\)](#) y asocia tus políticas de [IAM](#) a ese rol.

### Consideraciones

- Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).
- Antes de asignar el conjunto de permisos a las políticas de IAM, debe preparar su cuenta de miembro. El nombre de una política de IAM de su cuenta de miembro debe coincidir con el nombre

de la política de su cuenta de administración. IAM Identity Center no puede asignar el conjunto de permisos si la política no existe en su cuenta de miembro.

 Note

Cuando una política administrada por el cliente se adjunta a un conjunto de permisos, el nombre de la política no distingue entre mayúsculas y minúsculas.

- Los permisos que otorga la política no tienen por qué coincidir exactamente entre las cuentas.

### Asignar una política de IAM a un conjunto de permisos

1. Cree una política de IAM en cada uno de los lugares a los Cuentas de AWS que desee asignar el conjunto de permisos.
2. Asignar permisos a la política de IAM. Puede asignar diferentes permisos en diferentes cuentas. Para disfrutar de una experiencia coherente, configure y mantenga permisos idénticos en cada política. Puedes usar recursos de automatización, como AWS CloudFormation StackSets crear copias de una política de IAM con el mismo nombre y permisos en cada cuenta de miembro. Para obtener más información al respecto CloudFormation StackSets, consulte Cómo [trabajar con ella AWS CloudFormation StackSets](#) en la guía del AWS CloudFormation usuario.
3. Cree un conjunto de permisos en su cuenta de administración y añada su política de IAM a las políticas administradas por el cliente o al límite de permisos. Para obtener más información sobre cómo crear un conjunto de permisos, consulte [Crea un conjunto de permisos](#).
4. Añada cualquier política integrada, política administrada por AWS o política de IAM adicional que haya preparado.
5. Cree y asigne su conjunto de permisos.

### Eliminación de conjuntos de permisos de IAM Identity Center

Puede eliminar un conjunto de permisos de los usuarios y grupos de IAM Identity Center en la consola de IAM Identity Center. También puede eliminar un conjunto de permisos de una Cuenta de AWS. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

**Note**

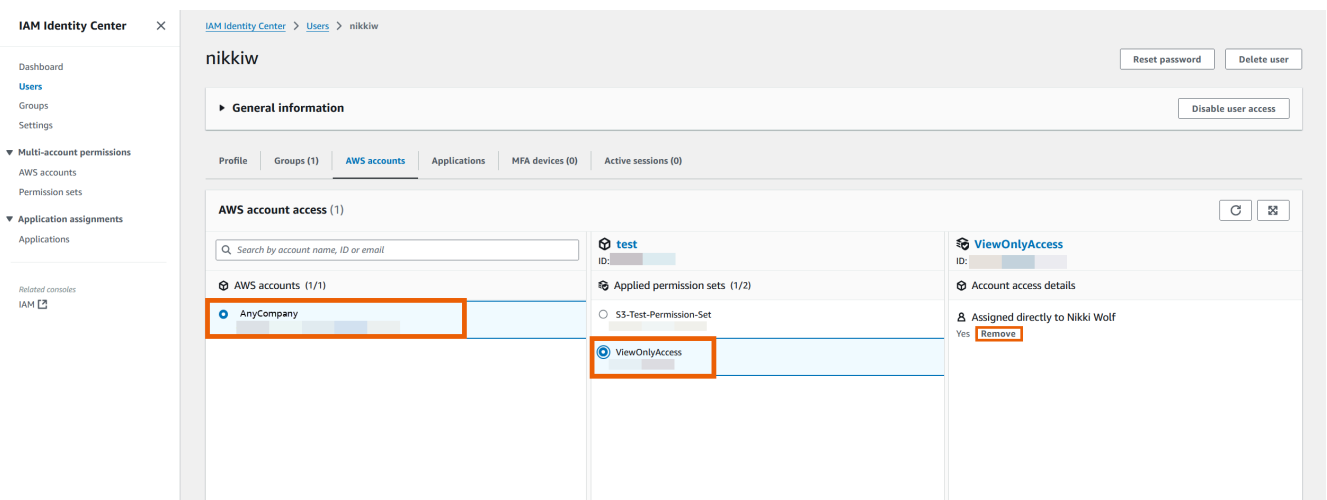
Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Remove permission set from a user

### Eliminación de un conjunto de permisos de un usuario

Utilice este procedimiento para eliminar un conjunto de permisos de un usuario con la consola de IAM Identity Center.

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En IAM Identity Center, seleccione Usuarios.
3. Seleccione el nombre de usuario del usuario al que desea eliminarle el conjunto de permisos.
4. En la página Detalles, elija la pestaña Cuentas de AWS. En acceso a la Cuenta de AWS , seleccione su Cuenta de AWS.
5. En el panel derecho, aparecen los permisos aplicados al usuario seleccionado. Seleccione el conjunto de permisos que desea eliminar. En Detalles de acceso a la cuenta, seleccione Eliminar.
6. Aparece un cuadro de diálogo que le pregunta si desea eliminar este conjunto de permisos. Seleccione Eliminar.

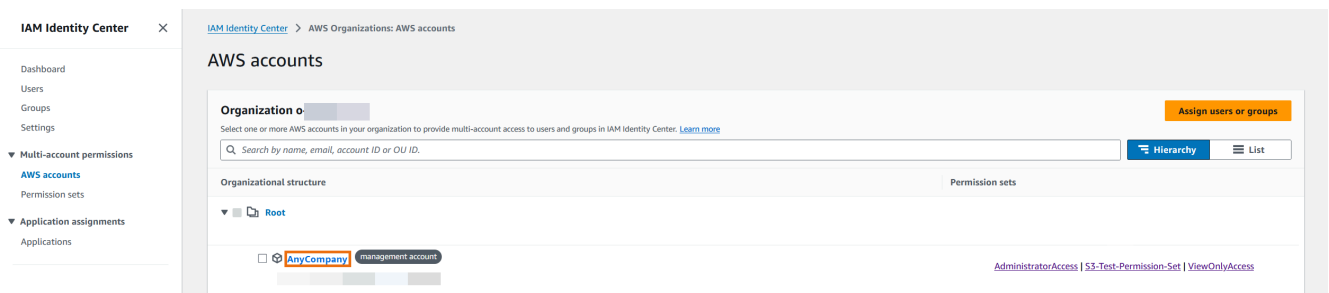


## Remove permission set from a group

### Eliminación de un conjunto de permisos de un grupo

Utilice este procedimiento para eliminar un conjunto de permisos de un grupo con la consola de IAM Identity Center.

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en. <https://console.aws.amazon.com/singlesignon/>
2. En Permisos para varias cuentas, seleccione Cuentas de AWS. Seleccione el enlace a su cuenta de administración.



3. En la pestaña Usuarios y grupos asignados, seleccione el grupo del que quiere eliminar el conjunto de permisos y, a continuación, seleccione Cambiar conjuntos de permisos.
4. En la página Cambiar conjuntos de permisos, borre el conjunto de permisos que desea eliminar y, a continuación, seleccione Guardar cambios.

## Remove permission set from an Cuenta de AWS

Utilice este procedimiento para eliminar un conjunto de permisos de la Cuenta de AWS con la consola de IAM Identity Center.

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, seleccione Cuentas de AWS. Seleccione el nombre Cuenta de AWS del que desea eliminar el conjunto de permisos.
3. En la página de Descripción general de la Cuenta de AWS, seleccione la pestaña Conjuntos de permisos. Seleccione el conjunto de permisos que desea eliminar. A continuación, seleccione Eliminar.

4. En el cuadro de diálogo Eliminar conjunto de permisos, confirme que se ha seleccionado el conjunto de permisos correcto, escriba **Delete** para confirmar la eliminación y, a continuación, seleccione Eliminar acceso.

## Eliminación de conjuntos de permisos de IAM Identity Center

Antes de poder eliminar un conjunto de permisos de IAM Identity Center, debe [eliminarlo](#) de todas las Cuentas de AWS que utilizan el conjunto de permisos. Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

### Consideraciones

- Para usar conjuntos de permisos, necesitará usar una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).
- Si desea revocar una sesión de conjunto de permisos activa, consulte [the section called “Finalización de las sesiones activas de los usuarios del personal”](#).
- Debe eliminar los conjuntos de permisos y las asignaciones de aplicaciones de los usuarios o grupos que desee eliminar antes de eliminarlos. De lo contrario, tendrá conjuntos de permisos y aplicaciones sin asignar y sin usar en IAM Identity Center.

Utilice el siguiente procedimiento para eliminar uno o más conjuntos de permisos, de modo que ningún miembro de la organización pueda utilizarlos. Cuenta de AWS

#### Important

Todos los usuarios y grupos a los que se haya asignado este conjunto de permisos, independientemente de quién lo utilice, ya no podrán iniciar sesión. Cuenta de AWS Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

Para eliminar un conjunto de permisos de un Cuenta de AWS

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Seleccione el conjunto de permisos que desea eliminar y, a continuación, elija Eliminar.



4. En el cuadro de diálogo Eliminar conjunto de permisos, escriba el nombre del conjunto de permisos para confirmar la eliminación y, a continuación, seleccione Eliminar. El nombre distingue entre mayúsculas y minúsculas.

## Configure las propiedades del conjunto de permisos

En el IAM Identity Center, los administradores pueden realizar las siguientes tareas de configuración y administración para controlar el acceso de los usuarios y la duración de la sesión.

| Tarea                                                                                                                                                      | Más información                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Los administradores pueden establecer la duración máxima de las sesiones de usuario al acceder a AWS los recursos a través del Centro de identidad de IAM. | <a href="#">Establezca la duración de la sesión para Cuentas de AWS</a>                                             |
| Los administradores pueden personalizar la página de destino que ven los usuarios tras autenticarse correctamente a través del IAM Identity Center.        | <a href="#">Configure el estado de la retransmisión para acceder rápidamente a Consola de administración de AWS</a> |
| Asegúrese de que los usuarios ya no tengan acceso a AWS los recursos cuando se revoquen sus permisos.                                                      | <a href="#">Utilice una política de denegación para revocar los permisos de los usuarios activos</a>                |

## Establezca la duración de la sesión para Cuentas de AWS

Para cada [conjunto de permisos](#), puede especificar una duración de la sesión para controlar el tiempo durante el cual un usuario puede iniciar sesión en una cuenta de Cuenta de AWS. Cuando transcurra la duración especificada, AWS cierra la sesión del usuario.

Al crear un nuevo conjunto de permisos, la duración de la sesión se establece de forma predeterminada en una hora (en segundos). La duración mínima de la sesión es de una hora y se puede establecer en un máximo de 12 horas. IAM Identity Center crea automáticamente roles de IAM en cada cuenta asignada para cada conjunto de permisos y las configura con una duración máxima de sesión de 12 horas.

Cuando los usuarios se federan en su Cuenta de AWS consola o cuando se utiliza el AWS Command Line Interface (AWS CLI), el Centro de Identidad de IAM utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, los roles de IAM generados por IAM Identity Center para los conjuntos de permisos solo los pueden asumir los usuarios de IAM Identity Center, lo que garantiza que se cumpla la duración de sesión especificada en el conjunto de permisos de IAM Identity Center.

 Important

Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol.

Una vez que se ha creado un conjunto de permisos, puede actualizarlo para aplicar una nueva duración de la sesión. Utilice el siguiente procedimiento para modificar la duración de la sesión para un conjunto de permisos.

Para definir la duración de la sesión

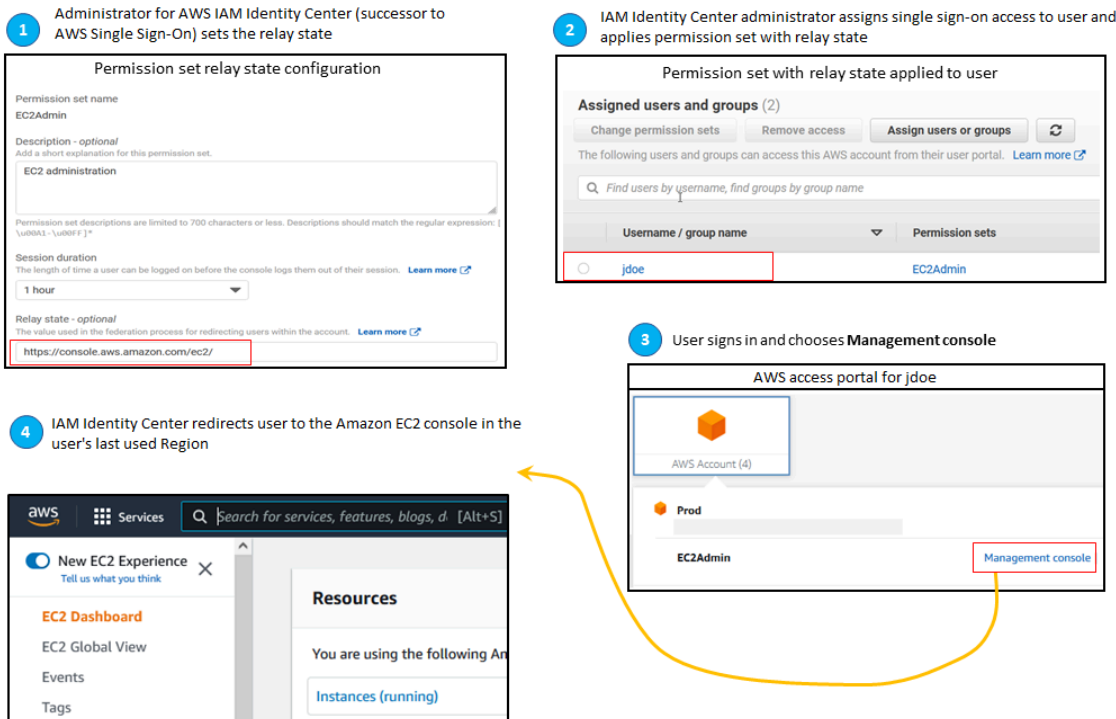
1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea cambiar la duración de la sesión.
4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.
5. En la página Editar la configuración general del conjunto de permisos, elija un nuevo valor para la duración de la sesión.
6. Si el conjunto de permisos está aprovisionado en alguna Cuentas de AWS, los nombres de las cuentas aparecen en Para volver Cuentas de AWS a aprovisionarse automáticamente. Una vez actualizado el valor de duración de la sesión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todas las Cuentas de AWS que usen el conjunto de permisos.
7. Seleccione Save changes (Guardar cambios).
8. En la parte superior de la página de Cuentas de AWS, aparece una notificación.

- Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
- Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

## Configure el estado de la retransmisión para acceder rápidamente a Consola de administración de AWS

De forma predeterminada, cuando un usuario inicia sesión en el portal de AWS acceso, elige una cuenta y, a continuación, elige el rol que AWS crea a partir del conjunto de permisos asignado, el Centro de Identidad de IAM redirige el navegador del usuario al. Consola de administración de AWS Puede cambiar este comportamiento si configura el estado de retransmisión en la URL de una consola diferente.

La configuración del estado de la retransmisión permite proporcionar al usuario un acceso rápido a la consola más adecuada para su rol. Por ejemplo, puede establecer el estado de retransmisión en la URL de la consola de Amazon EC2 (**<https://console.aws.amazon.com/ec2/>**) para redirigir al usuario a esa consola cuando elija el rol de administrador de Amazon EC2. Durante el redireccionamiento a la URL predeterminada o a la URL del estado de retransmisión, el Centro de Identidad de IAM dirige el navegador del usuario al punto final de la consola, en el último lugar Región de AWS utilizado por el usuario. Por ejemplo, si un usuario finalizó la última sesión de su consola en la región de Europa (Estocolmo) (eu-north-1), se redirige al usuario a la consola Amazon EC2 de esa región.



Para configurar IAM Identity Center para que redirija al usuario a una consola en una Región de AWS específica, incluya la especificación de la región como parte de la URL. Por ejemplo, para redirigir al usuario a la consola de Amazon EC2 en la región Este de EE. UU. (Ohio) (us-east-2), especifique la URL de la consola de Amazon EC2 en esa región (**https://us-east-2.console.aws.amazon.com/ec2/**). Si ha habilitado IAM Identity Center en la región Oeste de EE. UU. (Oregón) (us-west-2) y desea dirigir al usuario a esa región, especifique **https://us-west-2.console.aws.amazon.com**.

## Configurar el estado de la retransmisión

Utilice el siguiente procedimiento para configurar la URL del estado de retransmisión de un conjunto de permisos.

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea configurar la nueva URL de estado de retransmisión.
4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.

5. En la página Editar la configuración general del conjunto de permisos, en Estado de retransmisión, escriba la URL de la consola para cualquiera de los AWS servicios. Por ejemplo:

**`https://console.aws.amazon.com/ec2/`**

 Note

La URL del estado de retransmisión debe estar dentro de la Consola de administración de AWS.

6. Si el conjunto de permisos está aprovisionado en alguna Cuentas de AWS, los nombres de las cuentas aparecen en Cuentas de AWS Para volver a aprovisionarse automáticamente. Una vez actualizada la URL del estado de retransmisión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todas las Cuentas de AWS que usen el conjunto de permisos.
7. Seleccione Save changes (Guardar cambios).
8. En la parte superior de la página de organización de AWS , aparece una notificación.
  - Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
  - Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

 Note

Puedes automatizar este proceso mediante la AWS API, un AWS SDK o el AWS Command Line Interface(AWS CLI). Para obtener más información, consulte lo siguiente:

- Las acciones `CreatePermissionSet` o `UpdatePermissionSet` de la referencia de la [API de IAM Identity Center](#)
- Los comandos `create-permission-set` o `update-permission-set` de la sección [sso-admin](#) de la Referencia de comandos de AWS CLI .

## Utilice una política de denegación para revocar los permisos de los usuarios activos

Es posible que tengas que revocar el acceso de un usuario del Centro de Identidad de IAM Cuentas de AWS mientras esté utilizando activamente un conjunto de permisos. Puede quitarle la posibilidad de usar sus sesiones de rol de IAM activas al implementar una política de denegación para un usuario no especificado con antelación y, cuando sea necesario, puede actualizar la política de denegación para especificar el usuario cuyo acceso deseas bloquear. En este tema, se explica cómo crear una política de denegación y las consideraciones sobre cómo implementar la política.

Prepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos

Puede impedir que el usuario tome medidas con un rol de IAM que esté utilizando activamente al aplicar una política de denegación de acceso a un usuario específico mediante el uso de una política de control de servicios. También puede impedir que un usuario utilice cualquier conjunto de permisos hasta que cambie su contraseña, lo que evita que un usuario malintencionado haga un uso indebido de credenciales robadas. Si necesita denegar el acceso de forma generalizada e impedir que un usuario vuelva a entrar en un conjunto de permisos o acceda a otros conjuntos de permisos, también puede eliminar todos los accesos de los usuarios, detener la sesión activa del portal de acceso AWS e inhabilitar el inicio de sesión del usuario. Consulte [the section called “Finalización de las sesiones activas de los usuarios del personal”](#) para obtener información sobre cómo usar la política de denegación junto con acciones adicionales para una revocación de acceso más amplia.

### Política de denegación

Puede utilizar una política de denegación con una condición que coincida con el `UserID` del usuario en el almacén de identidades del IAM Identity Center para evitar que un rol de IAM que el usuario esté utilizando activamente lleve a cabo nuevas acciones. El uso de esta política evita que otros usuarios puedan estar utilizando el mismo conjunto de permisos al implementar la política de denegación. Esta política utiliza el marcador de posición de ID de usuario, *Add user ID here*, para `identitystore:userId` que deberá actualizarlo con el ID de usuario al que desee revocar el acceso.

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
```

```
    "Action": [
      "*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "identitystore:userId": "Add user ID here"
      }
    }
  }
]
```

Aunque puede usar otra clave de condición, por ejemplo, “aws:userId”, “identitystore:userId” es cierto que se trata de un valor único a nivel mundial que está asociado a una persona. El uso de “aws:userId” en esta condición puede verse afectado por la forma en que se sincronizan los atributos del usuario con respecto a la fuente de identidades y puede cambiar si el nombre de usuario o la dirección de correo electrónico del usuario cambian.

En la consola del IAM Identity Center, puede buscar el `identitystore:userId` de un usuario. Para ello, vaya a Usuarios, busque el usuario por su nombre, amplíe la sección de información general y copie el ID. También es conveniente detener la sesión del portal de AWS acceso de un usuario e inhabilitar su acceso de inicio de sesión en la misma sección mientras busca el seudónimo. Para automatizar el proceso de creación de una política de denegación, obtenga el seudónimo del usuario consultando el almacén de identidades. APIs

## Implementación de la política de denegación

Puedes usar un seudónimo que no sea válido, por ejemplo *Add user ID here*, para implementar la política de denegación con antelación mediante una política de control de servicios (SCP) que adjuntes a Cuentas de AWS los usuarios a la que puedan tener acceso. Este es el enfoque recomendado por su facilidad y velocidad de impacto. Cuando revoque el acceso de un usuario con la política de denegación, editará la política para reemplazar el marcador de posición de ID de usuario por el ID de la persona cuyo acceso deseas revocar. Esto impide que el usuario realice alguna acción con los permisos establecidos en todas las cuentas que asocie al SCP. Bloquea las acciones del usuario incluso si utiliza su sesión activa en el portal de acceso AWS para navegar a diferentes cuentas y asumir funciones diferentes. Con el acceso del usuario totalmente bloqueado por el SCP, puede deshabilitar su capacidad de iniciar sesión, revocar sus asignaciones y detener su sesión en el portal de AWS acceso si es necesario.

Como alternativa al uso SCPs, también puede incluir la política de denegación en la política integrada de conjuntos de permisos y en las políticas administradas por el cliente que utilizan los conjuntos de permisos a los que el usuario puede acceder.

Si debe revocar el acceso a más de una persona, puede utilizar una lista de valores en el bloque de condiciones, como:

```
"Condition": {
  "StringEquals": {
    "identitystore:userId": [" user1 userId", "user2 userId"...]
  }
}
```

#### Important

Independientemente del método o los métodos que utilice, debe tomar cualquier otra medida correctiva y mantener el ID del usuario en la política durante al menos 12 horas. Transcurrido ese tiempo, todas las funciones que el usuario haya asumido caducarán y, a continuación, podrá eliminar su ID de la política de denegación.

## Hacer referencia a conjuntos de permisos en las políticas de recursos, los mapas de configuración de Amazon EKS Cluster y las políticas AWS KMS clave

Al asignar un conjunto de permisos a una AWS cuenta, el Centro de Identidad de IAM crea un rol con un nombre que comienza por. `AWSReservedSSO_`

El nombre completo y el nombre de recurso de Amazon (ARN) del rol utilizan el siguiente formato:

| Name                                                                               | ARN                                                                                                               |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <code>AWSReservedSSO_ <i>permission-set-name</i><br/><i>e-unique-suffix</i></code> | <code>arn:aws:iam:: <i>aws-account-ID</i>:role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReser</code> |



| Name | ARN                                                          |
|------|--------------------------------------------------------------|
|      | vedSSO_ <i>permission-set-name</i><br><i>e_unique-suffix</i> |

Si su fuente de identidad en el Centro de identidad de IAM está alojada en us-east-1, no *aws-region* existe en el ARN. El nombre completo y el (ARN) del rol utilizan el siguiente formato:

| Name                                                                 | ARN                                                                                                                                                   |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_ <i>permission-set-name</i><br><i>e_unique-suffix</i> | arn:aws:iam:: <i>aws-account-ID</i> :role/<br>aws-reserved/sso.amazonaws.com/<br>AWSReservedSSO_ <i>permission-set-name</i><br><i>e_unique-suffix</i> |

Por ejemplo, si crea un conjunto de permisos que concede acceso a la AWS cuenta a los administradores de bases de datos, se crea el rol correspondiente con el siguiente nombre y ARN:

| Name                                                  | ARN                                                                                                                                           |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_DatabaseAdministrator_1234567890abcdef | arn:aws:iam::111122223333:role/<br>aws-reserved/sso.amazonaws.com/<br>eu-west-2/AWSReservedSSO_Dat<br>abaseAdministrator_12345678<br>90abcdef |

Si elimina todas las asignaciones a este conjunto de permisos de la AWS cuenta, también se eliminará el rol correspondiente que creó IAM Identity Center. Si más adelante realiza una nueva asignación al mismo conjunto de permisos, IAM Identity Center crea un nuevo rol para el conjunto de permisos. El nombre y el ARN del nuevo rol incluyen un sufijo diferente y único. En este ejemplo, el sufijo único es abcdef0123456789.

| Name                                                          | ARN                                                                                                                                   |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_DatabaseAdministrator_ <b>abcdef0123456789</b> | arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ <b>abcdef0123456789</b> |

El cambio de sufijo en el nuevo nombre y ARN del rol provocará que cualquier política que haga referencia al nombre y al ARN originales lo out-of-date sea, lo que interrumpirá el acceso de las personas que usen el conjunto de permisos correspondiente. Por ejemplo, un cambio en el ARN del rol interrumpirá el acceso de los usuarios del conjunto de permisos si se hace referencia al ARN original en las siguientes configuraciones:

- En el fichero `aws-auth ConfigMap` para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) cuando utiliza el `aws-auth ConfigMap` para el acceso al clúster.
- En una política basada en recursos para una clave (). AWS Key Management Service AWS KMS. Esta política también se denomina política de claves.

#### Note

Le recomendamos que utilice las [entradas de acceso de Amazon EKS](#) para gestionar el acceso a sus clústeres de Amazon EKS. Esto le permite usar los permisos de IAM para administrar los principales que tienen acceso a un clúster de Amazon EKS. Al utilizar las entradas de acceso de Amazon EKS, puede utilizar una entidad principal de IAM con permisos de Amazon EKS para recuperar el acceso a un clúster sin necesidad de ponerse en contacto con Soporte.

Si bien puede actualizar las políticas basadas en recursos de la mayoría de AWS los servicios para que hagan referencia a un nuevo ARN para un rol que corresponda a un conjunto de permisos, debe tener un rol de respaldo que cree en IAM para Amazon EKS si AWS KMS el ARN cambia. En el caso de Amazon EKS, el rol de IAM de respaldo debe existir en `aws-auth ConfigMap`. Para ello AWS KMS, debe estar en sus políticas clave. Si no tienes un rol de IAM alternativo con permisos para

actualizar la política `aws-auth ConfigMap` o la política AWS KMS clave, ponte en contacto con nosotros Soporte para recuperar el acceso a esos recursos.

## Recomendaciones para evitar interrupciones en el acceso

Para evitar interrupciones en el acceso debido a cambios en el ARN de un rol que corresponde a un conjunto de permisos, le recomendamos que haga lo siguiente.

- Mantenga al menos una asignación de conjunto de permisos.

Mantenga esta asignación en las AWS cuentas que contienen las funciones a las que hace referencia en Amazon EKS, en las políticas clave o en AWS KMS las políticas basadas en recursos para otras. `aws-auth ConfigMap` Servicios de AWS

Por ejemplo, si crea un conjunto de `EKSAccess` permisos y hace referencia al ARN de rol correspondiente desde la AWS cuenta `111122223333`, asigna permanentemente un grupo administrativo al conjunto de permisos de esa cuenta. Como la asignación es permanente, IAM Identity Center no eliminará el rol correspondiente, lo que elimina el riesgo de cambiar el nombre. El grupo administrativo siempre tendrá acceso sin correr el riesgo de que se incrementen los privilegios.

- Para los clústeres de Amazon EKS que utilizan **`aws-auth ConfigMap`** e AWS KMS incluyen un rol creado en IAM.

Si hace referencia al rol ARNs para los conjuntos de permisos de un `aws-auth ConfigMap` clúster de Amazon EKS o a las políticas clave para AWS KMS las claves, le recomendamos que también incluya al menos un rol que cree en IAM. El rol debe permitirle acceder al clúster de Amazon EKS o administrar la política AWS KMS clave. El conjunto de permisos debe poder asumir este rol. De esta forma, si el ARN del rol de un conjunto de permisos cambia, puede actualizar la referencia al ARN en la `aws-auth ConfigMap` política clave o. AWS KMS En la siguiente sección, se proporciona un ejemplo de cómo se puede crear una política de confianza para un rol creado en IAM. El rol solo lo puede asumir un conjunto de permisos de `AdministratorAccess`.

## Ejemplo de políticas de confianza personalizadas

A continuación se muestra un ejemplo de una política de confianza personalizada que proporciona un conjunto de permisos de `AdministratorAccess` con acceso a un rol creado en IAM. Entre los elementos clave de esta base, se incluyen los siguientes:

- El elemento principal de esta política de confianza especifica el principal de la AWS cuenta. En esta política, los directores de la AWS cuenta 111122223333 con `sts:AssumeRole` permisos pueden asumir la función que se crea en IAM.
- El `Condition` element de esta política de confianza especifica requisitos adicionales para las entidades principales que pueden asumir el rol creado en IAM. En esta política, el conjunto de permisos con el siguiente rol ARN puede asumir el rol.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/  
AWSReservedSSO_AdministratorAccess_*
```

#### Note

El elemento `Condition` incluye el operador de condiciones `ArnLike` y utiliza un comodín al final del ARN del rol de permisos, en lugar de un sufijo único. Esto significa que la política permite que el conjunto de permisos asuma el rol creado en IAM incluso si el ARN del rol del conjunto de permisos cambia.

## JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::111122223333:root"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {  
        "ArnLike": {  
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/  
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"  
        }  
      }  
    }  
  ]  
}
```

La inclusión de un rol que cree en IAM en dicha política le proporcionará acceso de emergencia a sus clústeres de Amazon EKS u otros AWS recursos si un conjunto de permisos o todas las asignaciones al conjunto de permisos se eliminan y se vuelven a crear accidentalmente. AWS KMS keys

## Control de acceso basado en atributos

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. Puede utilizar el Centro de Identidad de IAM para gestionar el acceso a sus AWS recursos a través de varias Cuentas de AWS atributos de usuario que procedan de cualquier fuente de identidad del Centro de Identidad de IAM. En AWS, estos atributos se denominan etiquetas. El uso de los atributos de usuario como etiquetas le ayuda a simplificar el proceso de creación de permisos detallados AWS y garantiza que sus empleados solo tengan acceso a AWS los recursos con las etiquetas correspondientes.

Por ejemplo, puede asignar a los desarrolladores Bob y Sally, que pertenecen a 2 equipos diferentes, el mismo conjunto de permisos en IAM Identity Center y, a continuación, seleccionar el atributo del nombre del equipo para controlar el acceso. Cuando Bob y Sally inician sesión en su Cuentas de AWS, el Centro de Identidad de IAM envía el atributo del nombre del equipo en la AWS sesión para que Bob y Sally solo puedan acceder a los recursos AWS del proyecto si el atributo del nombre del equipo coincide con la etiqueta del nombre del equipo del recurso del proyecto. Si Bob se pasa al equipo de Sally en el futuro, puede modificar su acceso simplemente actualizando el atributo de nombre de su equipo en el directorio corporativo. La próxima vez que Bob inicie sesión, tendrá acceso automáticamente a los recursos del proyecto de su nuevo equipo sin necesidad de actualizar los permisos de AWS.

Este enfoque también ayuda a reducir el número de permisos distintos que hay que crear y gestionar en IAM Identity Center, ya que los usuarios asociados a los mismos conjuntos de permisos ahora pueden tener permisos únicos en característica de sus atributos. Puede utilizar estos atributos de usuario en los conjuntos de permisos y las políticas basadas en recursos del Centro de Identidad de IAM para implementar el ABAC en los recursos y simplificar la gestión de permisos a gran escala AWS .

## Ventajas

Las siguientes son ventajas adicionales del uso de ABAC en IAM Identity Center.

- ABAC requiere menos conjuntos de permisos: dado que no tiene que crear diferentes políticas para diferentes roles de trabajo, debe crear menos conjuntos de permisos. Esto reduce la complejidad de la administración de permisos.
- Con ABAC, los equipos pueden cambiar y crecer rápidamente: los permisos para los nuevos recursos se conceden automáticamente en característica de los atributos cuando los recursos se etiquetan adecuadamente al crearlos.
- Utilice los atributos de los empleados de su directorio corporativo con ABAC: puede utilizar los atributos de los empleados existentes de cualquier fuente de identidad configurada en IAM Identity Center para tomar decisiones de control de acceso en AWS.
- AWS CloudTrail Controle quién accede a los recursos: los administradores de seguridad pueden determinar fácilmente la identidad de una sesión al revisar los atributos del usuario para realizar un seguimiento de la actividad de los usuarios. AWS

Para obtener información acerca de cómo configurar ABAC mediante la consola de IAM Identity Center, consulte [Atributos para controlar el acceso](#). Para obtener información sobre cómo habilitar y configurar ABAC mediante el Centro de identidad de IAM APIs, consulte [CreateInstanceAccessControlAttributeConfiguration](#) la Guía de referencia de la API del Centro de identidades de IAM.

## Temas

- [Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS](#)
- [Atributos para controlar el acceso](#)

## Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS

Esta lista de comprobación incluye las tareas de configuración necesarias para preparar los recursos de AWS y configurar IAM Identity Center para el acceso a ABAC. Completar las tareas en esta lista de verificación en orden. Cuando un enlace de referencia lo lleve a un tema, vuelva a ese tema para poder continuar con el resto de las tareas de esta lista de verificación.

| Paso | Tarea                                                                                                   | Referencia                                                                                 |
|------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1    | Revise cómo añadir etiquetas a todos sus recursos.<br>AWS Para implementar ABAC en IAM Identity Center, | <ul style="list-style-type: none"> <li>• <a href="#">Etiquetar recursos AWS</a></li> </ul> |

| Paso | Tarea                                                                                                                                                                                                                                                                                                                                                                                        | Referencia                                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | primero tendrá que añadir etiquetas a todos los recursos de AWS en los que desee implementar ABAC.                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                 |
| 2    | Revise cómo configurar su origen de identidad en IAM Identity Center con las identidades y los atributos de usuario asociados en su almacén de identidades. El Centro de Identidad de IAM le permite utilizar los atributos de usuario de cualquier fuente de identidad del Centro de Identidad de IAM compatible para ABAC in. AWS                                                          | <ul style="list-style-type: none"> <li>• <a href="#">Administración de su fuente de identidad</a></li> </ul>                                                                                                                                    |
| 3    | En función de los siguientes criterios, determine qué atributos desea utilizar para tomar decisiones de control de acceso AWS y envíelos al Centro de Identidad de IAM.                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• <a href="#">Introducción</a></li> </ul>                                                                                                                                                                |
|      | <ul style="list-style-type: none"> <li>• Si utiliza un proveedor de identidades (IdP) externo, decida si desea utilizar los atributos transferidos desde el IdP o seleccionar los atributos de IAM Identity Center.</li> </ul>                                                                                                                                                               | <ul style="list-style-type: none"> <li>• <a href="#">Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad</a></li> </ul>                                                                          |
|      | <ul style="list-style-type: none"> <li>• Si elige que su IdP envíe atributos, configure su IdP para que transmita los atributos en las aserciones de SAML. Consulte las secciones <code>Optional</code> del tutorial correspondiente a su IdP específico.</li> </ul>                                                                                                                         | <ul style="list-style-type: none"> <li>• <a href="#">Tutoriales de orígenes de identidad de IAM Identity Center</a></li> </ul>                                                                                                                  |
|      | <ul style="list-style-type: none"> <li>• Si utiliza un IdP como fuente de identidad y elige seleccionar atributos en IAM Identity Center, averigüe cómo configurar el SCIM para que los valores de los atributos procedan de su IdP. Si no puede utilizar SCIM con su IdP, añada los usuarios y sus atributos mediante la página de usuario de la consola de IAM Identity Center.</li> </ul> | <ul style="list-style-type: none"> <li>• <a href="#">Aprovisione usuarios y grupos desde un proveedor de identidades externo utilizando SCIM</a></li> <li>• <a href="#">Atributos de proveedor de identidad externos compatibles</a></li> </ul> |

| Paso | Tarea                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Referencia                                                                                                                                                                                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ul style="list-style-type: none"> <li>Si utiliza Active Directory o IAM Identity Center como fuente de identidad, o si utiliza un IdP y elige seleccionar atributos en IAM Identity Center, revise los atributos disponibles que puede configurar. A continuación, vaya inmediatamente al paso 4 para empezar a configurar los atributos de ABAC mediante la consola de IAM Identity Center.</li> </ul>                                                                                                                                | <ul style="list-style-type: none"> <li><a href="#">Elección de los atributos al utilizar IAM Identity Center como fuente de identidad</a></li> <li><a href="#">Elegir los atributos al utilizarlos AWS Managed Microsoft AD como fuente de identidad</a></li> <li><a href="#">Asignaciones predeterminadas entre IAM Identity Center y Microsoft AD</a></li> </ul> |
| 4    | <p>Seleccione los atributos que desee utilizar para ABAC en la página Atributos para el control de acceso de la consola de IAM Identity Center. En esta página, puede seleccionar los atributos para el control de acceso desde el origen de identidad que configuró en el paso 2. Una vez que sus identidades y sus atributos estén en el Centro de Identidad de IAM, debe crear pares clave-valor (mapeos) que se le transferirán Cuentas de AWS para que los utilice en las decisiones de control de acceso.</p>                     | <ul style="list-style-type: none"> <li><a href="#">Habilitación y configuración de atributos para el control de acceso</a></li> </ul>                                                                                                                                                                                                                              |
| 5    | <p>Cree políticas de permisos personalizadas dentro de su conjunto de permisos y utilice los atributos de control de acceso para crear reglas ABAC, de modo que los usuarios solo puedan acceder a los recursos con etiquetas coincidentes. Los atributos de usuario que configuró en el paso 4 se utilizan como etiquetas en AWS para tomar decisiones sobre el control de acceso. Puede hacer referencia a los atributos de control de acceso en la política de permisos mediante la condición <code>aws:PrincipalTag/key</code>.</p> | <ul style="list-style-type: none"> <li><a href="#">Crear políticas de permisos para ABAC en IAM Identity Center</a></li> </ul>                                                                                                                                                                                                                                     |



| Paso | Tarea                                                                                                                                                                                                                                                                | Referencia                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 6    | En sus archivos Cuentas de AWS, asigne los usuarios a los conjuntos de permisos que creó en el paso 5. De este modo, se garantiza que, cuando se federen en sus cuentas y accedan a AWS los recursos, solo obtengan acceso en función de las etiquetas coincidentes. | <ul style="list-style-type: none"> <li>• <a href="#">Asigne el acceso de usuario o grupo a Cuentas de AWS</a></li> </ul> |

Tras completar estos pasos, los usuarios que se federen en un único inicio Cuenta de AWS de sesión tendrán acceso a sus AWS recursos en función de los atributos coincidentes.

## Atributos para controlar el acceso

Atributos para el control de acceso es el nombre de la página de la consola de IAM Identity Center en la que se seleccionan los atributos de usuario que se quieren utilizar en las políticas para controlar el acceso a los recursos. Puedes asignar usuarios a las cargas de trabajo en AWS función de los atributos existentes en la fuente de identidad de los usuarios.

Por ejemplo, suponga que desea asignar acceso a los buckets de S3 en característica de los nombres de los departamentos. En la página Atributos para el control de acceso, seleccione el atributo de usuario Departamento para su uso con el control de acceso basado en atributos (ABAC). En el conjunto de permisos de IAM Identity Center, escriba una política que conceda acceso a los usuarios solo cuando el atributo Departamento coincida con la etiqueta de departamento que asignó a sus buckets de S3. IAM Identity Center transfiere el atributo de departamento del usuario a la cuenta a la que se accede. A continuación, el atributo se utiliza para determinar el acceso en característica de la política. Para obtener más información acerca de Pitr, consulte [Control de acceso basado en atributos](#).

## Introducción

La forma de empezar a configurar los atributos para el control de acceso depende del origen de identidad que utilice. Independientemente del origen de identidad que elija, una vez seleccionados los atributos, tendrá que crear o editar las políticas de conjuntos de permisos. Estas políticas deben permitir que las identidades de los usuarios accedan a los recursos de AWS .

### Elección de los atributos al utilizar IAM Identity Center como fuente de identidad

Al configurar IAM Identity Center como fuente de identidad, primero se añaden los usuarios y se configuran sus atributos. A continuación, vaya a la página Atributos para el control de acceso y

seleccione los atributos que desee utilizar en las políticas. Por último, navegue hasta la página Cuentas de AWS para crear o editar conjuntos de permisos para usar los atributos de ABAC.

### Elegir los atributos al utilizarlos AWS Managed Microsoft AD como fuente de identidad

Al configurar el Centro de Identidad de IAM AWS Managed Microsoft AD como fuente de identidad, primero se asigna un conjunto de atributos de Active Directory a los atributos de usuario del Centro de Identidad de IAM. A continuación, vaya a la página de atributos para el control de acceso. A continuación, elija los atributos que desee utilizar en la configuración de ABAC en característica del conjunto existente de atributos de SSO mapeados desde Active Directory. Por último, cree reglas de ABAC utilizando los atributos de control de acceso de los conjuntos de permisos para permitir que las identidades de los usuarios accedan a los recursos de AWS. Para obtener una lista de las asignaciones predeterminadas de los atributos de usuario del Centro de identidades de IAM a los atributos de usuario de su directorio, consulte. AWS Managed Microsoft AD [Asignaciones predeterminadas entre IAM Identity Center y Microsoft AD](#)

### Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad

Al configurar IAM Identity Center con un proveedor de identidades (IdP) externo como origen de identidad, hay 2 formas de utilizar los atributos de ABAC.

- Puede configurar su IdP para que envíe los atributos mediante aserciones de SAML. En este caso, IAM Identity Center transfiere el nombre y el valor del atributo desde el IdP para la evaluación de la política.

#### Note

Los atributos de las aserciones de SAML no estarán visibles en la página Atributos para el control de acceso. Deberá conocer estos atributos con antelación y añadirlos a las reglas de control de acceso al crear políticas. Si decide confiar en los atributos externos IdPs, estos atributos siempre se transferirán cuando los usuarios se federen en ellos. Cuentas de AWS En situaciones en las que los mismos atributos llegan a IAM Identity Center a través de SAML y SCIM, el valor de los atributos de SAML prevalece en las decisiones de control de acceso.

- Puede configurar los atributos que utilizará en la página Atributos para el control de acceso de la consola de IAM Identity Center. Los valores de atributos que elija aquí sustituyen a los valores de cualquier atributo coincidente que provenga de un IdP a través de una afirmación. Dependiendo de si utiliza o no SCIM, tenga en cuenta lo siguiente:

- Si utiliza SCIM, el IdP sincroniza automáticamente los valores de los atributos en IAM Identity Center. Es posible que los atributos adicionales necesarios para el control de acceso no estén presentes en la lista de atributos del SCIM. En ese caso, considere la posibilidad de colaborar con el administrador de TI de su IdP para enviar dichos atributos a IAM Identity Center mediante aserciones de SAML con el prefijo requerido `https://aws.amazon.com/SAML/Attributes/AccessControl:`. Para obtener información sobre cómo configurar los atributos de usuario para el control de acceso en su IdP para enviarlos mediante aserciones de SAML, consulte el [Tutoriales de orígenes de identidad de IAM Identity Center](#) de su IdP.
- Si no utiliza SCIM, debe añadir los usuarios manualmente y establecer sus atributos como si utilizara IAM Identity Center como origen de identidad. A continuación, vaya a la página Atributos para el control de acceso y seleccione los atributos que desee utilizar en las políticas.

Para obtener una lista completa de los atributos de usuario compatibles entre los atributos de usuario del Centro de Identidad de IAM y los atributos de usuario del externo IdPs, consulte. [Atributos de proveedores de identidad externos compatibles](#)

Para comenzar a utilizar ABAC en IAM Identity Center, consulte los temas siguientes.

#### Temas

- [Habilitación y configuración de atributos para el control de acceso](#)
- [Crear políticas de permisos para ABAC en IAM Identity Center](#)

## Habilitación y configuración de atributos para el control de acceso

Para utilizar el control de acceso basado en atributos (ABAC), primero debe habilitarlo en la página Configuración de la consola de IAM Identity Center o en la [API de IAM Identity Center](#). Independientemente de la fuente de identidad, siempre puede configurar los atributos de usuario desde el almacén de identidades para usarlos en ABAC. En la consola, puede hacerlo accediendo a la pestaña Atributos para el control de acceso de la página de configuración. Si utiliza un proveedor de identidades (IdP) externo como origen de identidades, también tiene la opción de recibir atributos del IdP externo en las aserciones SAML. En este caso, debe configurar el IdP externo para enviar los atributos deseados. Si un atributo de una afirmación de SAML también se define como atributo ABAC en IAM Identity Center, IAM Identity Center enviará el valor desde su almacén de identidades como etiqueta de sesión al iniciar [sesión](#) en una Cuenta de AWS.

 Note

No puede ver los atributos configurados y enviados por un IdP externo desde la página Atributos para el control de acceso de la consola de IAM Identity Center. Si transfiere atributos de control de acceso en las aserciones de SAML desde su IdP externo, esos atributos se envían directamente a la Cuenta de AWS cuando los usuarios se federan. Los atributos no estarán disponibles en IAM Identity Center para su mapeo.

## Temas

- [Activar atributos para el control de acceso](#)
- [Seleccione sus atributos para controlar el acceso](#)
- [Desactivar atributos para el control de acceso](#)

## Activar atributos para el control de acceso

Utilice el siguiente procedimiento para activar la característica de control de los atributos de acceso (ABAC) mediante la consola de IAM Identity Center.

 Note

Si ya tiene conjuntos de permisos y planea habilitar ABAC en su instancia de IAM Identity Center, las restricciones de seguridad adicionales requieren que primero tenga la política `iam:UpdateAssumeRolePolicy`. Estas restricciones de seguridad adicionales no son obligatorias si no ha creado ningún conjunto de permisos en su cuenta.

Si su instancia del Centro de Identidad de IAM se creó antes de diciembre de 2020 y planea habilitar ABAC en ella, debe tener la `iam:UpdateAssumeRolePolicy` política asociada a la función administrativa del Centro de Identidad de IAM, independientemente de si ha creado conjuntos de permisos en su cuenta.

## Cómo activar atributos para el control de acceso

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, busque el cuadro de información Atributos para el control de acceso y, a continuación, elija Activar. Continúe con el siguiente procedimiento para configurarlo.

## Seleccione sus atributos para controlar el acceso

Utilice el siguiente procedimiento para configurar atributos para la configuración de ABAC.

### Selección de los atributos mediante la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Atributos para el control de acceso, seleccione Agregar atributo e introduzca los detalles de Clave y Valor. Aquí es donde mapeará el atributo que proviene de su fuente de identidad a un atributo que IAM Identity Center pasa como etiqueta de sesión.

| Key ⓘ       | Value (optional) ⓘ                          | Remove |
|-------------|---------------------------------------------|--------|
| Department  | <code>\$(path:enterprise.department)</code> | ✕      |
| CostCenter  | <code>\$(path:enterprise.costCenter)</code> | ✕      |
| Add new key | Add new value                               |        |

La clave representa el nombre que se le da al atributo para su uso en las políticas. Puede ser cualquier nombre arbitrario, pero debe especificar ese nombre exacto en las políticas que cree para el control de acceso. Por ejemplo, supongamos que utiliza Okta (un IdP externo) como fuente de identidad y necesita transferir los datos del centro de costos de su organización como etiquetas de sesión. En Key, debe introducir un nombre que coincida de forma similar, CostCenter como su nombre de clave. Es importante tener en cuenta que, sea cual sea el nombre que elija aquí, también debe tener el mismo nombre en su [Clave de condición de aws:PrincipalTag](#) (es decir, "ec2:ResourceTag/CostCenter": "`$(aws:PrincipalTag/CostCenter)`").

#### Note

Use un atributo de un solo valor para su clave (por ejemplo, **Manager**). Por ejemplo, IAM Identity Center no admite atributos con varios valores para ABAC (por ejemplo, **Manager**, **IT Systems**).

El valor representa el contenido del atributo que proviene del origen de la identidad configurada. Aquí puede introducir cualquier valor de la tabla de fuentes de identidad correspondiente que aparece en [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos](#). Por ejemplo, utilizando el contexto proporcionado en el ejemplo mencionado anteriormente, revisaría la lista de atributos de IdP admitidos y determinaría que la coincidencia más cercana con un atributo compatible sería `${path:enterprise.costCenter}` y, a continuación, lo introduciría en el campo Valor. Consulta la captura de pantalla proporcionada arriba como referencia. Tenga en cuenta que no puede usar valores de atributos de IdP externos fuera de esta lista para ABAC a menos que utilice la opción de pasar los atributos a través de la aserción SAML.

5. Seleccione Save changes (Guardar cambios).

Ahora que ha configurado el mapeo de sus atributos de control de acceso, debe completar el proceso de configuración de ABAC. Para ello, cree sus reglas ABAC y agréguelas a sus conjuntos de permisos (políticas and/or basadas en recursos). Esto es necesario para poder conceder a las identidades de los usuarios el acceso a los recursos de AWS . Para obtener más información, consulte [Crear políticas de permisos para ABAC en IAM Identity Center](#).

#### Desactivar atributos para el control de acceso

Utilice el siguiente procedimiento para deshabilitar la característica ABAC y eliminar todas las asignaciones de atributos que se hayan configurado.

A fin de desactivar atributos para el control de acceso, siga estos pasos:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Administrar atributos para el control de acceso, seleccione Deshabilitar.
5. En el cuadro de diálogo Desactivar atributos para el control de acceso, revise la información y, cuando esté listo, escriba **DISABLE** y, a continuación, elija Confirmar.

**⚠ Important**

Este paso elimina todos los atributos y detiene el uso de los atributos para el control de acceso al federarse en Cuentas de AWS independientemente de si hay algún atributo en las aserciones de SAML de un proveedor de fuentes de identidad externo.

## Crear políticas de permisos para ABAC en IAM Identity Center

Puede crear políticas de permisos que determinen quién puede acceder a sus recursos de AWS en característica de los valores de atributos configurados. Cuando habilita ABAC y especifica atributos, IAM Identity Center transfiere los valores de atributo del usuario autenticado a IAM para utilizarlos en la evaluación de políticas.

Clave de condición de `aws:PrincipalTag`

Puede utilizar los atributos de control de acceso en sus conjuntos de permisos mediante la clave de condición `aws:PrincipalTag` para crear reglas de control de acceso. Por ejemplo, en la siguiente política, puede etiquetar todos los recursos de su organización con sus respectivos centros de costos. También puede utilizar un único conjunto de permisos que conceda a los desarrolladores acceso a los recursos de sus centros de costos. Ahora, cuando los desarrolladores se federan en la cuenta mediante el inicio de sesión único y su atributo de centro de costos, solo tienen acceso a los recursos de sus respectivos centros. A medida que el equipo vaya añadiendo más desarrolladores y recursos a su proyecto, solo tendrás que etiquetar los recursos con el centro de costos correcto. A continuación, se pasa la información del centro de costes en la AWS sesión cuando los desarrolladores se federan en ellos. Cuentas de AWS Por tanto, a medida que la organización agrega nuevos recursos y desarrolladores al centro de costos, los desarrolladores pueden administrar los recursos alineados con sus centros sin necesidad de actualizar los permisos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/
CostCenter}"
      }
    }
  }
]
}

```

Para obtener más información, consulte [aws:PrincipalTag](#) y [EC2: Iniciar o detener instancias en característica de las etiquetas principales y de recursos coincidentes](#) en la Guía del usuario de IAM.

Si las políticas contienen atributos no válidos en sus condiciones, la condición de la política fallará y se denegará el acceso. Para obtener más información, consulte [Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo](#).

## Entender los roles vinculados a servicios en IAM Identity Center

[Roles vinculados a servicios](#) son permisos predefinidos que permiten a IAM Identity Center delegar e implementar qué usuarios tienen acceso de inicio de sesión único a determinadas Cuentas de AWS de su organización en AWS Organizations. El servicio habilita esta funcionalidad al aprovisionar un rol vinculado al servicio en cada uno Cuenta de AWS de los miembros de su organización. Luego, el servicio permite que otros AWS servicios, como IAM Identity Center, aprovechen esas funciones para realizar tareas relacionadas con el servicio. Para obtener más información, consulte [AWS Organizations y los roles vinculados a servicios](#).

Al activar IAM Identity Center, este crea un rol vinculado al servicio en todas las cuentas de la organización en AWS Organizations. IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite



a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Para obtener más información, consulte [Configurar el acceso a Cuentas de AWS](#).

Las funciones vinculadas al servicio que se crean en cada una de ellas reciben un nombre. Cuenta de AWS `AWSServiceRoleForSSO` Para obtener más información, consulte [Uso de roles vinculados a servicios para IAM Identity Center](#).

#### Notas

- Si ha iniciado sesión en la cuenta de AWS Organizations administración, esta utilizará su función con la que ha iniciado sesión actualmente y no la función vinculada al servicio. De este modo se evita la escalada de privilegios.
- Cuando el IAM Identity Center realiza cualquier operación de IAM en la cuenta de AWS Organizations administración, todas las operaciones se realizan con las credenciales del director de IAM. Esto permite que los inicios de sesión CloudTrail proporcionen visibilidad de quién realizó todos los cambios de privilegios en la cuenta de administración.

# Configuración y uso del portal de AWS acceso

El portal de AWS acceso conecta a sus empleados con las aplicaciones en la nube a través del IAM Identity Center. Cuentas de AWS Los administradores configuran el portal y gestionan el acceso de los usuarios, mientras que los usuarios finales inician sesión una vez para acceder sin problemas a todos sus recursos autorizados.

El portal de AWS acceso proporciona acceso mediante inicio de sesión único a:

- Cuentas de AWS en su organización.
- AWS aplicaciones gestionadas como Amazon Quick y Kiro.
- Aplicaciones en la nube como Office 365, Concur, Salesforce y otras.

Cuando los usuarios inician sesión en el portal, encuentran las aplicaciones a Cuentas de AWS las que están autorizados a acceder sin necesidad de iniciar sesión adicional.

## Cómo empezar a utilizar el portal de AWS acceso

Para los administradores:

Necesita acceso administrativo a la instancia de su [organización o a la instancia](#) de [cuenta](#) de IAM Identity Center para configurar el portal de AWS acceso y administrar el acceso de los usuarios.

1. Si lo desea, personalice la URL del portal de AWS acceso.
2. Asigne el acceso de los usuarios a las aplicaciones Cuentas de AWS y las aplicaciones. AWS Los recursos asignados se muestran en el portal.

Para los usuarios finales:

El administrador debe haber completado la configuración del portal de AWS acceso y haberte proporcionado la URL del portal y las credenciales de inicio de sesión.

1. Obtenga la URL del portal de su administrador (normalmente `https://your-company.awsapps.com/start`).
2. Inicie sesión con las credenciales provistas por el administrador.
3. Acceda a los recursos de su portal.

# Configure el portal de AWS acceso

Como administrador, puede personalizar el portal de AWS acceso para que se adapte a las necesidades de su organización y garantizar que los usuarios puedan acceder fácilmente a sus recursos autorizados.

## Qué puede configurar

AWS activación del portal de acceso: configure el acceso inicial de los usuarios al portal de AWS acceso, incluida la activación de las credenciales de usuario y los procesos de inicio de sesión por primera vez.

URL del portal de AWS acceso personalizado (opcional): personalice la URL del portal de AWS acceso de su organización desde el formato predeterminado (`d-xxxxxxxxxx.awsapps.com/start`) a un subdominio más reconocible (`your-company.awsapps.com/start`).

### Antes de empezar

Asegúrese de tener acceso administrativo a IAM Identity Center, compruebe que IAM Identity Center esté configurado como una [instancia de organización](#) o una [instancia de cuenta](#) y planifique su nombre de subdominio personalizado (se trata de una configuración única que no se puede cambiar más adelante).

Una vez configurado, los usuarios pueden acceder al portal de AWS acceso mediante la URL personalizada y seguir el proceso de activación que haya establecido para su organización.

### Temas

- [Activar el portal de AWS acceso para los usuarios primerizos del IAM Identity Center](#)
- [Personalización de la URL del portal de AWS acceso](#)
- [Confirme que los usuarios puedan iniciar sesión en el portal de AWS acceso](#)

## Activar el portal de AWS acceso para los usuarios primerizos del IAM Identity Center

Si es la primera vez que intenta iniciar sesión en el portal de AWS acceso, consulte su correo electrónico para obtener instrucciones sobre cómo activar sus credenciales de usuario.

## Para activar las credenciales de usuario

1. En función del correo electrónico que haya recibido de su empresa, elija uno de los siguientes métodos para activar sus credenciales de usuario y poder empezar a utilizar el portal de AWS acceso.
  - a. Si ha recibido un correo electrónico con el asunto Invitación a unirse a AWS IAM Identity Center, ábralo y seleccione Aceptar invitación. En la página de Registro de usuarios nuevos, introduzca y confirme una contraseña y, a continuación, seleccione Establecer nueva contraseña. Deberá utilizar esa contraseña cada vez que inicie sesión en el portal.
  - b. Si fue el equipo de asistencia de TI o el administrador de TI de la empresa el que le envió el correo electrónico, siga las instrucciones proporcionadas para activar sus credenciales de usuario.
2. Después de activar sus credenciales de usuario proporcionando una nueva contraseña, el portal de AWS acceso iniciará sesión automáticamente. Si esto no ocurre, puede iniciar sesión manualmente en el portal de acceso de AWS usando las instrucciones que se indican en [Iniciar sesión en el portal de AWS acceso](#).

## Personalización de la URL del portal de AWS acceso

De forma predeterminada, puede acceder al portal de AWS acceso mediante una URL que siga este formato: `d-xxxxxxxxxx.awsapps.com/start`. Puede personalizar el complemento del modo siguiente: `your_subdomain.awsapps.com/start`.

### Important

Si cambia la URL del portal de AWS acceso, no podrá editarla más adelante.

### Cómo personalizar la URL

1. Abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En la consola de IAM Identity Center, elija Panel en el panel de navegación y localice la sección Resumen de configuración.
3. Pulse el botón Personalizar situado debajo de la URL del portal de AWS acceso.

 Note

Si el botón Personalizar no aparece, significa que el portal de acceso AWS ya se ha personalizado. La personalización de la URL del portal de AWS acceso es una operación que se realiza una sola vez y no se puede revertir.

4. Introduzca el nombre de subdominio que desee y pulse Guardar.

Ahora puede iniciar sesión en la AWS consola a través de su portal de AWS acceso con su URL personalizada.

## Confirme que los usuarios puedan iniciar sesión en el portal de AWS acceso

Los siguientes pasos son para que el administrador del Centro de Identidad de IAM confirme que el usuario del Centro de Identidad de IAM puede iniciar sesión en el portal de AWS acceso y acceder al. Cuenta de AWS

Inicie sesión en el portal de acceso AWS

1. Realice una de estas 2 operaciones para iniciar sesión en la Consola de administración de AWS.
  - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione el usuario root e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM y selecciona un rol de administrador.
2. Abra la [consola de IAM Identity Center](#)
3. En el panel de navegación, elija Panel.
4. En la página del panel de control, en el resumen de la configuración, selecciona la URL del portal de AWS acceso.
5. Inicie sesión mediante cualquiera de las siguientes opciones:
  - Si utiliza Active Directory o un proveedor de identidades (IdP) externo como origen de identidad, inicie sesión con las credenciales del usuario de Active Directory o IdP.

- Si utiliza el directorio predeterminado de Identity Center como origen de identidad, inicie sesión con el nombre de usuario que especificó al crear el usuario y la nueva contraseña que especificó para el usuario.
6. En la pestaña Cuentas, localiza la tuya Cuenta de AWS y amplíala.
  7. Se mostrarán los roles que tiene disponibles. Por ejemplo, si se le asignan tanto el conjunto de AdministratorAccesspermisos como el conjunto de permisos de facturación, esas funciones se muestran en el portal de AWS acceso. Seleccione el nombre del rol de IAM que desee usar para la sesión.
  8. Si se le redirige a la consola AWS de administración, habrá terminado correctamente de configurar el acceso a Cuenta de AWS.

 Note

Si no ve Cuentas de AWS en la lista, es probable que aún no se le haya asignado al usuario un conjunto de permisos para esa cuenta. Para obtener instrucciones sobre cómo asignar usuarios a un conjunto de permisos, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

Ahora que ha confirmado que puede iniciar sesión con las credenciales del Centro de Identidad de IAM, cambie al navegador que utilizó para iniciar sesión Consola de administración de AWS y cierre la sesión con sus credenciales de usuario raíz o de usuario de IAM.

 Important

Le recomendamos encarecidamente que utilice las credenciales del usuario administrativo del Centro de Identidad de IAM al iniciar sesión en el portal de AWS acceso para realizar tareas administrativas en lugar de utilizar las credenciales del usuario raíz o del usuario de IAM. Proteja las credenciales del Usuario raíz y utilícelas solo para las tareas que solo el Usuario raíz pueda realizar. Para permitir que otros usuarios accedan a sus cuentas y aplicaciones, y para administrar IAM Identity Center, cree y asigne conjuntos de permisos únicamente a través de IAM Identity Center.

# Utilice el portal de acceso AWS

Puede iniciar varias aplicaciones seleccionando la pestaña de aplicaciones Cuenta de AWS o aplicaciones en el portal. La presencia de iconos de aplicaciones en su portal de AWS acceso significa que un administrador de su empresa le ha concedido el acceso a esas aplicaciones Cuentas de AWS o aplicaciones. También significa que puede acceder a todas estas cuentas o aplicaciones desde el portal de AWS acceso sin tener que solicitar más datos de inicio de sesión.

## Cómo utilizar el portal de acceso AWS

Para usar el portal de AWS acceso:

1. Obtenga la URL del portal de su administrador (normalmente tiene el siguiente aspecto `https://your-company.awsapps.com/start`).
2. Inicie sesión con las credenciales provistas por el administrador.
3. Elija las cuentas y aplicaciones del portal a las que desee acceder.

El administrador controla lo que ve en el portal en función de su rol y sus permisos. Póngase en contacto con su administrador o con el servicio de asistencia para solicitar acceso adicional en las siguientes situaciones:

- No ve ninguna aplicación Cuenta de AWS o aplicación a la que necesite acceder.
- Si el acceso que tiene a una cuenta o aplicación determinada no es el previsto.

### Temas

- [Iniciar sesión en el portal de AWS acceso](#)
- [Restablecer la contraseña de usuario del portal de AWS acceso](#)
- [Obtener las credenciales de usuario del IAM Identity Center para o AWS CLI AWS SDKs](#)
- [Crear enlaces de acceso directo a Consola de administración de AWS destinos](#)
- [Registro de un dispositivo para MFA](#)
- [Visualización y finalización de la sesión activa](#)

## Iniciar sesión en el portal de AWS acceso

El portal de AWS acceso proporciona a los usuarios del IAM Identity Center un acceso de inicio de sesión único a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas a través de un portal web. A continuación, se describe cómo iniciar sesión en el portal de AWS acceso, consejos para iniciar sesión y cómo cerrar sesión en el AWS portal de acceso.

### Requisitos previos

El centro de identidad de IAM debe estar habilitado para usar el portal de AWS acceso. Para obtener más información, consulte [Activar IAM Identity Center](#).

#### Note

Después de iniciar sesión, la duración predeterminada de la sesión del portal de AWS acceso es de 8 horas. Tenga en cuenta que un administrador puede [cambiar la duración](#) de esta sesión.

## Inicie sesión en el portal de AWS acceso

Para iniciar sesión en el portal de AWS acceso

1. En la ventana del navegador, pegue la URL de inicio de sesión que se le proporcionó y elija Intro. La URL se ve así `d-xxxxxxxxx.awsapps.com/start` o `your_subdomain.awsapps.com/start`. Le recomendamos que guarde este enlace al portal como marcador para que pueda acceder al mismo más rápidamente en futuras ocasiones.
2. Inicie sesión con las credenciales de inicio de sesión estándar de la empresa.

#### Note

Si el administrador le envió una contraseña de un solo uso (OTP) por correo electrónico y es la primera vez que inicia sesión, escriba esa contraseña. Una vez que haya iniciado sesión, debe crear una contraseña nueva para poder acceder en el futuro.

Si se le solicita un código de verificación, compruebe su correo electrónico y, a continuación, copie y pegue el código en la página de inicio de sesión.



 Note

Los códigos de verificación suelen enviarse por correo electrónico, pero el método de entrega puede variar. Consulte con su administrador para obtener más información.

3. Una vez que haya iniciado sesión, podrá acceder Cuenta de AWS a cualquier aplicación que aparezca en el portal.

## Dispositivos de confianza

Después de seleccionar la opción Este es un dispositivo de confianza en la página de inicio de sesión, IAM Identity Center considerará que todos los inicios de sesión futuros desde ese dispositivo están autorizados. Esto significa que IAM Identity Center no ofrecerá la opción de introducir un código MFA mientras utilice ese dispositivo de confianza. Sin embargo, hay algunas excepciones, como iniciar sesión desde un navegador nuevo o cuando el dispositivo recibe una dirección IP desconocida.

## Consejos para iniciar sesión en el portal de AWS acceso

Estos son algunos consejos que le ayudarán a administrar su experiencia con el portal de AWS acceso.

- De vez en cuando, puede que tenga que cerrar sesión y volver a iniciarla en el portal de AWS acceso. Esto puede ser necesario para poder acceder a las nuevas aplicaciones que el administrador le haya asignado recientemente. Sin embargo, no será necesario, ya que todas las nuevas aplicaciones se actualizan cada hora.
- Al iniciar sesión en el portal de AWS acceso, puede abrir cualquiera de las aplicaciones que aparecen en el portal seleccionando el icono de la aplicación. Cuando haya terminado de usar la aplicación, puede cerrarla o cerrar sesión en el portal de AWS acceso. Al cerrar la aplicación solo finaliza la sesión de la aplicación en cuestión. Todas las demás aplicaciones que haya abierto desde el portal de AWS acceso permanecerán abiertas y en ejecución.
- Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS . El cierre de sesión del portal elimina por completo sus credenciales de la sesión del navegador.
- Una vez que inicie sesión en el portal de AWS acceso, podrá cambiar a un rol. Esto anula temporalmente los permisos de usuario originales y, en su lugar, le otorga los permisos asignados al rol. Para obtener más información, consulte [Cambiar a un rol \(consola\)](#).

## Cerrar sesión en el portal de AWS acceso

Al cerrar sesión del portal, se eliminan por completo sus credenciales de la sesión del navegador. Para obtener más información, [consulte Cerrar sesión en el portal de AWS acceso](#) en la AWS Sign-In guía.

Para cerrar sesión en el portal de AWS acceso

- En el portal de AWS acceso, seleccione Cerrar sesión en la barra de navegación.

### Note

Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS .

## Restablecer la contraseña de usuario del portal de AWS acceso

El portal de AWS acceso proporciona a los usuarios [del IAM Identity Center](#) un acceso de inicio de sesión único a todas sus AWS cuentas asignadas y aplicaciones en la nube a través de un portal web. El portal de AWS acceso es diferente del [Consola de administración de AWS](#), que es un conjunto de consolas de servicio para gestionar los recursos. AWS

Utilice este procedimiento para restablecer la contraseña de usuario del IAM Identity Center para el portal de AWS acceso. Más información sobre los [tipos de usuario](#) en la Guía del usuario de AWS Sign-In .

### Consideraciones

La función de restablecimiento de la contraseña para el portal de AWS acceso solo está disponible para los usuarios de las instancias del Centro de Identidad que utilizan el directorio de Identity Center o [AWS Managed Microsoft AD](#) como fuente de identidad. Si el usuario está conectado a un proveedor de identidad externo o a [AD Connector](#), el restablecimiento de la contraseña del usuario debe realizarse desde el proveedor de identidad externo o estar conectado a Active Directory.

- Si su fuente de identidad es un directorio del IAM Identity Center, consulte [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#).
- Si su fuente de identidad es una AWS Managed Microsoft AD, consulte [Requisitos de contraseña al restablecer una contraseña en AWS Managed Microsoft AD](#).

## Para restablecer la contraseña del portal de AWS acceso

1. Abra un navegador web y vaya a la página de inicio de sesión de su portal de AWS acceso.

Si no tiene la URL del portal de AWS acceso, compruebe su correo electrónico. Deberías haber recibido por correo electrónico una invitación para unirse al Centro de Identidad de AWS IAM que incluya una URL de inicio de sesión específica en el AWS portal de acceso. Como alternativa, es posible que su administrador le haya proporcionado directamente una contraseña de un solo uso y la URL del portal de AWS acceso. Si no encuentra esta información, pida al administrador que se la envíe.

Para obtener más información sobre cómo iniciar sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

2. Escriba su nombre y, a continuación, elija Siguiente.
3. En Contraseña, seleccione He olvidado la contraseña.

Verifique su nombre de usuario y escriba los caracteres de la imagen para confirmar que no es un robot. A continuación, elija Siguiente. Es posible que tenga que deshabilitar el software bloqueador de anuncios si no puede introducir caracteres.

4. Aparecerá un mensaje para confirmar que se envió un correo electrónico para restablecer la contraseña. Elija Continuar.
5. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña. En el correo electrónico, seleccione Restablecer contraseña.
6. En la página Restablecer la contraseña, compruebe su nombre de usuario, especifique una nueva contraseña para el portal de AWS acceso y, a continuación, seleccione Establecer nueva contraseña.
7. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña.

### Note

Un administrador puede restablecer su contraseña enviándole un correo electrónico con instrucciones para restablecerla o generando una contraseña de un solo uso y compartiéndola con usted. Si es un administrador, consulte [Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final](#).

# Obtener las credenciales de usuario del IAM Identity Center para o AWS CLI AWS SDKs

Puede acceder a AWS los servicios mediante programación mediante los kits de desarrollo de software ( ) AWS Command Line Interface o los kits de desarrollo de AWS software (SDKs) con las credenciales de usuario del IAM Identity Center. En este tema se describe cómo obtener credenciales temporales para un usuario en IAM Identity Center.

El portal de AWS acceso proporciona a los usuarios del Centro de Identidad de IAM un acceso único a sus aplicaciones y a las de la nube. Cuentas de AWS Tras iniciar sesión en el portal de AWS acceso como usuario del IAM Identity Center, podrá obtener credenciales temporales. A continuación, puede utilizar las credenciales, también denominadas credenciales de usuario del Centro de Identidad de IAM, en AWS CLI o AWS SDKs para acceder a los recursos de un. Cuenta de AWS

Si las utiliza AWS CLI para acceder a los AWS servicios mediante programación, puede utilizar los procedimientos de este tema para iniciar el acceso a. AWS CLI Para obtener información sobre el AWS CLI, consulte la Guía del [AWS Command Line Interface usuario](#).

Si lo utiliza AWS SDKs para acceder a los AWS servicios mediante programación, al seguir los procedimientos de este tema también se establece directamente la autenticación del. AWS SDKs Para obtener información acerca de AWS SDKs, consulte la Guía de [referencia de herramientas AWS SDKs y herramientas](#).

## Note

Los usuarios de IAM Identity Center son diferentes a los [usuarios de IAM](#). Los usuarios de IAM reciben credenciales a largo plazo para acceder a AWS los recursos. Los usuarios de IAM Identity Center reciben credenciales temporales. Le recomendamos que utilice credenciales temporales como práctica recomendada de seguridad para acceder a sus cuentas, Cuentas de AWS ya que estas credenciales se generan cada vez que inicia sesión.

## Requisitos previos

Para obtener credenciales temporales para su usuario de IAM Identity Center, necesitará lo siguiente:

- Un usuario de IAM Identity Center: iniciará sesión en el portal de acceso AWS como este usuario. Usted o su administrador pueden crearlo. Para obtener información sobre cómo activar IAM Identity Center y crear un usuario de IAM Identity Center, consulte [Introducción al IAM Identity Center](#).
- Acceso de usuario a un Cuenta de AWS: para conceder permiso a un usuario del Centro de Identidad de IAM para recuperar sus credenciales temporales, usted o un administrador deben asignar al usuario del Centro de Identidad de IAM un conjunto de [permisos](#). Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos de una Cuenta de AWS. Si su administrador creó el usuario de IAM Identity Center por usted, pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).
- AWS CLI instalado: para utilizar las credenciales temporales, debe instalar el. AWS CLI Para obtener instrucciones de instalación, consulte [Instalar o actualizar la última versión de la AWS CLI](#) en la Guía del usuario de AWS CLI .

## Consideraciones

Antes de completar los pasos para obtener credenciales temporales para el usuario de IAM Identity Center, tenga en cuenta los siguientes aspectos:

- IAM Identity Center crea roles de IAM: cuando se asigna a un usuario de IAM Identity Center un conjunto de permisos, IAM Identity Center crea un rol de IAM correspondiente a partir del conjunto de permisos. Las funciones de IAM creadas mediante conjuntos de permisos se diferencian de las funciones de IAM creadas AWS Identity and Access Management en los siguientes aspectos:
  - IAM Identity Center posee y protege los roles creados por los conjuntos de permisos. Solo IAM Identity Center puede modificar estos roles.
  - Solo los usuarios de IAM Identity Center pueden asumir los roles que corresponden a sus conjuntos de permisos asignados. No puede asignar el acceso a los conjuntos de permisos a los usuarios de IAM, a los usuarios federados de IAM ni a las cuentas de servicio.
  - No puede modificar una política de confianza de roles en estos roles para permitir el acceso a [entidades principales](#) fuera de IAM Identity Center.

Para obtener información sobre cómo obtener credenciales temporales para un rol que cree en IAM, consulte [Uso de credenciales de seguridad temporales con la AWS CLI](#) en la Guía del usuario de AWS Identity and Access Management .

- Puede configurar la duración de la sesión para los conjuntos de permisos: tras iniciar sesión en el portal de AWS acceso, el conjunto de permisos al que está asignado su usuario del Centro de Identidad de IAM aparece como función disponible. IAM Identity Center crea una sesión independiente para este rol. Esta sesión puede durar de una a 12 horas según la duración de la sesión configurada para el conjunto de permisos. De forma predeterminada, la sesión durará 1 hora. Para obtener más información, consulte [Establezca la duración de la sesión para Cuentas de AWS](#).

## Obtención y actualización de credenciales temporales

Puede obtener y actualizar credenciales temporales de su usuario de IAM Identity Center de forma automática o manual.

### Temas

- [Actualización automática de credenciales \(recomendada\)](#)
- [Actualización manual de credenciales](#)

### Actualización automática de credenciales (recomendada)

La actualización automática de credenciales utiliza el estándar de autorización de código de dispositivo Open ID Connect (OIDC)). Con este método, se inicia el acceso directamente mediante el comando `aws configure sso` en la AWS CLI. Puede usar este comando para acceder automáticamente a cualquier rol que esté asociado a cualquier conjunto de permisos al que esté asignado para cualquier Cuenta de AWS.

Para acceder al rol creado para su usuario del IAM Identity Center, ejecute el `aws configure sso` comando y, a continuación, autorícelo AWS CLI desde una ventana del navegador. Mientras tenga una sesión activa en el portal de AWS acceso, AWS CLI recuperará automáticamente las credenciales temporales y las actualizará automáticamente.

Para obtener más información, consulte [Configurar el perfil con el `aws configure sso wizard`](#) en la Guía del usuario AWS Command Line Interface .

Cómo obtener credenciales temporales que se actualicen automáticamente:

1. Inicie sesión en el portal de AWS acceso mediante la URL de inicio de sesión específica proporcionada por su administrador. Si creó el usuario del Centro de identidad de IAM, AWS envíe una invitación por correo electrónico que incluya su URL de inicio de sesión. Para obtener

más información, consulte [Iniciar sesión en el portal de AWS acceso en la Guía del](#) usuario de AWS inicio de sesión.

2. En la pestaña Cuentas, localice la página Cuenta de AWS de la que desea recuperar las credenciales. Al seleccionar la cuenta, aparecerán el nombre y el ID de la cuenta y la dirección de correo electrónico asociados a la cuenta.

 Note

Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado a un conjunto de permisos para esa cuenta. En este caso, póngase en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

3. Debajo del nombre de la cuenta, los permisos al que está asignado el usuario de IAM Identity Center aparecen como un rol disponible. Por ejemplo, si a su usuario del Centro de Identidad de IAM se le asigna el conjunto de PowerUserAccesspermisos de la cuenta, el rol aparecerá en el portal de AWS acceso como PowerUserAccess.
4. Según la opción que elija junto al nombre del rol, elija Claves de acceso o Línea de comandos o acceso mediante programación.
5. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado el AWS CLI.
6. En Credenciales de IAM Identity Center de AWS (recomendadas), se muestran sus credenciales de SSO Start URL y SSO Region. Estos valores son necesarios para configurar un perfil habilitado para IAM Identity Center y sso-session para la AWS CLI Para completar esta configuración, siga las instrucciones de [Configurar el perfil con el aws configure sso wizard](#) en la Guía del usuario de AWS Command Line Interface .

Siga utilizándolas AWS CLI según sea necesario Cuenta de AWS hasta que las credenciales hayan caducado.

## Actualización manual de credenciales

Puede usar el método de actualización manual de credenciales para obtener credenciales temporales para un rol que esté asociado a un conjunto de permisos específico en una Cuenta de AWS específica. Para ello, debe copiar y pegar los comandos necesarios para las credenciales temporales. Con este método, debe actualizar las credenciales temporales manualmente.

Puede ejecutar AWS CLI comandos hasta que caduquen sus credenciales temporales.

### Cómo obtener credenciales que se actualizan manualmente

1. Inicie sesión en el portal de AWS acceso mediante la URL de inicio de sesión específica proporcionada por su administrador. Si creó el usuario del Centro de identidad de IAM, AWS envíe una invitación por correo electrónico que incluya su URL de inicio de sesión. Para obtener más información, consulte [Iniciar sesión en el portal de AWS acceso en la Guía del](#) usuario de AWS inicio de sesión.
2. En la pestaña Cuentas, busque la Cuenta de AWS de la que desea recuperar las credenciales de acceso y amplíela para que muestre el nombre del rol de IAM (por ejemplo, Administrador). Según la opción que elija junto al nombre del rol de IAM, elija Claves de acceso o Línea de comandos o acceso mediante programación.

#### Note

Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado a un conjunto de permisos para esa cuenta. En este caso, póngase en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

3. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado el AWS CLI.
4. Elija una de las siguientes opciones:

- Opción 1: Definir variables de AWS entorno

Elija esta opción para anular toda la configuración de credenciales, incluida la configuración de los archivos `credentials` y `config`. Para obtener más información, consulte [Variables de entorno para configurar la AWS CLI](#) en la Guía del usuario de AWS CLI .

Para usar esta opción, copie los comandos en el portapapeles, péguelos en la ventana del AWS CLI terminal y, a continuación, presione Entrar para configurar las variables de entorno necesarias.

- Opción 2: añada un perfil al archivo de AWS credenciales

Elija esta opción para ejecutar comandos con diferentes conjuntos de credenciales.



Para usar esta opción, copie los comandos en el portapapeles y, a continuación, péguelos en el `AWS credentials` archivo compartido para configurar un nuevo perfil con nombre. Para obtener más información, consulte los [archivos de configuración y credenciales compartidos](#) en la Guía de referencia de herramientas AWS SDKs y herramientas. Para usar esta credencial, especifique la `--profile` opción en su AWS CLI comando. Esto afecta a todos los símbolos del sistema que utilicen el mismo archivo de credenciales.

- Opción 3: utilice valores individuales en su AWS cliente de servicio

Elija esta opción para acceder a AWS los recursos de un cliente AWS de servicio. Para obtener más información, consulte [Herramientas para crear en AWS](#).

Para usar esta opción, copie los valores en el portapapeles, péguelos en el código y asígnelos a las variables adecuadas para su SDK. Para obtener más información, consulte la documentación específica de su específico SDK API.

## Crear enlaces de acceso directo a Consola de administración de AWS destinos

Los enlaces de acceso directo creados en el portal de AWS acceso llevan a los usuarios del Centro de Identidad de IAM a un destino específico en el Consola de administración de AWS, con un conjunto de permisos específico y en un lugar específico. Cuenta de AWS

Los enlaces de acceso directo le ahorran tiempo a usted y a sus colaboradores. En lugar de navegar hasta la URL de destino deseada en Consola de administración de AWS (por ejemplo, una página de instancia de bucket de Amazon S3) a través de varias páginas, incluido el portal de AWS acceso, puede utilizar un enlace de acceso directo para llegar al mismo destino automáticamente.

### Opciones de destino del enlace de acceso directo

Los enlaces de acceso directo tienen tres opciones de destino, que se enumeran aquí por prioridad:

- (Opcional) Cualquier URL de destino Consola de administración de AWS especificada en el enlace de acceso directo. Por ejemplo, la página de instancias de bucket de Amazon S3.
- (Opcional) URL de estado de retransmisión configurada por el administrador para el conjunto de permisos en cuestión. Para obtener más información sobre el estado de retransmisión, consulte [Configure el estado de la retransmisión para acceder rápidamente a Consola de administración de AWS](#).

- Consola de administración de AWS casa. El destino por defecto si no especifica ninguna.

 Note

La navegación automática a un destino solo se realiza correctamente si se ha autenticado en el Centro de Identidad de IAM y se ha asignado el conjunto de permisos necesario para la AWS cuenta y la URL de destino.

El portal de AWS acceso incluye un botón Crear acceso directo que le ayuda a crear un enlace de acceso directo que se pueda compartir. Si tiene pensado especificar una URL de destino (la primera opción de la lista anterior), puede copiar la URL en un portapapeles para compartirla.

## Cree un enlace de acceso directo en el portal de AWS acceso

1. Con la sesión iniciada en el portal de AWS acceso, seleccione la pestaña Cuentas y, a continuación, pulse el botón Crear acceso directo.
2. En el cuadro de diálogo:
  - a. Elija una Cuenta de AWS utilizando el ID de la cuenta o el nombre de la cuenta. A medida que escribe, un menú desplegable muestra la cuenta IDs y los nombres coincidentes a los que puedes acceder. Puede elegir solo una cuenta a la que tenga acceso.
  - b. Si lo desea, elija un rol de IAM de la lista desplegable. Estos son los conjuntos de permisos que se le han asignado para la cuenta seleccionada. Si omite la elección del rol, se le pide a los usuarios que seleccionen uno que se les haya asignado para la cuenta elegida al utilizar el enlace de acceso directo.

 Note

No puede conceder nuevos accesos con los enlaces de acceso directo. Los enlaces de acceso directo solo funcionan con los conjuntos de permisos ya asignados al usuario. Si el usuario no tiene asignados los conjuntos de permisos necesarios para la cuenta y la URL de destino, se le deniega el acceso.

- c. Si lo desea, introduzca la URL de destino del portal de AWS acceso. Si omite introducir una URL, el destino se determina de forma automática al utilizar el enlace de acceso

directo, en función de las opciones de destino del enlace de acceso directo mencionadas anteriormente.

- d. El enlace abreviado se generará en la parte inferior del cuadro de diálogo, en función de lo que introduzca. Pulse el botón Copiar URL. Ahora puede crear un marcador con el enlace de acceso directo copiado o compartirlo con sus colaboradores que tengan acceso a la misma cuenta con el mismo conjunto de permisos o con otro conjunto de permisos suficiente.

## Construir enlaces de Consola de administración de AWS acceso directo seguros con codificación URL

Todos los valores de los parámetros de la URL, incluidos el ID de cuenta, el nombre del conjunto de permisos y la URL de destino, deben estar codificados en URL.

Los enlaces de AWS acceso directo amplían la URL del portal de acceso con la siguiente ruta:

/#/console?

account\_id=[*account\_ID*]&role\_name=[*permission\_set\_name*]&destination=[*destination*]

La URL completa de la AWS partición clásica sigue este patrón:

IPv4 punto final:

https://[*your\_subdomain*].awsapps.com/start/#/console?

account\_id=[*account\_ID*]&role\_name=[*permission\_set\_name*]&destination=[*destination*]

Punto final de doble pila

https://[*identity\_center\_instance\_id*].portal.[*region*].app.aws/#/console?

account\_id=[*account\_ID*]&role\_name=[*permission\_set\_name*]&destination=[*destination*]

Este es un ejemplo de enlace de acceso directo que permite a un usuario acceder a una cuenta 123456789012 con el conjunto de permisos de S3FullAccess y acceder a la página de inicio de la consola S3:

- IPv4 punto final: `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Punto final de doble pila: `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?`

account\_id=123456789012&role\_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome

- (AWS GovCloud (US) Region) IPv4 punto final: `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) Punto final de doble pila: `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

## Registro de un dispositivo para MFA

Los usuarios del directorio de Identity Center deben usar el siguiente procedimiento en el portal de acceso de AWS para registrar el nuevo dispositivo para la autenticación multifactor (MFA).

### Important

Actualmente, los [proveedores de identidad externos](#) no admiten la MFA en IAM Identity Center.

## Antes de empezar

Le recomendamos que primero descargue la aplicación de autenticación adecuada en su dispositivo antes de iniciar los pasos de este procedimiento. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#).

## Registro de su dispositivo

### Cómo registrar el dispositivo para su uso con MFA

1. Inicie sesión en su portal de AWS acceso. Para obtener más información, consulte [Iniciar sesión en el portal de AWS acceso](#).
2. Cerca de la parte superior derecha de la página, seleccione dispositivos MFA.
3. En la página Dispositivos de autenticación multifactor (MFA), seleccione Registrar dispositivo.

 Note

Si la opción Registrar dispositivo MFA aparece atenuada, póngase en contacto con el administrador para que le ayude a registrar el dispositivo.

4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:

- Aplicación de autenticación

1. En la página Configurar la aplicación de autenticación, IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
2. Con el dispositivo de MFA físico, haga lo siguiente:
  - a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#). Si la aplicación de MFA admite varias cuentas (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo de MFA).
  - b. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación.
    - i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
    - ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

 Important

Cuando configure un dispositivo MFA para que funcione con IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudarle si pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de

estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA.

3. En la página Configurar la aplicación de Authenticator, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

 Important

Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente a su usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Asignar MFA. El dispositivo MFA ahora puede empezar a generar contraseñas de un solo uso y ya está listo para usarse con ellas. AWS

- Llave de seguridad o autenticador integrado

1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

 Note

La experiencia varía según el navegador o la plataforma. Una vez que el dispositivo se haya registrado correctamente, podrá asociar un nombre descriptivo al dispositivo recién inscrito. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar.

## Visualización y finalización de la sesión activa

Puede usar su portal de AWS acceso para ver la lista de sus sesiones activas y, si es necesario, finalizar una o más sesiones.

Finalice su sesión activa mediante su portal de AWS acceso

1. Inicie sesión en su portal de AWS acceso. Para obtener más información, consulte [Iniciar sesión en el portal de AWS acceso](#).

2. Cerca de la parte superior derecha de la página, seleccione Seguridad.
3. En la página Seguridad, el número entre paréntesis junto a Sesiones activas indica cuántas sesiones activas tiene. Seleccione la casilla de verificación situada junto a cada sesión que desea finalizar y, a continuación, seleccione Finalizar sesiones.

 Tip

Para la sesión en segundo plano del usuario, puede buscar sesiones por el nombre de recurso de Amazon (ARN) del trabajo que utiliza la sesión. En la lista Tipo de sesión, seleccione Sesiones de usuario en segundo plano y, a continuación, introduzca el ARN del trabajo en el cuadro de búsqueda.

Solo puede finalizar las sesiones activas que estén cargadas. Si tiene muchas sesiones, seleccione Cargar más sesiones activas para ver las sesiones adicionales.

4. Seleccione la casilla de verificación situada junto a cada sesión que desea finalizar y, a continuación, seleccione Finalizar sesiones.
5. Aparecerá un cuadro de diálogo que confirma que está finalizando las sesiones activas. Revise la información y, si desea continuar, escriba `confirm` y, luego, seleccione Finalizar sesiones.
6. Volverá a su lista de sesiones activas. Aparecerá una barra de notificación verde para indicar que las sesiones seleccionadas se eliminaron correctamente.

# Uso del centro de identidad de IAM en varios Regiones de AWS

En este tema se explica cómo usarlo AWS IAM Identity Center en varios Regiones de AWS. Descubra cómo replicar su instancia en otras regiones, gestionar el acceso y las sesiones del personal, implementar aplicaciones y mantener el acceso a las cuentas durante las interrupciones del servicio.

Cuando habilita una instancia organizativa del IAM Identity Center, elige una única Región de AWS (región principal). Puede replicar esta instancia en una instancia adicional Regiones de AWS si cumple con ciertos requisitos previos. IAM Identity Center replica automáticamente las identidades de los empleados, los conjuntos de permisos, las asignaciones de usuarios y grupos, las sesiones y otros metadatos de la región principal a las regiones adicionales elegidas.

## Ventajas del soporte multirregional

La replicación de IAM Identity Center a una versión adicional Regiones de AWS ofrece dos ventajas clave:

- Flexibilidad de Cuenta de AWS acceso mejorada: sus empleados pueden acceder al suyo incluso si la instancia del IAM Identity Center sufre una interrupción del servicio en su Cuenta de AWS región principal. Esto se aplica al acceso con los permisos proporcionados antes de la interrupción.
- Mayor flexibilidad a la hora de elegir las regiones de implementación para las aplicaciones AWS administradas: puede implementar aplicaciones AWS administradas en las regiones que prefiera para cumplir con los requisitos de residencia de los datos de las aplicaciones y mejorar el rendimiento gracias a la proximidad a los usuarios. Las aplicaciones implementadas en otras regiones acceden a las identidades replicadas de la fuerza laboral a nivel local para lograr un rendimiento y una confiabilidad óptimos.

## Requisitos y consideraciones previos

Antes de replicar su instancia de IAM Identity Center, asegúrese de que se cumplen los siguientes requisitos:

- Tipo de instancia: su instancia del IAM Identity Center debe ser una instancia de [organización](#). El soporte multirregional no está disponible en las instancias de [cuentas](#).



- Fuente de identidad: la instancia del centro de identidad de IAM debe estar conectada a un proveedor de identidad (IdP) externo, como. [Okta](#) La compatibilidad multirregional no está disponible para las instancias que utilizan [Active Directory o el directorio](#) del [Centro de identidad como fuente](#) de identidad.
- AWS Regiones: la compatibilidad multirregional está disponible en [las regiones comerciales y está habilitada de forma predeterminada](#) en la suya. Cuenta de AWS En la actualidad, no se admiten las regiones de suscripción voluntaria.
- Tipo de clave KMS para el cifrado en reposo: la instancia del IAM Identity Center debe estar configurada con una clave KMS de varias regiones [gestionada por el cliente](#). La clave KMS debe estar ubicada en la misma AWS cuenta que el IAM Identity Center. Para obtener más información, consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).
- AWS compatibilidad de aplicaciones gestionadas: consulte la tabla de aplicaciones [the section called “Aplicaciones que puede utilizar con IAM Identity Center”](#) para confirmar los dos requisitos de aplicación siguientes:
  - Todas las aplicaciones AWS gestionadas que utilice su organización deben ser compatibles con el centro de identidad de IAM, que está configurado con una clave KMS administrada por el cliente.
  - Las aplicaciones AWS gestionadas que desee implementar en otras regiones deben admitir este tipo de implementación.
- Compatibilidad con el IdP externo: para aprovechar al máximo el soporte multirregional, el IdP externo debe admitir el servicio al consumidor de múltiples afirmaciones (ACS). URLs Se trata de una función de SAML que es compatible IdPs con Okta, y Microsoft Entra ID. PingFederate PingOne JumpCloud

Si utiliza un IdP que no admite varios ACS URLs, por ejemplo, le recomendamos que trabaje con su proveedor de IdP para habilitar esta función. Google Workspace Para ver las opciones que están disponibles sin varios ACS URLs, consulte [the section called “Uso de aplicaciones AWS gestionadas sin varios ACS URLs”](#) y. [the section called “Cuenta de AWS resiliencia de acceso sin varios ACS URLs”](#)

## Elegir una región adicional

Al elegir una región adicional entre las regiones comerciales habilitadas de forma predeterminada, tenga en cuenta los siguientes factores:

- **Requisitos de conformidad:** si necesita ejecutar aplicaciones AWS administradas que accedan a conjuntos de datos limitados a una región específica por motivos de cumplimiento, elija la región en la que residen los conjuntos de datos.
- **Optimización del rendimiento:** si la residencia de los datos no es un factor, seleccione la región más cercana a los usuarios de la aplicación para optimizar su experiencia.
- **Soporte de aplicaciones:** compruebe que AWS las aplicaciones requeridas estén disponibles en la región elegida.
- **Cuenta de AWS Flexibilidad de acceso:** para garantizar la continuidad del acceso a Cuenta de AWS s, elija una región geográficamente alejada de la región principal de su instancia de IAM Identity Center.

#### Note

El Centro de Identidad de IAM tiene una cuota en el número de. Regiones de AWS Para obtener más información, consulte [the section called “Cuotas adicionales”](#).

## Replique el centro de identidad de IAM en una región adicional

Si su entorno cumple los [requisitos previos](#), como configurar el centro de identidad de IAM con una clave KMS de varias regiones gestionada por el cliente, complete los siguientes pasos para replicar la instancia del centro de identidad de IAM en otra región. Su región principal seguirá funcionando con normalidad durante y después de estos pasos.

### Paso 1: Cree una clave de réplica en la región adicional

Antes de replicar el centro de identidad de IAM en una región, primero debe crear una clave de réplica de la clave de KMS gestionada por el cliente en esa región y configurar la clave de réplica con los permisos necesarios para las operaciones del centro de identidad de IAM. Para obtener instrucciones sobre cómo crear réplicas de claves multirregionales, consulte [Crear](#) réplicas de claves multirregionales.

El enfoque recomendado para los permisos de claves de KMS consiste en copiar la política de claves de la clave principal, lo que otorga los mismos permisos ya establecidos para el centro de identidad de IAM en la región principal. Como alternativa, puede definir políticas clave específicas para cada región, aunque este enfoque aumenta la complejidad de la administración de permisos en todas las regiones y puede requerir una coordinación adicional a la hora de actualizar las políticas en el futuro.

 Note

AWS KMS no sincroniza tu política de claves de KMS en todas las regiones de tu clave de KMS multirregional. Para mantener sincronizada la política de claves de KMS en todas las regiones clave de KMS, tendrás que aplicar los cambios en cada región de forma individual.

## Paso 2: Añadir la región al Centro de identidades de IAM

Al añadir una región al Centro de Identidad de IAM, se activa la replicación automática de los datos del Centro de Identidad de IAM en esa región. La replicación es asíncrona con una coherencia eventual. En las pestañas siguientes se proporcionan instrucciones para hacerlo en cualquier momento. Consola de administración de AWS AWS CLI

### Console

Para añadir una región

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, seleccione Configuración.
3. Seleccione la pestaña Administración.
4. En la sección Regiones del centro de identidad de IAM, seleccione Añadir región.
5. En la sección Regiones de AWS disponible para la replicación, elija la que prefiera Región de AWS. Si la región no aparece en la lista, no está disponible para la replicación porque la clave KMS no se ha replicado allí. Para obtener más información, consulte [the section called "Implementación de claves KMS administradas por el cliente"](#).
6. Elija Añadir región.
7. En la sección Regiones del centro de identidad de IAM, supervisa el estado de la región. Utilice el botón Actualizar (flecha circular) para comprobar el estado más reciente de la región según sea necesario. Una vez completada la replicación, continúe con el paso 2.

### AWS CLI

Para agregar una región

```
aws sso-admin add-region \  
--instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
```

```
--region-name eu-west-1
```

Para comprobar el estado actual de la región

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Cuando el estado de la región sea ACTIVO, puede continuar con el paso 2.

La duración de la replicación inicial en una región adicional depende de la cantidad de datos de la instancia de IAM Identity Center. En la mayoría de los casos, los cambios incrementales posteriores se replican en cuestión de segundos.

## Paso 3: Actualizar la configuración del IdP externo

Siga el tutorial de su IdP externo [Tutoriales sobre orígenes de identidad](#) para seguir los siguientes pasos:

Paso 3.a: Agregue el Assertion Consumer Service (ACS) URLs a su IdP externo

Este paso permite el inicio de sesión directo en cada región adicional y es necesario para permitir el inicio de sesión en las aplicaciones AWS gestionadas implementadas en esas regiones y para acceder a s a Cuenta de AWS través de esas regiones. Para saber dónde encontrar el ACS URLs, consulte. [Los puntos finales ACS son el principal y el adicional Regiones de AWS](#)

Paso 3.b (opcional): hacer que Portal de acceso a AWS esté disponible en el portal de IdP externo

Haga que la aplicación Portal de acceso a AWS de la región adicional esté disponible como aplicación de marcadores en el portal de IdP externo. Las aplicaciones de marcadores contienen solo un enlace (URL) al destino deseado y son similares a los marcadores de un navegador. Para encontrarlo Portal de acceso a AWS URLs en la consola, seleccione Ver todo Portal de acceso a AWS URLs en la sección Regiones del Centro de Identidad de IAM. Para obtener más información, consulte [the section called “AWS acceda a los puntos finales del portal en el principal y en el adicional Regiones de AWS”](#).

El IAM Identity Center admite el SSO de SAML iniciado por el IdP en cada región adicional, pero el externo IdPs normalmente lo admite con una sola URL de ACS. Para mantener la continuidad, recomendamos mantener la URL ACS de la región principal en uso para el SSO de SAML iniciado

por el IdP y utilizar las aplicaciones de marcadores y los marcadores del navegador para acceder a otras regiones.

## Paso 4: Confirme las listas de firewalls y puertas de enlace permitidas

[Revise las listas de dominios permitidos en los firewalls o pasarelas y actualícelas en función de las listas de dominios permitidos documentadas.](#)

## Paso 5: Proporcione información a sus usuarios

Proporcione a sus usuarios información sobre la nueva configuración, incluida la Portal de acceso a AWS URL de la región adicional y cómo utilizarlas. Consulte las siguientes secciones para obtener información relevante:

- [the section called “Acceso de la fuerza laboral a través de una región adicional”](#)
- [the section called “Conmutación por error a una región adicional para acceder Cuenta de AWS ”](#)
- [the section called “Implementación y administración de aplicaciones en múltiples Regiones de AWS”](#)

## La región cambia más allá de añadir la primera región

Puede añadir y eliminar regiones adicionales. La región principal no se puede eliminar sino eliminando toda la instancia del IAM Identity Center. Para obtener más información sobre la eliminación de una región, consulte [the section called “Eliminar una región del centro de identidad de IAM”](#).

No puedes promover una región adicional para que sea la principal ni degradar la región principal para que pase a ser adicional.

## ¿Qué datos se replican?

IAM Identity Center replica los siguientes datos:

| Datos                                                                     | Origen y destino de la replicación                       |
|---------------------------------------------------------------------------|----------------------------------------------------------|
| Identities de la fuerza laboral (usuarios, grupos, pertenencias a grupos) | Desde la región principal hasta las regiones adicionales |

| Datos                                                                        | Origen y destino de la replicación                                                                         |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Conjuntos de permisos y sus asignaciones a usuarios y grupos                 | De la región principal a las regiones adicionales                                                          |
| Configuración (como la configuración SAML del IdP externo)                   | De la región principal a las regiones adicionales                                                          |
| Metadatos de aplicaciones y asignaciones de aplicaciones a usuarios y grupos | Desde la región del centro de identidad de IAM conectada a una aplicación a las demás regiones habilitadas |
| Emisores de tokens de confianza                                              | De la región principal a las regiones adicionales                                                          |
| Sesiones                                                                     | De la región de origen de la sesión a las demás regiones habilitadas                                       |

#### Note

El centro de identidad de IAM no replica los datos almacenados en las aplicaciones AWS gestionadas. Además, no cambia la presencia regional de la implementación de una aplicación. Por ejemplo, si su instancia del Centro de Identidad de IAM se encuentra en EE. UU. Este (Norte de Virginia) y tiene Amazon Redshift implementado en la misma región, la replicación del Centro de Identidad de IAM en EE. UU. Oeste (Oregón) no afecta a la región de despliegue de Amazon Redshift ni a los datos que almacena.

#### Consideraciones:

- Identificadores de recursos globales en todas las regiones habilitadas: los usuarios, grupos, conjuntos de permisos y otros recursos tienen los mismos identificadores en todas las regiones habilitadas.

- La replicación no afecta a las funciones de IAM aprovisionadas: las funciones de IAM existentes aprovisionadas a partir de las asignaciones de conjuntos de permisos se utilizan al iniciar sesión en la cuenta desde cualquier región habilitada.

## Acceso de la fuerza laboral a través de una región adicional

En esta sección Portal de acceso a AWS, Cuenta de AWS se explica cómo sus empleados pueden acceder a las aplicaciones y a las aplicaciones si ha activado el IAM Identity Center en varias regiones.

Portal de acceso a AWS En una región adicional, se muestran las Cuenta de AWS s y las aplicaciones a las que sus empleados tienen acceso de la misma manera que en la región principal. Sus empleados pueden iniciar sesión Portal de acceso a AWS en otra región a través de un enlace directo al punto final del portal regional (por ejemplo <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>) o a través de una [aplicación de marcadores](#) que haya configurado en el IdP externo.

APIs Como usuario del IAM Identity Center, puede utilizar el Portal de acceso a AWS punto de conexión de una región adicional AWS CLI para autorizar su acceso. Esta funcionalidad funciona de la misma manera que en la región principal. Sin embargo, las autorizaciones de CLI no se replican en las regiones habilitadas. Por lo tanto, debe autorizar la CLI en cada región de forma individual.

## Sesiones de usuario en múltiples Regiones de AWS

El IAM Identity Center replica las sesiones de usuario de la región de origen a las demás regiones habilitadas. La revocación y el cierre de sesión en una región también se replican en las demás regiones.

### Revocación de sesiones por parte de los administradores del Centro de Identidad de IAM

Los administradores del IAM Identity Center pueden revocar las sesiones de los usuarios en otras regiones. Como las sesiones se replican en todas las regiones, en condiciones normales basta con revocar una sesión en una sola región y dejar que IAM Identity Center replique el cambio en las demás regiones habilitadas. Si la región principal del Centro de Identidad de IAM sufre una interrupción, los administradores pueden realizar esta operación en otras regiones.

## Portal de acceso a AWS puntos finales en la principal y en la adicional Regiones de AWS

Si necesita buscar el portal de AWS acceso URLs para las regiones habilitadas, siga estos pasos:

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, seleccione Configuración.
3. Seleccione la pestaña Administración.
4. En la sección Regions for IAM Identity Center, selecciona Ver todos los AWS accesos al portal URLs.

En la siguiente tabla, se especifican los Portal de acceso a AWS puntos finales de las regiones principales y adicionales de una instancia del centro de identidad de IAM.

| Portal de acceso a AWS endpoint  | Región principal | Región adicional | Patrón de URL y ejemplo                                                                                                                                   |
|----------------------------------|------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clásico: IPv4 solo <sup>1</sup>  | Sí               | No               | Patrón: <code>https://[Identity Store ID].awsapps.com/start</code><br><br>Ejemplo: <code>https://d-12345678.awsapps.com/start</code>                      |
| Solo un alias personalizado IPv4 | Sí (opcional)    | No               | Patrón: <code>https://[custom alias].awsapps.com/start</code><br><br>Ejemplo: <code>https://mycompany.awsapps.com/start</code>                            |
| Alternativa IPv4 : solo 2        | Sí               | Sí               | Patrón: <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code><br><br>Ejemplo: <code>https://ssoins-11111h2222j33pp.eu-w</code> |



| Portal de acceso a AWS endpoint | Región principal | Región adicional | Patrón de URL y ejemplo                                                                                                                                                        |
|---------------------------------|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                  |                  | est-1.portal.amazonservices.com                                                                                                                                                |
| Doble pila 2                    | Sí               | Sí               | <p>Patrón: <code>https://[Identity Center instance ID].portal.[Region].app.aws</code></p> <p>Ejemplo: <code>https://ssoins-11111h2222j33pp.portal.eu-west-1.app.aws</code></p> |

<sup>1</sup> En otras regiones, no se admite el alias personalizado y el dominio `awsapps.com` principal no está disponible.

<sup>2</sup> Los puntos de enlace del portal alternativo IPv4 y de doble pila no tienen el final `/start` en la URL.

## Los puntos finales de Assertion Consumer Service (ACS) son el principal y el adicional Regiones de AWS

Si necesita buscar el ACS URLs o descargarlo como parte de los metadatos del SAML, siga estos pasos:

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, seleccione Configuración.
3. Seleccione la pestaña Fuente de identidad.
4. En el menú desplegable Acciones, selecciona Administrar la autenticación.
5. La sección de metadatos del proveedor de servicios muestra la URL Portal de acceso a AWS y el ACS de cada región habilitada. IPv4-Only y Dual-Stack URLs se muestran en pestañas separadas. Si su IdP admite la carga de un archivo de metadatos SAML, puede elegir Descargar archivo de metadatos para descargar el archivo de metadatos SAML con todos los ACS. URLs Si su IdP no admite la carga de un archivo de metadatos, o si prefiere agregar ACS de URLs forma individual, puede copiar el ACS individual URLs de la tabla de la consola o seleccionar Ver ACS URLs y, a continuación, Copiar todo. URLs Conserve la URL de ACS que ya está

configurada para la región principal para garantizar que el inicio de sesión único con SAML iniciado por el proveedor de servicios desde la región principal siga funcionando.

En la siguiente tabla se especifican los puntos de conexión del SAML Assertion Consumer Service (ACS) en las regiones principal y adicional de una instancia del IAM Identity Center:

| Punto final ACS        | Región principal | Región adicional | Patrón de URL y ejemplo                                                                                                                                                                                                                 |
|------------------------|------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv4 solo              | Sí               | Sí               | <p>Patrón:</p> <p><code>https://[Region].signin.aws/platform/saml/acs/ [Tenant ID]</code></p> <p>Ejemplo: <code>https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code></p>                  |
| IPv4 Solo alternativa* | Sí               | No               | <p>Patrón: <code>https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID]</code></p> <p>Ejemplo: <code>https://us-west-2.signin.aws.amazon.com/platform/saml/acs/111111111111111111-aaee-ffff-dddd-111111111111</code></p> |
| Doble pila             | Sí               | Sí               | <p>Patrón:</p> <p><code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code></p> <p>Ejemplo: <code>https://us-west-2.sso.signin.aws/platform/sam</code></p>                                                             |

| Punto final ACS | Región principal | Región adicional | Patrón de URL y ejemplo                                |
|-----------------|------------------|------------------|--------------------------------------------------------|
|                 |                  |                  | l/acs/1111111111111111-aaee<br>-ffff-dddd-111111111111 |

\* En el caso de las instancias que se habilitaron antes de febrero de 2026, conserve este punto de conexión, ya que así lo requiere el inicio de sesión único de SAML en la región principal iniciado por el proveedor de servicios. El Centro de Identidad de IAM no utiliza este punto de conexión para las instancias que se habilitaron en febrero de 2026 o después.

## Uso de aplicaciones AWS gestionadas sin varios ACS URLs

Algunos proveedores de identidad externos (IdPs) no admiten el servicio al consumidor de múltiples afirmaciones (ACS) URLs en su aplicación IAM Identity Center. Varios ACS URLs son una función de SAML que se requiere para iniciar sesión directamente en una región específica en un centro de identidad de IAM multirregional.

Por ejemplo, si lanza una aplicación AWS gestionada a través de un enlace a una aplicación, el sistema activa el inicio de sesión a través de la región del centro de identidad de IAM conectada a la aplicación. Sin embargo, si la URL de ACS de esa región no está configurada en el IdP externo, se produce un error en el inicio de sesión.

Para resolver este problema, póngase en contacto con su proveedor de IdP para habilitar la compatibilidad con varios ACS. URLs Mientras tanto, puede seguir utilizando aplicaciones AWS administradas en otras regiones. En primer lugar, inicie sesión en la región cuya URL de ACS esté configurada en el IdP externo (la región principal de forma predeterminada). Tras tener una sesión activa en el Centro de identidades de IAM, puede iniciar la aplicación desde el portal de AWS acceso de cualquier región habilitada o mediante un enlace a la aplicación.

## Conmutación por error a otra región para acceder Cuenta de AWS

El tema del Cuenta de AWS acceso a través del Centro de Identidad de IAM se trata ampliamente en. [Cuenta de AWS acceder](#) En esta sección se proporcionan detalles adicionales relacionados con el mantenimiento del Cuenta de AWS acceso a varias regiones Regiones de AWS en caso de que se produzca una interrupción del servicio en la región principal.

Si su instancia del IAM Identity Center sufre una interrupción en la región principal (por ejemplo, el portal de AWS acceso de la región principal no está disponible), sus empleados pueden cambiarse a otra región para seguir accediendo Cuenta de AWS a las aplicaciones y a las que no se vean afectadas. Para obtener más información, consulte [the section called “Acceso de la fuerza laboral a través de una región adicional”](#).

Le recomendamos que comunique los Portal de acceso a AWS puntos finales de las regiones adicionales y la configuración del IdP externo (por ejemplo, marcar aplicaciones para las regiones adicionales) a sus empleados tan pronto como complete la configuración. [the section called “Replique el centro de identidad de IAM en una región adicional”](#) Esto les permitirá estar preparados para la conmutación por error a otra región si fuera necesario.

Del mismo modo, recomendamos que AWS CLI los usuarios creen [AWS CLI perfiles](#) para regiones adicionales para cada uno de los perfiles que tengan en la región principal. A continuación, pueden cambiar a ese perfil si se produce una interrupción del servicio en la región principal.

#### Note

La continuidad del acceso a Cuenta de AWS s también depende del estado del IdP externo y de los permisos, como las asignaciones de conjuntos de permisos y la pertenencia a grupos, que se aprovisionen y repliquen antes de una interrupción del servicio. Recomendamos que su organización también configure el acceso [AWS sin barreras para mantener el AWS acceso](#) a un pequeño grupo de usuarios privilegiados cuando el IdP externo interrumpa el servicio. El [acceso de emergencia](#) es una opción similar que evita el uso de usuarios de IAM, pero también depende del IdP externo.

## Cuenta de AWS resiliencia de acceso sin varios ACS URLs

Algunos proveedores de identidad externos (IdPs) no admiten el servicio al consumidor de múltiples afirmaciones (ACS) URLs en su aplicación IAM Identity Center. Varios ACS URLs son una función de SAML que se requiere para iniciar sesión directamente en una región específica en un centro de identidad de IAM multirregional.

Para permitir que sus usuarios accedan a sus regiones Cuentas de AWS a través de varias regiones del centro de identidad de IAM, debe configurar el ACS regional respectivo URLs en el IdP externo. Sin embargo, si el IdP externo admite solo una URL de ACS en su aplicación del Centro de identidad de IAM, los usuarios pueden iniciar sesión directamente en una sola región del centro de identidad de IAM.

Para resolver este problema, póngase en contacto con su proveedor de IdP para habilitar la compatibilidad con varios ACS. URLs Mientras tanto, puede utilizar regiones adicionales como respaldo para acceder a Cuentas de AWS ellas.

Si se produce una interrupción del servicio del IAM Identity Center en la región principal, debe actualizar la URL de ACS en el IdP externo con la URL de ACS de una región adicional. Tras esta actualización, sus usuarios pueden acceder al portal de AWS acceso de la región adicional mediante la aplicación IAM Identity Center existente en el portal de IdP externo o mediante un enlace directo que comparta con ellos.

Le recomendamos que pruebe esta configuración periódicamente para asegurarse de que funciona cuando sea necesario y que comunique este proceso de conmutación por error a su organización.

 Note

Si utiliza una región adicional para acceder a ella Cuentas de AWS en esta configuración, es posible que sus usuarios no puedan acceder a las aplicaciones AWS gestionadas que están conectadas a la región principal. Por lo tanto, lo recomendamos solo como medida temporal para mantener el acceso a ellas Cuentas de AWS.

## Implementación y administración de aplicaciones en varias AWS regiones

El tema del acceso a las aplicaciones a través del Centro de Identidad de IAM se trata ampliamente en [Acceso de aplicaciones](#). En esta sección se proporcionan detalles adicionales relacionados con la implementación y la administración de aplicaciones en múltiples Regiones de AWS aplicaciones.

### Implementación y administración de aplicaciones AWS administradas en múltiples Regiones de AWS

Con una instancia de IAM Identity Center de una sola región, puede implementar aplicaciones AWS administradas en la misma región que su instancia. Algunas aplicaciones, como Amazon Q Business, admiten una conexión entre regiones con el Centro de Identidad de IAM, lo que permite su despliegue fuera de la región del Centro de Identidad de IAM si la aplicación de interés está disponible allí. Sin embargo, las llamadas entre regiones pueden reducir el rendimiento de las aplicaciones, y la mayoría de las aplicaciones AWS administradas no admiten este tipo de conexión.

Una instancia del IAM Identity Center multirregional le permite implementar aplicaciones AWS gestionadas en cualquier región habilitada con una conexión al IAM Identity Center de la misma región («conexión región-local»). El despliegue en la región principal es compatible con todas las aplicaciones gestionadas integradas. AWS Para confirmar qué aplicaciones AWS gestionadas admiten el despliegue en otras regiones del Centro de Identidad de IAM, consulte la tabla de aplicaciones en [the section called “Aplicaciones que puede utilizar con IAM Identity Center”](#). En cualquier caso, la aplicación AWS gestionada debe estar disponible en la región en la que desee implementarla.

Con una conexión regional local al IAM Identity Center, las aplicaciones AWS gestionadas acceden a las identidades de los empleados de la misma región para lograr un rendimiento y una fiabilidad óptimos. [Recomendamos elegir una conexión regional local al implementar una aplicación AWS gestionada siempre que se cumplan los requisitos previos.](#)

Para implementar una aplicación AWS gestionada en una región adicional del Centro de Identidad de IAM, inicie la implementación en esa región a través de la consola de aplicaciones o la API del mismo modo que la implementó en la región principal.

#### Consideraciones:

- Si aún no ha replicado su centro de identidad de IAM en esa región, le recomendamos que lo haga primero para que la implementación de la aplicación se complete de inmediato.
- AWS En muchos casos, las aplicaciones gestionadas establecerán automáticamente una conexión región-local si ya has replicado el Centro de Identidad de IAM en la región.
- [Si una aplicación AWS gestionada ofrece una conexión entre regiones al Centro de identidades de IAM, le recomendamos que elija una conexión regional local siempre que se cumplan los requisitos previos.](#)
- Si la aplicación no admite el despliegue en otras regiones, puede desplegarla en la región principal siempre que la aplicación esté disponible allí.

#### Important

Si su instancia del IAM Identity Center es multirregional, todas las aplicaciones AWS gestionadas que utilice su organización deben ser compatibles con el IAM Identity Center configurado con una clave KMS gestionada por el cliente, independientemente de la región de despliegue de la aplicación. Confirme esto antes de implementar una aplicación y [the](#)

[section called “Aplicaciones que puede utilizar con IAM Identity Center”](#) antes de configurar una clave KMS administrada por el cliente en su centro de identidad de IAM.

## Región de administración de una aplicación

Tras implementar una aplicación AWS gestionada en una región adicional del Centro de Identidad de IAM mediante una conexión regional local, se gestionan la aplicación y sus asignaciones a los usuarios y grupos de la misma región. El Centro de Identidad de IAM replica los metadatos de la aplicación, incluidas las asignaciones a usuarios y grupos a otras regiones habilitadas, de modo que sus empleados puedan lanzar aplicaciones desde cualquier región habilitada.

Si su aplicación AWS gestionada utiliza una conexión entre regiones al IAM Identity Center, puede gestionar los detalles de la aplicación, como el nombre y la descripción, y las asignaciones de la aplicación a los usuarios y grupos mediante la consola y la API del IAM Identity Center en la región conectada. Independientemente del tipo de conexión, puede gestionar la aplicación a través de su consola en la región de despliegue.

## Propagación de identidades confiables

Puede utilizar la propagación de identidades fiable con aplicaciones AWS gestionadas que la admitan en cualquier región habilitada de su instancia del IAM Identity Center.

Todas las aplicaciones que se propagan el contexto de identidad entre sí deben estar en la misma región.

## La dependencia de una aplicación de su región de IAM Identity Center conectada

Cada aplicación AWS gestionada se conecta a una región específica del centro de identidad de IAM durante la implementación. Por lo tanto, la aplicación depende de esa región para el inicio de sesión de los usuarios, incluso si su centro de identidad de IAM está habilitado en varias regiones. Si su centro de identidad de IAM sufre una interrupción en esa región, es posible que los usuarios no puedan acceder a las aplicaciones AWS gestionadas conectadas a la región.

## Implementación y administración de aplicaciones administradas por el cliente en múltiples Regiones de AWS

El IAM Identity Center admite SAML y aplicaciones [administradas por el OAuth2 cliente](#). Puede optar por crearlas en cualquier región habilitada de su instancia del IAM Identity Center. Tras crear una, puede gestionar la aplicación y sus asignaciones a los usuarios y grupos de la misma región.

# Eliminar una región del centro de identidad de IAM

Para eliminar una región adicional de su instancia del centro de identidad de IAM, siga estos pasos:

## Paso 1: Actualizar la configuración del IdP externo

Puede optar por eliminar la URL de ACS de esta región de su IdP externo o conservarla en caso de que desee volver a añadir esta región más adelante. Te recomendamos que elimines u ocultes la aplicación de marcadores para la que hayas creado Portal de acceso a AWS en esta región.

## Paso 2: Eliminar la región

### Console

Para añadir una región

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, seleccione Configuración.
3. Seleccione la pestaña Administración.
4. En la sección Regiones del centro de identidad de IAM, elija la región adicional que desee eliminar.
5. Elija Eliminar .
6. Antes de confirmar la eliminación seleccionando Eliminar región, preste atención a la advertencia sobre la posible pérdida de acceso a las aplicaciones que se crearon en esta región del centro de identidad de IAM. Si no está seguro de si dispone de dichas aplicaciones, seleccione Aplicaciones en el panel de navegación y confirme la región conectada en la columna Creada desde para cada aplicación AWS gestionada y gestionada por el cliente.

### Note

Puede seguir incurriendo en cargos por la implementación de aplicaciones AWS administradas que aún estén conectadas a la región eliminada, incluso si pierde el acceso a estas aplicaciones. Para evitarlo, debe eliminar estas implementaciones de aplicaciones AWS gestionadas mediante la consola de aplicaciones o la API antes de eliminar la región en el Centro de identidades de IAM. Si ya has eliminado la región



del Centro de Identidad de IAM, puedes volver a añadir la región para restablecer el acceso a las aplicaciones.

7. En la sección Regiones del Centro de Identidad de IAM, supervise el estado de la región. Utilice el botón Actualizar (flecha circular) para ver el estado más reciente de la región, según sea necesario. Una vez eliminada la región, la región deja de aparecer en la lista de regiones.

## AWS CLI

Para eliminar una región

```
aws sso-admin remove-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

Para comprobar el estado actual de la región

```
aws sso-admin describe-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

Cuando se elimine la región, continúe con el paso 2.

## Paso 3: Eliminar la clave de réplica

Puede optar por eliminar la clave de réplica de esta región para evitar incurrir en gastos de almacenamiento de KMS. Para obtener más información, consulte [Eliminar una AWS KMS clave](#).

### Important

Asegúrese de eliminar solo la clave de réplica en esta región específica. Las demás regiones del centro de identidad de IAM siguen confiando en la clave KMS de las demás regiones habilitadas para su funcionamiento normal.

## El servicio de centro de identidad de IAM es APIs compatible en otras regiones AWS

| API                                            | Funcionalidad en regiones adicionales                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">API de Identity Center</a>         | <p>Compatible:</p> <ul style="list-style-type: none"> <li>• read/write Operaciones de administración de aplicaciones</li> <li>• Operaciones de lectura de instancias</li> </ul> <p>No admitido:</p> <ul style="list-style-type: none"> <li>• Cualquier operación de escritura que no esté relacionada con la aplicación</li> <li>• Operaciones de lectura de conjuntos de permisos y asignación de cuentas</li> </ul> |
| <a href="#">API del almacén de identidades</a> | Operaciones de lectura                                                                                                                                                                                                                                                                                                                                                                                                |
| <a href="#">API de OIDC</a>                    | Se admiten todas las operaciones                                                                                                                                                                                                                                                                                                                                                                                      |
| <a href="#">API del portal de acceso</a>       | Se admiten todas las operaciones                                                                                                                                                                                                                                                                                                                                                                                      |
| <a href="#">API de SCIM</a>                    | No se admite ninguna operación                                                                                                                                                                                                                                                                                                                                                                                        |

## AWS CloudTrail eventos del IAM Identity Center en la región principal y adicional

En AWS CloudTrail, puede auditar las acciones que los usuarios y administradores del Centro de Identidad de IAM llevan a cabo en todas las instancias habilitadas Regiones de AWS de su Centro de Identidad de IAM. Los AWS CloudTrail eventos se emiten y registran en la región en la que se lleva a cabo la acción. Para obtener más información, consulte [the section called “Registro y supervisión”](#).

## Disponibilidad de los casos de uso del IAM Identity Center en la región principal y en las regiones adicionales

| Característica                                                                                                                                                  | Disponibilidad regional                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directorio de personal con un portal de usuarios                                                                                                                |                                                                                                                                                                                                |
| Acceso de los usuarios al portal Portal de acceso a AWS , que incluye el inicio de sesión y las sesiones globales (un inicio de sesión para todas las regiones) | Todas las regiones habilitadas                                                                                                                                                                 |
| Visualización de todas las cuentas asignadas                                                                                                                    | Todas las regiones habilitadas                                                                                                                                                                 |
| Visualización de todas las aplicaciones asignadas (independientemente de dónde se hayan creado las aplicaciones)                                                | Todas las regiones habilitadas                                                                                                                                                                 |
| Lea el acceso a los usuarios, grupos y membresías en la AWS consola o a través de Identity Store APIs                                                           | Todas las regiones habilitadas                                                                                                                                                                 |
| Revocar las sesiones de usuario                                                                                                                                 | Todas las regiones habilitadas                                                                                                                                                                 |
| Sincronización automática de usuarios y grupos desde una fuente de identidad externa, como un IdP externo, mediante la API SCIM o la API Identity Store         | Solo en la región principal                                                                                                                                                                    |
| Configure el aprovisionamiento automático de identidades con SCIM                                                                                               | Solo en la región principal                                                                                                                                                                    |
| Configurar el SSO de SAML con un iDP externo                                                                                                                    | Solo en la región principal: acceso de lectura a través de la consola en todas las regiones habilitadas                                                                                        |
| Create/update/delete operaciones sobre usuarios, grupos y membresías a grupos a través de la consola o Identity Store APIs.                                     | Región principal: disponible a través de la API Identity Store, pero bloqueada en la consola del IAM Identity Center cuando se utiliza la API SCIM para el aprovisionamiento (excepto disable/ |

| Característica                                                                                                                     | Disponibilidad regional                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                    | enable el acceso y la eliminación de usuarios, que siempre están disponibles). Regiones adicionales: no disponibles                                       |
| Acceso a varias cuentas                                                                                                            |                                                                                                                                                           |
| Acceda a las cuentas asignadas a través de los Portal de acceso a AWS enlaces AWS CLI, y de acceso directo                         | Todas las regiones habilitadas                                                                                                                            |
| Gestione los conjuntos de permisos de varias cuentas y sus asignaciones en la consola y APIs (incluido el acceso elevado temporal) | Solo en la región principal                                                                                                                               |
| Acceso a aplicaciones y AWS servicios                                                                                              |                                                                                                                                                           |
| Implemente aplicaciones AWS administradas a través de la consola de aplicaciones y APIs                                            | Todas las regiones habilitadas: están sujetas a la disponibilidad regional de las aplicaciones y a la compatibilidad para su despliegue en otras regiones |
| Cree aplicaciones administradas por el cliente a través de la consola de Identity Center y APIs                                    | Todas las regiones habilitadas                                                                                                                            |
| Gestione los metadatos y las asignaciones de las aplicaciones en la consola y APIs                                                 | Región del centro de identidad de IAM conectada a la aplicación                                                                                           |
| Inicie aplicaciones desde Portal de acceso a AWS o directamente a través de un enlace de aplicación o un marcador                  | Todas las regiones habilitadas                                                                                                                            |
| SSO en instancias de Amazon EC2                                                                                                    | Todas las regiones habilitadas                                                                                                                            |
| Propagación de identidad confiable                                                                                                 |                                                                                                                                                           |
| Crear un emisor de tokens de confianza                                                                                             | Solo en la región principal                                                                                                                               |

| Característica                                                                                                                                                                                                         | Disponibilidad regional                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Propagación de identidad confiable con aplicaciones AWS administradas                                                                                                                                                  | Todas las regiones habilitadas: las aplicaciones que se propagan el contexto de identidad entre sí deben estar en la misma región                                            |
| Otras funciones administrativas                                                                                                                                                                                        |                                                                                                                                                                              |
| Todas las demás funciones administrativas, como la administración de regiones, la administración de claves de KMS, la administración de instancias y la administración de sesiones (excepto la revocación de sesiones) | Solo en la región principal: el acceso de lectura está disponible en todas las regiones habilitadas para algunos datos (excluidas las asignaciones de conjuntos de permisos) |

# Diseño de resiliencia y comportamiento regional

El servicio IAM Identity Center está totalmente gestionado y utiliza AWS servicios duraderos y de alta disponibilidad, como Amazon S3 y Amazon EC2. Para garantizar la disponibilidad en caso de que se produzca una interrupción en la zona de disponibilidad, el IAM Identity Center opera en varias zonas de disponibilidad. Puede replicar su instancia del IAM Identity Center en regiones adicionales para mantener el acceso a la cuenta con los permisos ya proporcionados en caso de que se produzca una interrupción regional. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).

Habilita el Centro de Identidad de IAM en su AWS Organizations cuenta de administración. Esto es necesario para que IAM Identity Center pueda aprovisionar, desaproveccionar y actualizar las funciones en todas sus funciones. Cuentas de AWS Al activar el Centro de Identidad de IAM, se despliega en la Región de AWS región actualmente seleccionada, denominada «región principal». Si desea realizar el despliegue en una región específica Región de AWS, cambie la selección de región antes de activar el Centro de identidad de IAM, ya que la región principal no se puede cambiar una vez activado el Centro de identidades de IAM.

El Centro de identidades de IAM solo admite la mayoría de las funciones administrativas de la región principal. Esto incluye la conexión a un proveedor de identidad externo, la sincronización de usuarios y grupos y la creación y asignación de conjuntos de permisos a usuarios y grupos. Por el contrario, la administración de las aplicaciones y sus asignaciones deben realizarse en la región del centro de identidad de IAM en la que se creó la aplicación.

## Note

[Incluso si su centro de identidad de IAM está replicado en otras regiones, le recomendamos que configure AWS Break-Glass Access](#). Esto le ayuda a mantener el AWS acceso de un pequeño grupo de usuarios con privilegios durante eventos como una interrupción del servicio en el IdP externo. El [acceso de emergencia](#) es otra opción que utiliza identidades de un IdP externo en lugar de usuarios de IAM; sin embargo, no protege contra una interrupción en el IdP externo.

Si bien IAM Identity Center determina el acceso desde la región en la que se habilita el servicio, las Cuentas de AWS son globales. Esto significa que, una vez que los usuarios inicien sesión en el Centro de Identidad de IAM, podrán operar en cualquier región al acceder a Cuentas de AWS través

del Centro de Identidad de IAM. Sin embargo, la mayoría de las aplicaciones AWS administradas, como Amazon SageMaker AI, deben instalarse en una región de la instancia del centro de identidad de IAM para que los usuarios se autenticuen y asignen acceso a estas aplicaciones. Para obtener información sobre las restricciones regionales a la hora de utilizar una aplicación con el Centro de Identidad de IAM, consulte la documentación de la aplicación y [the section called “Implementación y administración de aplicaciones AWS administradas en múltiples Regiones de AWS”](#)

También puede utilizar el Centro de identidades de IAM para autenticar y autorizar el acceso a las aplicaciones gestionadas por el cliente basadas en SAML a las que se puede acceder a través de una URL pública, independientemente de la plataforma o la nube en la que se haya creado la aplicación.

No recomendamos utilizarlas [Instancias de cuenta de IAM Identity Center](#) como medio para implementar la resiliencia, ya que no permiten el acceso a las AWS cuentas y crean un segundo punto de control aislado que no está conectado a la instancia de la organización.

## Diseñado para la disponibilidad

En la siguiente tabla se muestra la disponibilidad para la que se diseñó el Centro de Identidad de IAM en una sola AWS región. Estos valores no representan un acuerdo de nivel de servicio ni una garantía, sino que proporcionan información sobre los objetivos de diseño. Los porcentajes de disponibilidad hacen referencia al acceso a los datos o las funciones y no a la durabilidad (por ejemplo, la retención de datos a largo plazo).

| Componente de servicio                        | Objetivo de diseño de disponibilidad |
|-----------------------------------------------|--------------------------------------|
| Plano de datos (incluido el inicio de sesión) | 99.95%                               |
| Plano de control                              | 99.90%                               |

## Configure el acceso de emergencia al Consola de administración de AWS

El IAM Identity Center se creó a partir de una AWS infraestructura de alta disponibilidad y utiliza una arquitectura de zonas de disponibilidad para eliminar los puntos únicos de error. Para disponer de un nivel de protección adicional en el improbable caso de que se produzca una avería o se produjera

una Región de AWS avería en el centro de identidad de IAM, le recomendamos que configure una configuración que pueda utilizar para proporcionar acceso temporal al Consola de administración de AWS

AWS le permite:

- [Conecte su IdP de terceros a IAM Identity Center.](#)
- Conecte su IdP de terceros a una persona Cuentas de AWS mediante la federación basada en [SAML 2.0](#).

Si utiliza IAM Identity Center, puede utilizar estas funciones para crear la configuración de acceso de emergencia que se describe en las siguientes secciones. Esta configuración le permite utilizar el IAM Identity Center como mecanismo de acceso. Cuenta de AWS Si el Centro de Identidad de IAM se interrumpe, los usuarios de sus operaciones de emergencia pueden iniciar sesión en el Consola de administración de AWS mediante la federación directa con las mismas credenciales que utilizan para acceder a sus cuentas. Esta configuración funciona cuando IAM Identity Center no está disponible, pero el plano de datos de IAM y su proveedor de identidades (IdP) externo están disponibles. [Si prefiere no depender del IdP externo, considere configurar AWS el acceso break-glass](#)

#### Important

Le recomendamos que implemente esta configuración antes de que se produzca una interrupción, ya que no podrá crearla si también se interrumpe su acceso para crear los roles de IAM requeridos. Pruebe esta configuración periódicamente para asegurarse de que su equipo sepa qué hacer en caso de que se interrumpa IAM Identity Center.

## Temas

- [Resumen de la configuración del acceso de emergencia](#)
- [Cómo diseñar sus roles de operaciones críticas](#)
- [Cómo planificar su modelo de acceso](#)
- [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#)
- [Cómo crear la configuración de acceso de emergencia](#)
- [Tareas de preparación de emergencias](#)
- [Proceso de conmutación por error de emergencia](#)



- [Volver a las operaciones normales](#)
- [Configuración única de una aplicación de federación de IAM directa en Okta](#)
- [Configuración única de una aplicación de federación de IAM directa con ADFS](#)

## Resumen de la configuración del acceso de emergencia

Complete las tareas siguientes para configurar el acceso de emergencia:

1. [Cree una cuenta de operaciones de emergencia en su organización en AWS Organizations](#). Esta cuenta pasará a ser su cuenta de operaciones de emergencia.
2. Conecte el IdP a la cuenta de operaciones de emergencia mediante la [federación basada en SAML 2.0](#).
3. En la cuenta de operaciones de emergencia, [cree un rol para la federación de proveedores de identidades de terceros](#). Además, cree un rol de operaciones de emergencia en cada una de sus cuentas de carga de trabajo, con los permisos necesarios.
4. [Delegue el acceso a sus cuentas de carga de trabajo para el rol de IAM](#) que creó en la cuenta de operaciones de emergencia. Para autorizar el acceso a su cuenta de operaciones de emergencia, cree un grupo de operaciones de emergencia en su IdP, sin miembros.
5. Permita que el grupo de operaciones de emergencia de su IdP utilice el rol de operaciones de emergencia creando una regla en su IdP que [permita el acceso federado de SAML 2.0 a la Consola de administración de AWS](#).

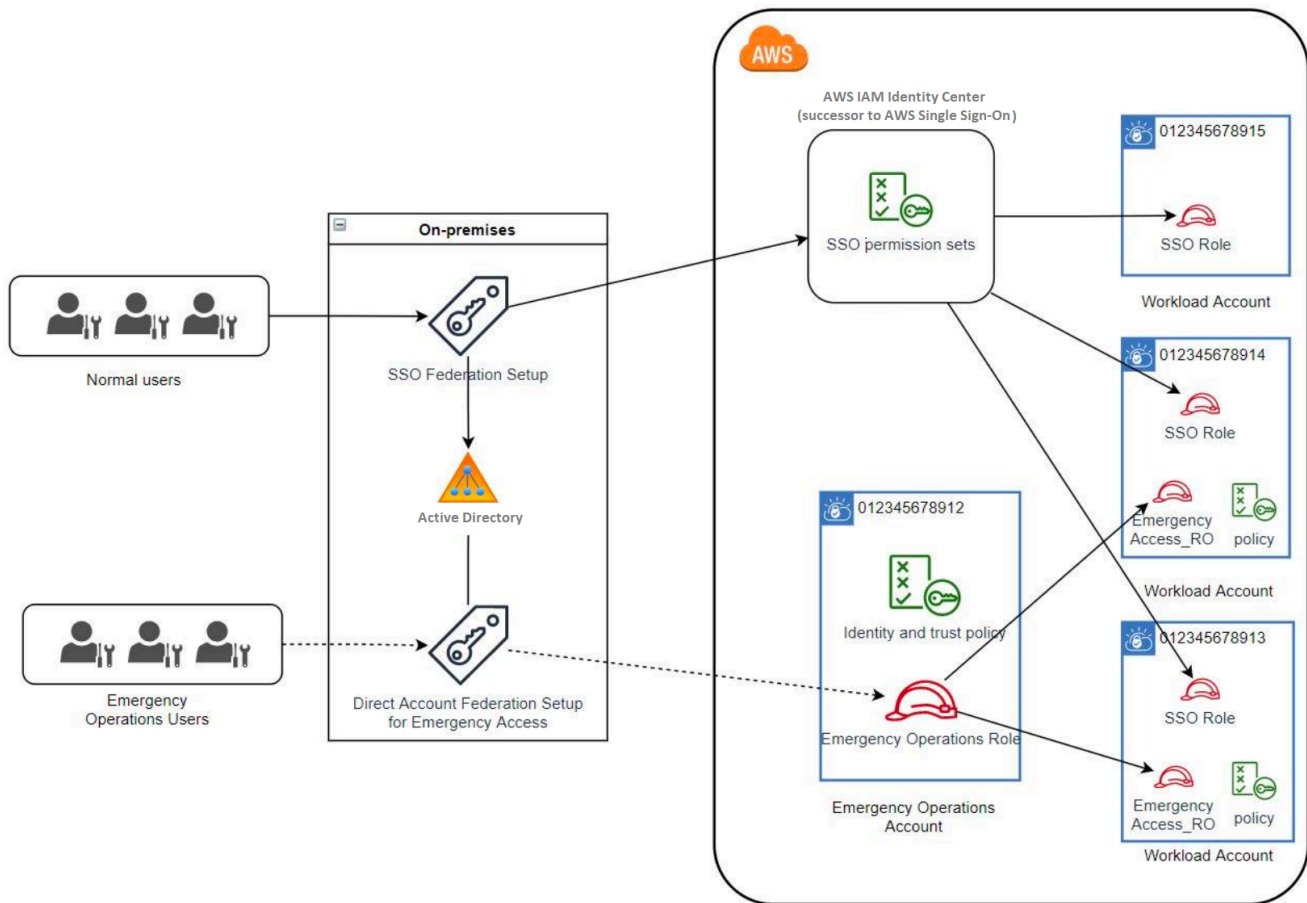
Durante las operaciones normales, nadie tiene acceso a la cuenta de operaciones de emergencia porque el grupo de operaciones de emergencia de su IdP no tiene miembros. En caso de que se produzca una interrupción en IAM Identity Center, utilice su IdP para añadir usuarios de confianza al grupo de operaciones de emergencia de su IdP. A continuación, estos usuarios pueden iniciar sesión en su IdP, acceder a la Consola de administración de AWS cuenta de operaciones de emergencia y asumir la función de operaciones de emergencia en la cuenta de operaciones de emergencia. A partir de ahí, estos usuarios pueden [cambiar de rol](#) al de acceso de emergencia en sus cuentas de carga de trabajo, donde tienen que realizar tareas operativas.

## Cómo diseñar sus roles de operaciones críticas

Con este diseño, se configura una cuenta única Cuenta de AWS en la que se federa a través de IAM, de modo que los usuarios puedan asumir funciones operativas fundamentales. Las funciones de operaciones críticas tienen una política de confianza que permite a los usuarios asumir el rol

correspondiente en sus cuentas de carga de trabajo. Los roles de las cuentas de carga de trabajo proporcionan los permisos que los usuarios necesitan para realizar tareas esenciales.

En el diagrama siguiente se proporciona información general del diseño.



## Cómo planificar su modelo de acceso

Antes de configurar el acceso de emergencia, cree un plan sobre cómo funcionará el modelo de acceso. Utilice el siguiente proceso para crear este plan:

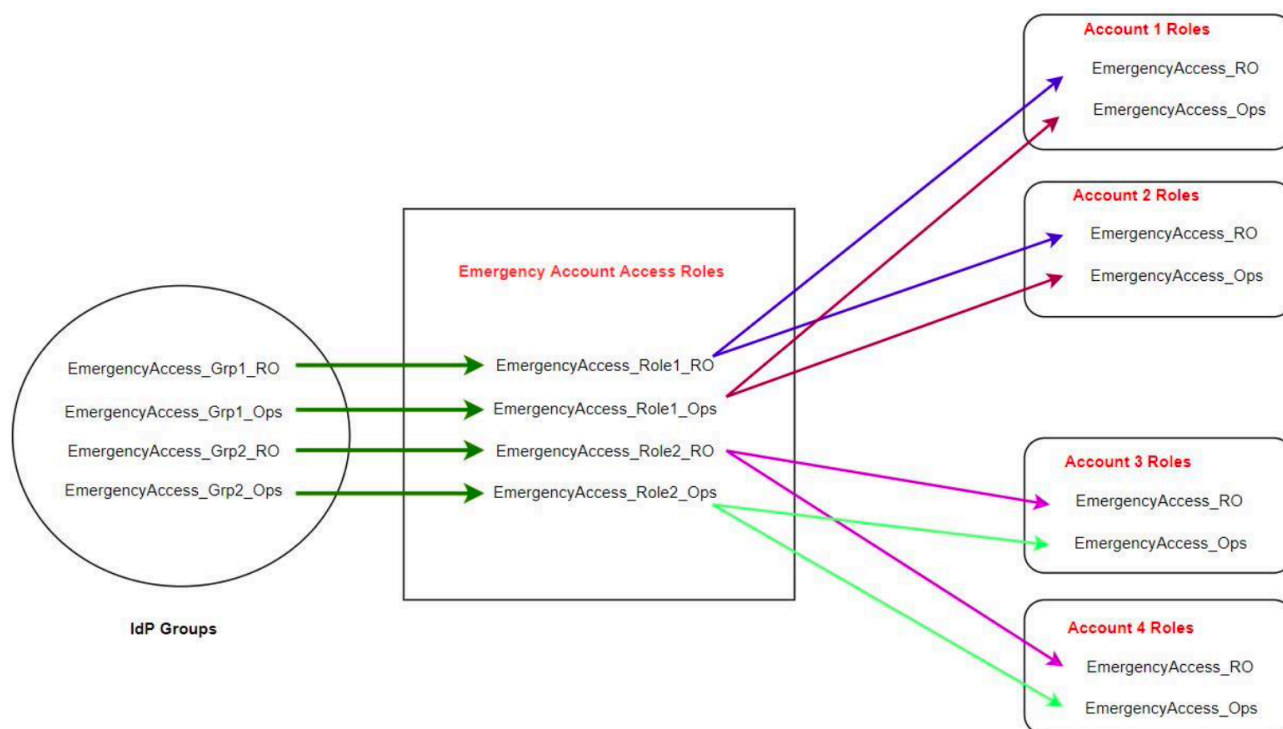
1. Identifique los Cuentas de AWS lugares en los que el acceso de emergencia de los operadores es esencial durante una interrupción en el IAM Identity Center. Por ejemplo, es probable que sus cuentas de producción sean esenciales, pero es posible que sus cuentas de desarrollo y prueba no lo sean.
2. Para ese conjunto de cuentas, identifique los roles críticos específicos que necesita en sus cuentas. En todas estas cuentas, defina de manera coherente lo que pueden hacer los roles.

Esto simplifica el trabajo en su cuenta de acceso de emergencia, en la que puede crear roles multicuentas. Le recomendamos que comience con 2 roles distintos en estas cuentas: de solo lectura (RO) y de operaciones (Ops). Si es necesario, puede crear más roles y asignarlos a un grupo distinto de usuarios de acceso de emergencia en su configuración.

- Identifique y cree grupos de acceso de emergencia en su IdP. Los miembros del grupo son los usuarios a los que está delegando el acceso a los roles de acceso de emergencia.
- Defina qué roles pueden asumir estos grupos en la cuenta de acceso de emergencia. Para ello, defina reglas en su IdP que generen notificaciones que enumeren los roles a los que puede acceder el grupo. Estos grupos pueden entonces asumir sus roles de solo lectura o de operaciones en la cuenta de acceso de emergencia. A partir de esos roles, pueden asumir los roles correspondientes en sus cuentas de carga de trabajo.

## Cómo diseñar una asignación de roles, cuentas y grupos de emergencia

En el siguiente diagrama, se muestra cómo asignar los grupos de acceso de emergencia a los roles de la cuenta de acceso de emergencia. El diagrama también muestra las relaciones de confianza entre roles que permiten que los roles de las cuentas de acceso de emergencia accedan a los roles correspondientes de las cuentas de carga de trabajo. Recomendamos que el diseño de su plan de emergencia utilice estas asignaciones como punto de partida.



## Cómo crear la configuración de acceso de emergencia

Utilice la siguiente tabla de asignación para crear su configuración de acceso de emergencia. Esta tabla refleja un plan que incluye 2 roles en las cuentas de carga de trabajo: de solo lectura (RO) y de operaciones (Ops), con las correspondientes políticas de confianza y permisos. Las políticas de confianza permiten que los roles de las cuentas de acceso de emergencia accedan a los roles de las cuentas de carga de trabajo individuales. Los roles individuales de la cuenta de carga de trabajo también tienen políticas de permisos sobre lo que el rol puede hacer en la cuenta. Las políticas de permisos pueden ser [políticas administradas por AWS](#) o [políticas administradas por el cliente](#).

| Cuenta                         | Roles a crear                                                                                                                              | Política de confianza         | Política de permisos                                     |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------|
| Cuenta 1                       | Emergency<br>Access_RO                                                                                                                     | Emergency<br>Access_Role1_RO  | arn:aws:iam::aws:policy/ReadOnlyAccess                   |
| Cuenta 1                       | Emergency<br>Access_Ops                                                                                                                    | Emergency<br>Access_Role1_Ops | arn:aws:iam::aws:policy/job-function/SystemAdministrator |
| Cuenta 2                       | Emergency<br>Access_RO                                                                                                                     | Emergency<br>Access_Role2_RO  | arn:aws:iam::aws:policy/ReadOnlyAccess                   |
| Cuenta 2                       | Emergency<br>Access_Ops                                                                                                                    | Emergency<br>Access_Role2_Ops | arn:aws:iam::aws:policy/job-function/SystemAdministrator |
| Cuenta de acceso de emergencia | Emergency<br>Access_Role1_RO<br><br>Emergency<br>Access_Role1_Ops<br><br>Emergency<br>Access_Role2_RO<br><br>Emergency<br>Access_Role2_Ops | IdP                           | AssumeRole para el recurso de rol en la cuenta           |

En este plan de asignación, la cuenta de acceso de emergencia contiene 2 roles de solo lectura y 2 roles de operaciones. Estos roles confían en su IdP para autenticar y autorizar a los grupos seleccionados a acceder a los roles pasando los nombres de los roles en aserciones. En las cuentas 1 y 2 de carga de trabajo hay los correspondientes roles de solo lectura y operaciones. Para la cuenta de carga de trabajo 1, el rol EmergencyAccess\_R0 confía en el rol EmergencyAccess\_Role1\_R0 que reside en la cuenta de acceso de emergencia. En la tabla se especifican patrones de confianza similares entre los roles de solo lectura y operaciones de la cuenta de carga de trabajo y los correspondientes roles de acceso de emergencia.

## Tareas de preparación de emergencias

Para preparar la configuración de acceso de emergencia, recomendamos que realice las siguientes tareas antes de que se produzca una emergencia.

1. Configure una aplicación de federación de IAM directa en su IdP. Si utiliza Okta u otro dispositivo externo IdPs como fuente de identidad, consulte [Configuración única de una aplicación de federación de IAM directa en Okta](#). Si utiliza Active Directory como fuente de identidad, consulte [Configuración única de una aplicación de federación de IAM directa con ADFS](#).
2. Cree una conexión de IdP en la cuenta de acceso de emergencia a la que se pueda acceder durante el evento.
3. Cree roles de acceso de emergencia en las cuentas de acceso de emergencia tal y como se describe en la tabla de asignación anterior.
4. Cree roles de operaciones temporales con políticas de confianza y permisos en cada una de las cuentas de carga de trabajo.
5. Cree grupos de operaciones temporales en su IdP. Los nombres de los grupos dependerán de los nombres de los roles de operaciones temporales.
6. Pruebe la federación de IAM directa.
7. Deshabilite la aplicación de federación de IdP en su IdP para evitar su uso regular.

## Proceso de conmutación por error de emergencia

Si no hay una instancia del IAM Identity Center disponible y decide que debe proporcionar acceso de emergencia a la consola de AWS administración, le recomendamos el siguiente proceso de conmutación por error.

1. El administrador del IdP habilita la aplicación de federación de IAM directa en su IdP.

2. Los usuarios solicitan el acceso al grupo de operaciones temporal a través del mecanismo que ya tiene, como una solicitud por correo electrónico, un canal de Slack u otra forma de comunicación.
3. Los usuarios que añada a sus grupos de acceso de emergencia inician sesión en el IdP, seleccionan la cuenta de acceso de emergencia y los usuarios eligen un rol para usarlo en la cuenta de acceso de emergencia. A partir de estos roles, pueden asumir roles en las cuentas de carga de trabajo correspondientes que tienen una confianza cruzada con el rol de cuenta de emergencia.

## Volver a las operaciones normales

Consulte el [AWS Health Dashboard](#) para confirmar cuándo se restablece el estado del servicio del IAM Identity Center. Para volver a las operaciones normales, siga estos pasos:

1. Cuando el icono de estado del servicio de IAM Identity Center indique que el servicio está en buen estado, inicie sesión en IAM Identity Center.
2. Si puede iniciar sesión correctamente en IAM Identity Center, comunique a los usuarios con acceso de emergencia que IAM Identity Center está disponible. Indique a estos usuarios que cierren sesión y usen el portal de AWS acceso para volver a iniciar sesión en el Centro de identidad de IAM.
3. Una vez que todos los usuarios con acceso de emergencia cierren la sesión, deshabilite en el IdP la aplicación de federación de IdP. Le recomendamos que realice esta tarea después del horario de trabajo.
4. Elimine todos los usuarios del grupo de acceso de emergencia del IdP.

Su infraestructura de roles de acceso de emergencia sigue funcionando como un plan de acceso alternativo, pero ahora está deshabilitada.

## Configuración única de una aplicación de federación de IAM directa en Okta

1. Inicie sesión en su cuenta de Okta como usuario con permisos administrativos.
2. En la Consola de administración de Okta, en Aplicaciones, seleccione Aplicaciones.
3. Seleccione Explorar el catálogo de aplicaciones. Busque y elija Federación de cuentas de AWS . Seleccione Agregar integración.
4. Para configurar la federación de IAM directa, siga AWS los pasos que se indican en [Cómo configurar SAML 2.0 para](#) la federación de cuentas. AWS Para gestionar situaciones de error

regionales, al configurar el punto final de inicio de sesión, te recomendamos que habilite tanto el punto de enlace no regional como varios puntos de enlace regionales en todas las regiones en las que opere, a fin de mejorar la resiliencia de la federación. Al configurar la URL de ACS para este acceso de emergencia, le recomendamos que utilice el punto de enlace regional de una región diferente a la región en la que está desplegado su centro de identidad de IAM. Consulte los [puntos de conexión de inicio de sesión](#) en la Referencia AWS general para ver la lista de puntos de enlace regionales.

- En la pestaña Opciones de inicio de sesión, seleccione SAML 2.0 e introduzca los ajustes de Filtro de grupo y Patrón de valores de rol. El nombre del grupo para el directorio de usuarios depende del filtro que configure.

|                    |                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|
| Group Filter       | <code>^aws\#\S+\#(?{{role}})[\w\.-]+\#(?{{accountid}}\d+)\\$</code>                                 |
| Role Value Pattern | <code>arn:aws:iam::\${accountid}:saml-provider/Okta,arn:aws:iam::\${accountid}:role/\${role}</code> |

En la figura anterior, la variable `role` corresponde al rol de operaciones de emergencia en su cuenta de acceso de emergencia. Por ejemplo, si crea el `EmergencyAccess_Role1_R0` rol (como se describe en la tabla de mapeo) en Cuenta de AWS 123456789012 y si la configuración del filtro de grupo está configurada como se muestra en la figura anterior, el nombre de su grupo debería serlo. `aws#EmergencyAccess_Role1_R0#123456789012`

- En el directorio (por ejemplo, el directorio de Active Directory), cree el grupo de acceso de emergencia y especifique un nombre para el directorio (por ejemplo, `aws#EmergencyAccess_Role1_R0#123456789012`). Asigne sus usuarios a este grupo mediante el mecanismo de aprovisionamiento existente.
- En la cuenta de acceso de emergencia, [configure una política de confianza personalizada](#) que proporcione los permisos necesarios para que se asuma el rol de acceso de emergencia durante una interrupción. A continuación, se muestra un ejemplo de una política de confianza personalizada asociada al rol `EmergencyAccess_Role1_R0`. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#). Sustituya el ARN del proveedor de SAML de ejemplo por el correcto que haya creado en la cuenta de acceso de emergencia. Sustituya los puntos finales regionales del ejemplo por las regiones que elija.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML
PROVIDER NAME]"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": [
            "https://signin.aws.amazon.com/saml",
            "https://us-west-2.signin.aws.amazon.com/saml",
            "https://us-west-1.signin.aws.amazon.com/saml",
            "https://us-east-2.signin.aws.amazon.com/saml"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": "sts:SetSourceIdentity"
    }
  ]
}
```

8. A continuación se muestra un ejemplo de una declaración de una política de permisos asociada al rol `EmergencyAccess_Role1_R0`. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).



## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
        "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
      ]
    }
  ]
}
```

9. En las cuentas de carga de trabajo, configure una política de confianza personalizada. A continuación se muestra un ejemplo de declaración de una política de confianza asociada al rol EmergencyAccess\_R0. En este ejemplo, la cuenta 123456789012 es la cuenta de acceso de emergencia. Para ver un ejemplo, consulte la cuenta de carga de trabajo en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

 Note

La mayoría de IdPs permiten mantener desactivada la integración de una aplicación hasta que sea necesaria. Le recomendamos que mantenga la aplicación de federación de IAM directa desactivada en su IdP hasta que sea necesaria para el acceso de emergencia.

## Configuración única de una aplicación de federación de IAM directa con ADFS

Esta guía describe el proceso de configuración único para configurar la federación de IAM directa y ADFS permitir el acceso de emergencia Cuentas de AWS cuando el Centro de Identidad de IAM no esté disponible.

### Requisitos previos

Si planea realizar la configuración ADFS con Microsoft AD AWS administrado, le recomendamos que primero [configure la replicación multirregional](#) y continúe con los siguientes pasos en la región adicional y no en la región principal para garantizar la resiliencia.

### Planifique la convención de nomenclatura de los grupos de Active Directory

Cree grupos de AD con un patrón de nomenclatura específico que permita la coincidencia automática entre los nombres de los grupos y las funciones de AWS IAM.

Formato de nomenclatura de grupos: AWS-<AccountNumber>-<RoleName>

Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#). Cuando se asigna a un usuario a este grupo, se le concede acceso al EmergencyAccess\_Role1\_R0 rol de la cuenta123456789012. Si un usuario está asociado a varios grupos, verá una lista de las funciones disponibles Cuenta de AWS y podrá elegir qué función desea asumir.

## AWS configuración

La configuración completa incluye las configuraciones de una cuenta de acceso de emergencia y de las cuentas de carga de trabajo. Para ver una ilustración de la configuración general, consulte [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).

1. [Cree un proveedor de identidades SAML](#)
2. [Cree funciones de acceso de emergencia](#)
3. [Configure los roles de las cuentas de carga](#)

### Cree un proveedor de identidades SAML

En la cuenta de acceso de emergencia, cree un proveedor de identidades SAML en IAM siguiendo los pasos que se indican en [Crear un proveedor de identidades SAML](#) en IAM. Descarga los metadatos necesarios de tu servidor: ADFS

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

### Cree funciones de acceso de emergencia

[Cree funciones de acceso de emergencia](#) en la cuenta de emergencia utilizando la federación SAML 2.0 como tipo de entidad de confianza. Seleccione el proveedor de SAML 2.0 que creaste en el paso anterior.

#### Consideraciones:

- Incluya todas las regiones en las que opera: seleccione todas las regiones en las que tenga cargas de trabajo activas para garantizar que la federación siga disponible durante una interrupción regional.
- Configure al menos un punto final regional adicional, incluso si opera en una sola región; por ejemplo, si solo opera en `us-east-1`, agréguelo `us-west-2` como punto final secundario. Puede transferir por error su IdP al punto de inicio de sesión de `us-west-2` SAML y seguir accediendo a sus `us-east-1` recursos, incluso sin ninguna carga de trabajo incorporada. `us-west-2`
- Habilite tanto el punto final no regional como el punto final regional: aunque el punto final no regional (`https://signin.aws.amazon.com/saml`) tiene una alta disponibilidad, está alojado en un único punto final regional ( ) Región de AWS `us-east-1`, mientras que los puntos finales

regionales (<https://<region>.signin.aws.amazon.com/saml>) mejoran la resiliencia al reducir la dependencia de un único punto final global.

## Configure la política de confianza

Consulte un [Configuración única de una aplicación de federación de IAM directa en Okta](#) ejemplo de política de confianza con varios puntos de conexión regionales de inicio de sesión. Sustituya los puntos de enlace regionales y el proveedor de SAML de ejemplo por los suyos. ARNs

## Configure las políticas de permisos

Consulte un [Configuración única de una aplicación de federación de IAM directa en Okta](#) ejemplo de la política de permisos que adjunta a las funciones de acceso de emergencia.

## Configure los roles de las cuentas de carga

Para las funciones de la cuenta de carga de trabajo, configure una política de confianza personalizada que permita que las funciones de acceso de emergencia de la cuenta de acceso de emergencia las asuman. Consulte un [Configuración única de una aplicación de federación de IAM directa en Okta](#) ejemplo de política de confianza, donde la cuenta 123456789012 es la cuenta de acceso de emergencia.

## Configuración de Active Directory

En los siguientes pasos se describe cómo configurar Active Directory y ADFS el acceso de emergencia.

1. [Crear grupos](#)
2. [Cree una parte de confianza](#)
3. [Cree reglas de reclamación](#)

## Crear grupos

Cree grupos de emergencia en Active Directory de acuerdo con la convención de nomenclatura descrita anteriormente (por ejemplo, AWS-123456789012-EmergencyAccess\_Role1\_R0). Asigne usuarios a estos grupos mediante sus mecanismos de aprovisionamiento existentes.

## Cree una parte de confianza

ADFS la federación requiere una configuración de parte de confianza. La parte que confía es AWS Security Token Service (AWS STS), que subcontrata la autenticación ADFS como proveedor de identidad.

1. En la consola ADFS de administración, utilice el menú Acción y seleccione Añadir la confianza de la persona que confía. Seleccione Reclamaciones pendientes al añadir una parte de confianza.
2. Para los metadatos de la federación, introduzca la URL de los metadatos de la información de metadatos del proveedor de identidad en la consola de IAM. Por ejemplo:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. Defina el nombre para mostrar de la parte que confía (por ejemplo, AWS Account Access) y, a continuación, seleccione Siguiente.
4. Seleccione a quién quieres permitir el acceso AWS. Puede seleccionar grupos específicos y definir requisitos como el MFA.
5. Seleccione Cerrar en la página de finalización para completar el asistente de creación de confianza de personas que confían en el usuario. AWS ahora está configurado como una parte que confía.

## Cree reglas de reclamación

ADFS utiliza el lenguaje de normas de reclamaciones para emitir y transformar las reclamaciones entre los proveedores de reclamaciones y las partes que confían en ellas. Debe crear cuatro reglas de reclamación: NameId Get AD Groups y Roles for AWS Access. RoleSessionName

Haga clic con el botón derecho en la parte que confía y, a continuación, seleccione Editar política de emisión de reclamaciones. Seleccione Añadir regla para añadir reglas.

### 1NameId.

- a. Seleccione Transformar una reclamación entrante y, a continuación, seleccione Siguiente.
- b. Utilice los siguientes valores:
  - Nombre de la regla de reclamación: NameId
  - Tipo de reclamación entrante: Windows Account Name

- Tipo de reclamación saliente: Name ID
- Formato de ID de nombre saliente: Persistent Identifier
- Comprobar todos los valores de las reclamaciones: marcado

c. Seleccione Aceptar.

## 2. RoleSessionName

a. Seleccione Add Rule (Agregar regla).

b. En la lista de plantillas de reglas de reclamación, seleccione Enviar atributos de LDAP como notificaciones.

c. Utilice los siguientes valores:

- Nombre de la regla de reclamación: RoleSessionName
- Almacén de atributos: Active Directory
- Atributo de LDAP: E-Mail-Addresses
- Tipo de reclamación saliente: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`

d. Seleccione Aceptar.

## 3. Obtenga grupos de AD

a. Seleccione Add Rule (Agregar regla).

b. En la lista de plantillas de reglas de reclamación, selecciona Enviar reclamaciones mediante una regla personalizada y, a continuación, selecciona Siguiente.

c. En Nombre de la regla de reclamación Get AD Groups, introduzca y, a continuación, en Regla personalizada, introduzca lo siguiente:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Esta regla personalizada utiliza un script en el lenguaje de las reglas de notificación que recupera todos los grupos de los que es miembro el usuario autenticado y los coloca en una notificación temporal denominada `http://temp/variable`

 Note

Asegúrese de que no haya ningún espacio en blanco al final para evitar resultados inesperados.

#### 4. Atributos del rol

- a. Seleccione Add Rule (Agregar regla).
- b. En la lista de plantillas de reglas de reclamación, seleccione Enviar reclamaciones mediante una regla personalizada y, a continuación, elija Siguiente.
- c. En Nombre de la regla de reclamaciónRoles, introduzca y, a continuación, en Regla personalizada, introduzca lo siguiente:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]  
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
    RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/  
<ADFS>,arn:aws:iam::$1:role/"));
```

Esta regla personalizada utiliza expresiones regulares para transformar cada una de las pertenencias a grupos del formulario AWS-<Account Number>-<Role Name> en el ARN del rol de IAM y el ARN del proveedor de federación de IAM que se espera. AWS

 Note

En el ejemplo de lenguaje de reglas anterior, ADFS representa el nombre lógico dado al proveedor de identidades SAML en la configuración del proveedor de identidades. AWS Cámbielo en función del nombre lógico que haya elegido en la consola de IAM para su proveedor de identidad.

### Probar la configuración

Compruebe que la solución funciona autenticándose en. <https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx> Seleccione el nombre de la parte de confianza que creaste en la lista desplegable de sitios.

## Actualiza el punto final de aserción de SAML predeterminado en ADFS

### Important

Al configurar la confianza de la parte de confianza en ADFS, el punto final de aserción de SAML se establece de forma predeterminada en el `https://signin.aws.amazon.com/` que no se trata de un punto final global y se encuentra en `us-east-1`. Le recomendamos que modifique el punto final predeterminado por un punto final regional diferente del lugar en el que está configurado su centro de identidad de IAM para garantizar la resiliencia. Por ejemplo, si su centro de identidad de IAM está desplegado en `us-east-1` y usted también opera en `us-west-2`, cambie el punto final predeterminado para consumidores de SAML Assertion a `https://us-west-2.signin.aws.amazon.com/saml`.

1. Seleccione Propiedades en la carpeta de confianza de la parte que confía y vaya a la pestaña Supervisión. Desactive la casilla Actualizar automáticamente la parte que confía.
2. Ve a la pestaña Puntos de conexión, selecciona tu terminal de inicio de sesión preferido y selecciona Editar.
3. Selecciona la casilla Establecer la URL de confianza como predeterminada. Seleccione Aceptar y Aplicar para que la configuración surta efecto.

### Note

La mayoría de IdPs permiten mantener desactivada la integración de una aplicación hasta que sea necesaria. Le recomendamos que mantenga la aplicación de federación de IAM directa desactivada en su IdP hasta que sea necesaria para el acceso de emergencia.



# Seguridad en AWS IAM Identity Center

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información sobre los programas de conformidad aplicables AWS IAM Identity Center, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza IAM Identity Center. En los siguientes temas se le mostrará cómo configurar IAM Identity Center para cumplir con sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos del IAM Identity Center.

## Temas

- [Administración de identidades y accesos para IAM Identity Center](#)
- [Consola de IAM Identity Center y autorización de la API](#)
- [AWS STS condicionan las claves de contexto del IAM Identity Center](#)
- [Registro y supervisión en IAM Identity Center](#)
- [Validación de la conformidad en IAM Identity Center](#)
- [Resiliencia en IAM Identity Center](#)
- [Seguridad de la infraestructura en IAM Identity Center](#)

# Administración de identidades y accesos para IAM Identity Center

El acceso al Centro de Identidad de IAM requiere credenciales que AWS pueda utilizar para autenticar sus solicitudes. Esas credenciales deben tener permisos para acceder a AWS los recursos, como una aplicación AWS gestionada.

La autenticación del portal de AWS acceso está controlada por el directorio que haya conectado al IAM Identity Center. Sin embargo, la autorización de los Cuentas de AWS que están disponibles para los usuarios desde el portal de AWS acceso viene determinada por dos factores:

1. A quién se le ha asignado el acceso a ellas Cuentas de AWS en la consola del IAM Identity Center. Para obtener más información, consulte [Acceso mediante inicio de sesión único a Cuentas de AWS](#).
2. Qué nivel de permisos se ha concedido a los usuarios en la consola de IAM Identity Center para permitirles el acceso adecuado a esas Cuentas de AWS. Para obtener más información, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

En las siguientes secciones se explica cómo, como administrador, puede controlar el acceso a la consola del IAM Identity Center o delegar el acceso administrativo a day-to-day las tareas desde la consola del IAM Identity Center.

- [Autenticación](#)
- [Control de acceso](#)

## Autenticación

Aprenda a acceder AWS mediante las identidades de [IAM](#).

## Control de acceso

Aunque tenga credenciales válidas para autenticar las solicitudes, si no tiene permisos, no podrá crear recursos de IAM Identity Center ni acceder a estos. Por ejemplo, debe tener permisos para crear un directorio conectado de IAM Identity Center.

### Note

Si su instancia de IAM Identity Center está configurada con una clave de KMS administrada por el cliente, los administradores de IAM Identity Center y otros actores que necesiten

acceder a la clave de KMS necesitarán permisos adicionales. Consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).

En las secciones siguientes se describe cómo administrar los permisos de IAM Identity Center. Recomendamos que lea primero la información general.

- [Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center](#)
- [Ejemplos de políticas basadas en identidades para IAM Identity Center](#)
- [Ejemplos de política basada en recursos para IAM Identity Center](#)
- [Uso de roles vinculados a servicios para IAM Identity Center](#)

## Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a los recursos se rigen por políticas de permisos. Para proporcionar acceso, un administrador de cuentas puede agregar permisos a las identidades de IAM (es decir, usuarios, grupos y roles). Algunos servicios (por ejemplo, AWS Lambda) también admiten añadir permisos a recursos.

### Note

Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

## Temas

- [Recursos y operaciones de IAM Identity Center](#)
- [Titularidad de los recursos](#)
- [Administración del acceso a los recursos](#)
- [Especificación de elementos de política: acciones, efectos, recursos y entidades principales](#)
- [Especificación de las condiciones de una política](#)

## Recursos y operaciones de IAM Identity Center

En IAM Identity Center, los recursos principales son instancias de aplicación, perfiles y conjuntos de permisos.

### Titularidad de los recursos

El propietario de un recurso es Cuenta de AWS quien creó un recurso. Es decir, el propietario Cuenta de AWS del recurso es la entidad principal (la cuenta, un usuario o un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si Usuario raíz de la cuenta de AWS crea un recurso del Centro de identidad de IAM, como una instancia de aplicación o un conjunto de permisos, usted Cuenta de AWS es el propietario de ese recurso.
- Si crea un usuario en su AWS cuenta y le concede permisos para crear los recursos del IAM Identity Center, el usuario podrá crear los recursos del IAM Identity Center. Sin embargo, su AWS cuenta, a la que pertenece el usuario, es propietaria de los recursos.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear recursos del Centro de Identidad de IAM, cualquier persona que pueda asumir el rol podrá crear recursos del Centro de Identidad de IAM. Su Cuenta de AWS, a la que pertenece el rol, será la propietaria de los recursos de IAM Identity Center.

### Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

#### Note

En esta sección se explica el uso de IAM en el contexto de IAM Identity Center. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte [What is IAM?](#) (¿Qué es IAM?) en la Guía del usuario de IAM. Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte [AWS Referencia de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan "políticas basadas en recursos". IAM Identity Center solo admite políticas basadas en identidades (políticas de IAM).

## Temas

- [Políticas basadas en identidades \(políticas de IAM\)](#)
- [Políticas basadas en recursos](#)

## Políticas basadas en identidades (políticas de IAM)

Puede agregar permisos a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjunta una política de permisos a un usuario o grupo de tu cuenta Cuenta de AWS: el administrador de la cuenta puede utilizar una política de permisos asociada a un usuario concreto para conceder permisos a ese usuario para añadir un recurso del IAM Identity Center, como una nueva aplicación.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas.

Para obtener más información sobre el uso de IAM para delegar permisos, consulte [Access management](#) (Administración de accesos) en la Guía del usuario de IAM.

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `List`. Estas acciones muestran información sobre un recurso de IAM Identity Center, como una instancia de la aplicación o un conjunto de permisos. Tenga en cuenta que el carácter comodín (\*) en el elemento `Resource` indica que las acciones están permitidas para todos los recursos de IAM Identity Center propiedad de la cuenta.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sso:List*",
      "Resource": "*"
    }
  ]
}
```

```
}  
  ]  
}
```

Para obtener más información acerca del uso de políticas basadas en identidades con IAM Identity Center, consulte [Ejemplos de políticas basadas en identidades para IAM Identity Center](#). Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte [Identidades \(usuarios, grupos y roles\)](#) en la Guía del usuario de IAM.

## Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. IAM Identity Center no admite políticas basadas en recursos.

## Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada recurso de IAM Identity Center (consulte [Recursos y operaciones de IAM Identity Center](#)), el servicio define un conjunto de operaciones de la API. Para conceder permisos para estas operaciones de la API, IAM Identity Center define un conjunto de acciones que usted puede especificar en una política. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- **Recurso:** en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.
- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `sso:DescribePermissionsPolicies` permite al usuario ejecutar la operación `DescribePermissionsPolicies` de IAM Identity Center.
- **Efecto:** especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede o permite el acceso de forma explícita a un recurso, el acceso será denegado de forma implícita. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- **Entidad principal:** en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe

especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). IAM Identity Center no admite políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte [Referencia de políticas de AWS IAM](#) en la Guía del usuario de IAM.

## Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones que se deben cumplir para que se aplique una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte [Condition](#) en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para IAM Identity Center. Sin embargo, hay claves de AWS condición que puede utilizar según convenga. Para obtener una lista completa de AWS las claves, consulte las [claves de condición globales disponibles](#) en la Guía del usuario de IAM.

## Ejemplos de políticas basadas en identidades para IAM Identity Center

En este tema se proporcionan ejemplos de políticas de IAM que puede crear para conceder permisos a los usuarios y roles para administrar IAM Identity Center.

### Important

Le recomendamos que primero consulte los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de IAM Identity Center. Para obtener más información, consulte [Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center](#).

En las secciones de este tema se explica lo siguiente:

- [Ejemplos de políticas personalizadas](#)
- [Permisos necesarios para usar la consola de IAM Identity Center](#)

## Ejemplos de políticas personalizadas

En esta sección se proporcionan ejemplos de casos de uso habituales que requieren una política de IAM personalizada. Estas políticas de ejemplo son políticas basadas en la identidad, que no especifican el elemento de la entidad principal. Esto se debe a que, con una política basada en identidades, no se especifica la entidad principal que obtiene el permiso. En su lugar, usted adjunta la política a la entidad principal. Cuando se adjunta una política de permisos basada en la identidad a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos. Puede crear políticas basadas en la identidad en IAM y adjuntarlas a usuarios, grupos y roles. and/or También puede aplicar estas políticas a los usuarios de IAM Identity Center al crear un conjunto de permisos en IAM Identity Center.

### Note

Utilice estos ejemplos cuando cree políticas para su entorno y asegúrese de realizar pruebas tanto en casos positivos (“acceso concedido”) como negativos (“acceso denegado”) antes de implementar estas políticas en su entorno de producción. Para obtener más información sobre cómo probar las políticas de IAM, consulte [Probar las políticas de IAM con el simulador de política de IAM](#) en la Guía del usuario de IAM.

## Temas

- [Ejemplo 1: permitir que un usuario visualice IAM Identity Center](#)
- [Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM](#)
- [Ejemplo 3: permitir a un usuario administrar aplicaciones en IAM Identity Center](#)
- [Ejemplo 4: permitir a un usuario administrar usuarios y grupos en el directorio de Identity Center](#)

### Ejemplo 1: permitir que un usuario visualice IAM Identity Center

La siguiente política de permisos concede permisos de solo lectura a un usuario para que pueda visualizar todos los ajustes y la información del directorio configurados en IAM Identity Center.



 Note

Esta política se proporciona únicamente con fines ilustrativos. En un entorno de producción, le recomendamos que utilice la política ViewOnlyAccess AWS gestionada del Centro de identidades de IAM.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListAccountAssignments",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListPermissionSets",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso-directory:DescribeDirectory",
        "sso-directory:SearchUsers",
        "sso-directory:SearchGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM

La siguiente política de permisos permite a un usuario crear, administrar y desplegar conjuntos de permisos para sus Cuentas de AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AttachManagedPolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:CreatePermissionSet",
        "sso>DeleteAccountAssignment",
        "sso>DeleteInlinePolicyFromPermissionSet",
        "sso>DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:UpdatePermissionSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMListPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:ListPolicies"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AccessToSSOProvisionedRoles",
      "Effect": "Allow",
```

```

        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:GetRole",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription"
        ],
        "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:GetSAMLProvider"
        ],
        "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
    }
]
}

```

#### Note

Los permisos adicionales que figuran en "Sid": "AccessToSSOProvisionedRoles" las secciones y son necesarios únicamente para que el usuario pueda crear asignaciones en la cuenta AWS Organizations de administración. "Sid": "IAMListPermissions" En algunos casos, es posible que también deba agregar iam:UpdateSAMLProvider a estas secciones.

### Ejemplo 3: permitir a un usuario administrar aplicaciones en IAM Identity Center

La siguiente política de permisos concede permisos para que los usuarios visualicen y configuren aplicaciones en IAM Identity Center, incluidas las aplicaciones SaaS preintegradas del catálogo de IAM Identity Center.

 Note

La operación `sso:AssociateProfile` utilizada en el siguiente ejemplo de política es necesaria para administrar las asignaciones de usuarios y grupos a las aplicaciones. También permite al usuario asignar usuarios y grupos Cuentas de AWS mediante los conjuntos de permisos existentes. Si un usuario debe gestionar el Cuenta de AWS acceso desde el Centro de identidades de IAM y necesita los permisos necesarios para gestionar los conjuntos de permisos, consulte [Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM](#).

Desde octubre de 2020, muchas de estas operaciones solo están disponibles a través de la consola AWS . Este ejemplo de política incluye acciones de “lectura”, como enumerar, obtener y buscar, que, en este caso, son relevantes para que la consola funcione sin errores.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AssociateProfile",
        "sso:CreateApplicationInstance",
        "sso:ImportApplicationInstanceServiceProviderMetadata",
        "sso>DeleteApplicationInstance",
        "sso>DeleteProfile",
        "sso:DisassociateProfile",
        "sso:GetApplicationTemplate",
        "sso:UpdateApplicationInstanceServiceProviderConfiguration",
        "sso:UpdateApplicationInstanceDisplayData",
        "sso>DeleteManagedApplicationInstance",
        "sso:UpdateApplicationInstanceStatus",
        "sso:GetManagedApplicationInstance",
        "sso:UpdateManagedApplicationInstanceStatus",
        "sso>CreateManagedApplicationInstance",
        "sso:UpdateApplicationInstanceSecurityConfiguration",
        "sso:UpdateApplicationInstanceResponseConfiguration",
        "sso:GetApplicationInstance",
```

```

        "sso:CreateApplicationInstanceCertificate",
        "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
        "sso:UpdateApplicationInstanceActiveCertificate",
        "sso:DeleteApplicationInstanceCertificate",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationTemplates",
        "sso:ListApplications",
        "sso:ListApplicationInstances",
        "sso:ListDirectoryAssociations",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:ListInstances",
        "sso:GetProfile",
        "sso:GetSSOStatus",
        "sso:GetSsoConfiguration",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}
]
}

```

#### Ejemplo 4: permitir a un usuario administrar usuarios y grupos en el directorio de Identity Center

La siguiente política de permisos concede permisos para permitir que un usuario pueda crear, visualizar, modificar y eliminar usuarios y grupos en IAM Identity Center.

En algunos casos, las modificaciones directas de los usuarios y grupos de IAM Identity Center están restringidas. Por ejemplo, cuando se selecciona Active Directory o un proveedor de identidades externo con el aprovisionamiento automático activado como fuente de identidad.

#### JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Effect": "Allow",
    "Action": [
        "sso-directory:ListGroupForUser",
        "sso-directory:DisableUser",
        "sso-directory:EnableUser",
        "sso-directory:SearchGroups",
        "sso-directory>DeleteGroup",
        "sso-directory:AddMemberToGroup",
        "sso-directory:DescribeDirectory",
        "sso-directory:UpdateUser",
        "sso-directory:ListMembersInGroup",
        "sso-directory:CreateUser",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchUsers",
        "sso:ListDirectoryAssociations",
        "sso-directory:RemoveMemberFromGroup",
        "sso-directory>DeleteUser",
        "sso-directory:DescribeUsers",
        "sso-directory:UpdateGroup",
        "sso-directory:CreateGroup"
    ],
    "Resource": "*"
  }
]
}

```

## Permisos necesarios para usar la consola de IAM Identity Center

Para que un usuario pueda trabajar con la consola de IAM Identity Center sin errores, necesita permisos adicionales. Si se ha creado una política de IAM más restrictiva que los permisos mínimos requeridos, la consola no funcionará como es debido para los usuarios con esa política. El siguiente ejemplo muestra el conjunto de permisos que podrían ser necesarios para garantizar un funcionamiento sin errores en la consola de IAM Identity Center.

### JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```

```

    "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "sso:GetProfile",
        "sso:GetSharedSsoConfiguration",
        "sso:GetSsoConfiguration",
        "sso:GetSSOStatus",
        "sso:GetTrust",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListTagsForResource",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeGroups",
        "sso-directory:DescribeUsers",
        "sso-directory:ListGroupsForUser",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}

```

```
]
}
```

## Ejemplos de política basada en recursos para IAM Identity Center

Todas las aplicaciones que funcionan con el IAM Identity Center y utilizan la [OAuth versión 2.0](#) requieren una política basada en los recursos. La aplicación puede gestionarse por el cliente o gestionarse. AWS La política basada en los recursos requerida, denominada política de aplicación (o [ActorPolicy](#) en la APIs), define qué [directores de IAM](#) están autorizados a ejecutar acciones de la API del método de autenticación de IAM, por ejemplo. [CreateTokenWithIAM](#) El método de autenticación de IAM permite a un responsable de IAM, como una función o un AWS servicio de IAM, autenticarse en el servicio OIDC del IAM Identity Center presentando las credenciales de IAM para solicitar o gestionar los tokens de acceso en /token? Punto final aws\_iam=t.

La política de la aplicación regula las operaciones de emisión de tokens ([CreateTokenWithIAM](#)). La política también regula las acciones que solo permiten permisos y que solo las aplicaciones AWS administradas utilizan para validar y revocar los tokens ([IntrospectTokenWithIAM](#) [RevokeTokenWithIAM](#)). En el caso de una aplicación administrada por el cliente, esta política se configura especificando las entidades principales de IAM que están autorizadas a realizar llamadas a [CreateTokenWithIAM](#). Cuando una entidad principal autorizada activa esta acción de API, la entidad autorizada recibe los tokens de acceso y actualización de la aplicación.

Si utiliza la consola del Centro de Identidad de IAM para configurar una aplicación gestionada por el cliente para la [propagación de identidades de forma fiable](#), consulte el paso 4 de [Configurar aplicaciones OAuth 2.0 gestionadas por el cliente para obtener información sobre cómo configurar la política de aplicaciones](#). Para obtener una política ejemplo, consulte [Ejemplo de política: permitir que un rol de IAM cree tokens de acceso y actualización tokens](#), más adelante en este tema.

### Requisitos de la política

La política debe cumplir los siguientes requisitos:

- La política debe incluir un elemento `Version` establecido en «2012-10-17».
- La política debe incluir al menos un elemento `Statement`.
- Cada política `Statement` debe incluir los siguientes elementos: `Effect`, `Principal`, `Action` y `Resource`.



## Elementos de una política

La política debe incluir los siguientes elementos:

### Versión

Especifica la versión del documento de política. Configure la versión en 2012-10-17 (la última versión).

### Instrucción

Contiene la política Statements. La política debe contener al menos un valor Statement.

Cada política Statement está formada por los siguientes elementos:

#### Efecto

(Obligatorio) Determina si desea permitir o denegar los permisos en la declaración de política. Los valores válidos son Allow o Deny.

#### Principal

(Obligatorio) La [entidad principal](#) es la identidad que obtiene los permisos especificados en la declaración de política. Puede especificar los roles de IAM o las entidades principales de servicio de AWS .

#### Action

(Obligatorio) Las operaciones de la API del servicio OIDC de IAM Identity Center para permitir o denegar. Entre las acciones válidas se incluyen:

- `sso-oauth:CreateTokenWithIAM`: Esta acción, que corresponde a la operación de la [CreateTokenWithIAM](#) API, otorga permiso para crear y devolver los tokens de acceso y actualizar las aplicaciones cliente autorizadas que se autentican mediante cualquier entidad de IAM, como un rol de AWS servicio o un usuario. Estos tokens pueden contener ámbitos definidos que especifiquen permisos, como `read:profile` o `write:data`.
- `sso-oauth:IntrospectTokenWithIAM` [solo con permiso]: otorga permiso para validar y recuperar información sobre los tokens de acceso OAuth 2.0 activos y los tokens de actualización, incluidos sus alcances y permisos asociados. Este permiso solo lo utilizan las aplicaciones AWS gestionadas y no está documentado en la referencia de la API OIDC del IAM Identity Center.
- `RevokeTokenWithIAM` [solo permiso]: otorga permiso para revocar los tokens de acceso OAuth 2.0 y actualizar los tokens, invalidándolos antes de su caducidad normal. Este

permiso solo lo utilizan las aplicaciones AWS gestionadas y no está documentado en la referencia de la API del OIDC del IAM Identity Center.

## Recurso

(Obligatorio) En esta política, el valor del elemento Resource es "\*", que significa «esta aplicación».

Para obtener más información sobre la sintaxis de las AWS políticas, consulte la [Referencia de políticas de AWS IAM en la Guía](#) del usuario de IAM.

## Ejemplo de política: permitir que un rol de IAM cree tokens de acceso y actualización tokens

La siguiente política de permisos otorga permisos a ExampleAppClientRole, un rol de IAM asumido por una carga de trabajo para crear y devolver los tokens de acceso y actualización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      },
      "Action": "sso-oauth:CreateTokenWithIAM",
      "Resource": "*"
    }
  ]
}
```

## AWS políticas gestionadas para el Centro de Identidad de IAM

Cómo [crear políticas de IAM administradas por el cliente](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puede utilizar las políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas administradas de AWS, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas administradas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

Las nuevas acciones que permiten enumerar y eliminar las sesiones de los usuarios están disponibles en el nuevo espacio de nombres de `identitystore-auth`. Los permisos adicionales para las acciones de este espacio de nombres se actualizarán en esta página. Al crear sus políticas de IAM personalizadas, evite utilizar \* después de `identitystore-auth`, ya que esto se aplica a todas las acciones que existan en el espacio de nombres ahora o en el futuro.

## AWS política gestionada: `AWSSSOMasterAccountAdministrator`

La política `AWSSSOMasterAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a los directores que desempeñan la función de AWS IAM Identity Center administradores. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede asociar la política `AWSSSOMasterAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMasterAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la posibilidad de crear una instancia de IAM Identity Center, los usuarios, los conjuntos de permisos y las asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados

y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibirá estos permisos automáticamente.

Esta política también incluye AWS Key Management Service los permisos necesarios para las instancias del IAM Identity Center que utilizan claves administradas por el cliente para el cifrado.

### Agrupaciones de permisos

Esta política se agrupa en instrucciones basadas en el conjunto de permisos proporcionados.

- `AWSSSOMasterAccountAdministrator`: permite a IAM Identity Center [transferir el rol de servicio](#) designado como `AWSServiceRoleforSSO` a IAM Identity Center, para que más adelante pueda asumir el rol y realizar acciones en su nombre. Esto es necesario cuando la persona o la aplicación intenta habilitar IAM Identity Center. Para obtener más información, consulte [Configurar el acceso a Cuentas de AWS](#).
- `AWSSSOMemberAccountAdministrator`— Permite a IAM Identity Center realizar acciones de administrador de cuentas en un entorno de varias AWS cuentas. Para obtener más información, consulte [AWS política gestionada: AWSSSOMember AccountAdministrator](#).
- `AWSSSOManageDelegatedAdministrator`: permite a IAM Identity Center registrar y anular el registro de un administrador delegado para su organización.
- `AllowKMSKeyUseViaService` `AllowKMSKeyDiscovery` — Permite realizar AWS Key Management Service operaciones con las claves gestionadas por el cliente que utilizan las instancias del IAM Identity Center.

Para ver los permisos de esta política, consulte la Referencia [AWSSSOMasterAccountAdministrator](#) de políticas AWS gestionadas.

### Información adicional acerca de esta política

Cuando el Centro de Identidad de IAM se activa por primera vez, el servicio del Centro de Identidad de IAM crea un [rol vinculado al servicio](#) en la cuenta de AWS Organizations administración (anteriormente, cuenta maestra) para que el Centro de Identidad de IAM pueda administrar los recursos de su cuenta. Las acciones obligatorias son `iam:CreateServiceLinkedRole` y `iam:PassRole`.

### AWS política gestionada: AWSSSOMember AccountAdministrator

La política `AWSSSOMemberAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a las entidades principales que

desempeñan el rol de un administrador de IAM Identity Center. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede asociar la política `AWSSSOMemberAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMemberAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la capacidad de crear usuarios, conjuntos de permisos y asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibe estos permisos automáticamente.

Esta política también incluye AWS Key Management Service los permisos necesarios para las instancias del IAM Identity Center que utilizan claves administradas por el cliente para el cifrado.

Para ver los permisos de esta política, consulte la Referencia [AWSSSOMemberAccountAdministrator](#) de políticas AWS gestionadas.

Información adicional acerca de esta política

Los administradores de IAM Identity Center administran a los usuarios, los grupos y las contraseñas en su almacén de directorios de Identity Center (sso-directory). El rol de administrador de la cuenta incluye permisos para las siguientes acciones:

- `"sso:*"`
- `"sso-directory:*"`

Los administradores del centro de identidad de IAM necesitan permisos limitados para realizar las siguientes Directory Service acciones para realizar las tareas diarias.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`

- `"ds:CreateAlias"`

Estos permisos permiten a los administradores de IAM Identity Center identificar los directorios existentes y administrar aplicaciones para que puedan configurarse para su uso con IAM Identity Center. Para obtener más información acerca de cada una de estas acciones, consulte [Permisos de la API de Directory Service : referencia acerca de las acciones, los recursos y las condiciones](#).

IAM Identity Center utiliza las políticas de IAM para conceder permisos a los usuarios de IAM Identity Center. Los administradores de IAM Identity Center crean conjuntos de permisos y les adjuntan políticas. El administrador de IAM Identity Center debe tener los permisos para enumerar las políticas existentes, de modo que pueda elegir qué políticas usar con el conjunto de permisos que está creando o actualizando. Para establecer permisos seguros y funcionales, el administrador de IAM Identity Center debe tener permisos para ejecutar la validación de la política de IAM Access Analyzer.

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

Los administradores del centro de identidad de IAM necesitan un acceso limitado a las siguientes AWS Organizations acciones para realizar las tareas diarias:

- `"organizations:EnableAWSServiceAccess"`
- `"organizations:ListRoots"`
- `"organizations:ListAccounts"`
- `"organizations:ListOrganizationalUnitsForParent"`
- `"organizations:ListAccountsForParent"`
- `"organizations:DescribeOrganization"`
- `"organizations:ListChildren"`
- `"organizations:DescribeAccount"`
- `"organizations:ListParents"`
- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

Estos permisos permiten a los administradores de IAM Identity Center trabajar con los recursos de la organización (cuentas) para realizar tareas administrativas básicas de IAM Identity Center, como las siguientes:

- Identificación de la cuenta de administración que pertenece a la organización
- Identificación de las cuentas de los miembros que pertenecen a la organización
- Habilitar el acceso AWS al servicio para las cuentas
- Configuración y administración de un administrador delegado

Para obtener más información acerca de cómo hacer uso de un administrador delegado con IAM Identity Center, consulte [Administración delegada](#). Para obtener más información sobre cómo se utilizan estos permisos AWS Organizations, consulte [Uso AWS Organizations con otros AWS servicios](#).

## AWS política gestionada: AWSSSODirectory administrador

Puede asociar la política AWSSSODirectoryAdministrator a las identidades de IAM.

Esta política concede permisos administrativos a los usuarios y grupos de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta pueden realizar cualquier actualización a los usuarios y grupos de IAM Identity Center. Esta política también incluye AWS Key Management Service los permisos necesarios para las instancias del IAM Identity Center que utilizan claves administradas por el cliente para el cifrado.

Esta política incluye los permisos siguientes:

- Directorio de IAM Identity Center: acceso administrativo completo a las operaciones del directorio de IAM Identity Center.
- Almacén de identidades: acceso administrativo completo a las operaciones y la autenticación del almacén de identidades.
- IAM Identity Center: permiso para enumerar asociaciones de directorios.
- AWS Key Management Service: permisos para descifrar, describir y generar claves de datos para las claves administradas por el cliente que utilizan las instancias de IAM Identity Center.

Para ver los permisos de esta política, consulte el apartado [AWSSSODirectoryAdministrator](#) en la Referencia de políticas AWS gestionadas.

## AWS política gestionada: AWSSSORRead únicamente

Puede asociar la política `AWSSSORReadOnly` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver los usuarios y grupos de IAM Identity Center directamente. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden visualizar los ajustes de IAM Identity Center, pero no pueden cambiar ninguno de los valores de la configuración.

Esta política también incluye AWS Key Management Service los permisos necesarios para las instancias del IAM Identity Center que utilizan claves administradas por el cliente para el cifrado.

Para ver los permisos de esta política, consulte [AWSSSORReadSolo](#) en la referencia de políticas AWS gestionadas.

## AWS política gestionada: AWSSSODirectory ReadOnly

Puede asociar la política `AWSSSODirectoryReadOnly` a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver los usuarios y grupos en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver las asignaciones, los conjuntos de permisos, las aplicaciones ni los ajustes de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden ver los usuarios de IAM Identity Center, pero no pueden cambiar ningún atributo de usuario ni asignar dispositivos de MFA.

Esta política también incluye AWS Key Management Service los permisos necesarios para las instancias del IAM Identity Center que utilizan claves administradas por el cliente para el cifrado.

Para ver los permisos de esta política, consulte la Referencia [AWSSSODirectoryReadOnly](#) de políticas AWS gestionadas.

## AWS política gestionada: AWSIdentity SyncFullAccess

Puede asociar la política `AWSIdentitySyncFullAccess` a las identidades de IAM.

Las entidades principales que cuentan con esta política adjunta tienen permisos de acceso total para crear y eliminar perfiles de sincronización, asociar o actualizar un perfil de sincronización con un



destino de sincronización, crear, enumerar y eliminar filtros de sincronización, e iniciar o detener la sincronización.

### Detalles del permiso

Para ver los permisos de esta política, consulte la Referencia [AWSIdentitySyncFullAccess](#) de políticas AWS gestionadas.

### AWS política gestionada: AWSIdentity SyncReadOnlyAccess

Puede asociar la política `AWSIdentitySyncReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver información sobre el perfil de sincronización de identidades, los filtros y la configuración de destino. Las entidades principales que cuentan con esta política adjunta no pueden actualizar la configuración de sincronización. Por ejemplo, las entidades principales que cuentan con estos permisos pueden visualizar los ajustes de sincronización de identidades, pero no pueden cambiar ninguno de los valores del perfil o del filtro.

Para ver los permisos de esta política, consulte la Referencia [AWSIdentitySyncReadOnlyAccess](#) de políticas AWS gestionadas.

### AWS política gestionada: AWSSSOService RolePolicy

No puede adjuntar la política `AWSSSOServiceRolePolicy` a las identidades de IAM.

Esta política está asociada a una función vinculada al servicio que permite a IAM Identity Center delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a una entrada específica. Cuentas de AWS Organizations Al habilitar la IAM, se crea una función vinculada al servicio en todos los ámbitos de la organización. Cuentas de AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Los roles vinculados al servicio que se crean en cada uno de ellos reciben un nombre. Cuenta de AWS `AWSServiceRoleForSSO` Para obtener más información, consulte [Uso de roles vinculados a servicios para IAM Identity Center](#).

### AWS política gestionada: AWSIAMIdentity CenterAllowListForIdentityContext

Al asumir un rol con el contexto de identidad del Centro de Identidad de IAM, AWS Security Token Service (AWS STS) asocia automáticamente la `AWSIAMIdentityCenterAllowListForIdentityContext` política al rol.

Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center. Se bloquearán todas las demás acciones que se invoquen en este contexto. El contexto de identidad se transmite como `ProvidedContext`.

Para ver los permisos de esta política, consulte la Referencia de políticas [AWSIAMIdentityCenterAllowListForIdentityContext](#) de políticas AWS gestionadas.

## AWS política gestionada: AWSIdentity CenterExternalManagementPolicy

Puede asociar la política `AWSIdentityCenterExternalManagementPolicy` a las identidades de IAM.

Esta política proporciona acceso para gestionar los usuarios del IAM Identity Center desde un proveedor externo.

Para ver los permisos de esta política, consulte la Referencia [AWSIdentityCenterExternalManagementPolicy](#) de políticas AWS gestionadas.

## IAM Identity Center actualiza las políticas AWS gestionadas

En la siguiente tabla se describen las actualizaciones de las políticas AWS gestionadas del Centro de Identidad de IAM desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre los cambios que se produzcan en esta página, suscríbase al canal RSS en la página de historial de documentos de IAM Identity Center.

| Cambio                                                    | Descripción                                                                                                      | Fecha                   |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">AWSIdentityCenterExternalManagementPolicy</a> | Se actualizó la política administrada para cambiar el ARN del inquilino de aprovisionamiento.                    | 5 de diciembre de 2025  |
| <a href="#">AWSIdentityCenterExternalManagementPolicy</a> | Esta política proporciona acceso para gestionar los usuarios del IAM Identity Center desde un proveedor externo. | 21 de noviembre de 2025 |

| Cambio                                                                                                                                                                                                                             | Descripción                                                                                                                                                                                                                                                           | Fecha                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">AWSSSOMasterAccountAdministrator</a> , <a href="#">AWSSSOMemberAccountAdministrator</a> , <a href="#">AWSSSORadÚnicamente</a> , <a href="#">AWSSSODirectoryadministrator</a> , <a href="#">AWSSSODirectoryReadOnly</a> | Se actualizaron las políticas gestionadas para incluir AWS KMS los permisos necesarios para las instancias del IAM Identity Center que utilizan claves gestionadas por el cliente para el cifrado.                                                                    | 17 de septiembre de 2025 |
| <a href="#">AWSSSOServiceRolePolicy</a>                                                                                                                                                                                            | Ahora esta política incluye nuevos permisos para realizar llamadas a <code>identity-sync:DeleteSyncProfile</code> .                                                                                                                                                   | 11 de febrero de 2025    |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a>                                                                                                                                                                    | Esta política ahora incluye las <code>qapps:ListQAppSessionData</code> <code>qapps:ExportQAppSessionData</code> acciones necesarias para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 2 de octubre de 2024     |
| <a href="#">AWSSSOMasterAccountAdministrator</a>                                                                                                                                                                                   | El Centro de Identidad de IAM ha añadido una nueva acción para conceder <code>DeleteSyncProfile</code> permisos que le permitan utilizar esta política para eliminar los perfiles de sincronización. Esta acción está asociada a la <code>DeleteInstance</code> API.  | 26 de septiembre de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                               | Fecha                   |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye la <code>s3:ListCallerAccessGrants</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                                                            | 4 de septiembre de 2024 |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las <code>aws:APIAccessAll</code> , <code>es:ESHttpHead</code> , <code>es:ESHttpPost</code> , <code>es:ESHttpGet</code> , <code>es:ESHttpPatch</code> , <code>es:ESHttpDelete</code> , y <code>es:ESHttpPut</code> acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 12 de julio de 2024     |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                          | Fecha               |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las opcionesqapps:PredictQApp ,qapps:ImportDocument , qapps:AssociateLibraryItemReview qapps:DisassociateLibraryItemReview qapps:GetQAppSession qapps:UpdateQAppSession qapps:GetQAppSessionMetadata qapps:UpdateQAppSessionMetadata ,y qapps:TagResource las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 27 de junio de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                  | Fecha              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las acciones elasticmapreduce:AddJobFlowSteps ,elasticmapreduce:DescribeCluster ,elasticmapreduce:CancelSteps ,elasticmapreduce:DescribeStep y elasticmapreduce:ListSteps para respaldar la propagación de identidades confiables en Amazon EMR. | 17 de mayo de 2024 |

| Cambio                                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Fecha               |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye las acciones <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps&gt;DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DisassociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps:CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps:CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps:CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , y <code>qapps:StopQAppSession</code> las acciones para respaldar las sesiones de consola con | 30 de abril de 2024 |

| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                                 | Fecha               |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                         | identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                                                                                                                                      |                     |
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | Esta política ahora incluye las <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acciones necesarias para respaldar <code>signin&gt;CreateTrustedIdentityPropagationApplicationForConsole</code> las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Esta política ahora incluye las <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acciones necesarias para respaldar <code>signin&gt;CreateTrustedIdentityPropagationApplicationForConsole</code> las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |



| Cambio                                                                 | Descripción                                                                                                                                                                                                                                      | Fecha               |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSSSOReadSolo</u></a>                                  | Esta política ahora incluye la <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye la <code>qbusiness:PutFeedback</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                       | 26 de abril de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Fecha               |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las opciones <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , y <code>q:UpdateTroubleshootingCommandResult</code> las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 24 de abril de 2024 |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye la <code>sts:SetContext</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                                                                                                                                                                                                                 | 19 de abril de 2024 |

| Cambio                                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                    | Fecha                   |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye las <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , y <code>qbusiness&gt;DeleteConversation</code> las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 11 de abril de 2024     |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | La política ahora incluye las acciones <code>s3:GetAccessGrantsInstanceForPrefix</code> y <code>s3:GetDataAccess</code> .                                                                                                                                                                                                                                                      | 26 de noviembre de 2023 |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center.                                                                                                                                                                       | 15 de noviembre de 2023 |
| <a href="#"><u>AWSSSODirectoryReadOnly</u></a>                         | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten a los usuarios enumerar y obtener sesiones.                                                                                                                                                                                                        | 21 de febrero de 2023   |

| Cambio                                           | Descripción                                                                                                                                                                              | Fecha                 |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">AWSSSOServiceRolePolicy</a>          | Ahora esta política permite realizar la acción <a href="#">UpdateSAMLProvider</a> en la cuenta de administración.                                                                        | 20 de octubre de 2022 |
| <a href="#">AWSSSOMasterAccountAdministrator</a> | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |
| <a href="#">AWSSSOMemberAccountAdministrator</a> | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |
| <a href="#">AWSSSODirectoryAdministrator</a>     | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |

| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                    | Fecha                |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | Esta política ahora incluye nuevos permisos para realizar llamadas <a href="#"><u>ListDelegatedAdministrators</u></a> . AWS Organizations Ahora esta política también incluye un subconjunto de permisos de AWSSSOManageDelegatedAdministrator que incluye permisos para realizar llamadas a <a href="#"><u>RegisterDelegatedAdministrator</u></a> y <a href="#"><u>DeregisterDelegatedAdministrator</u></a> . | 16 de agosto de 2022 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Esta política ahora incluye nuevos permisos para llamar <a href="#"><u>ListDelegatedAdministrators</u></a> AWS Organizations. Ahora esta política también incluye un subconjunto de permisos de AWSSSOManageDelegatedAdministrator que incluye permisos para realizar llamadas a <a href="#"><u>RegisterDelegatedAdministrator</u></a> y <a href="#"><u>DeregisterDelegatedAdministrator</u></a> .             | 16 de agosto de 2022 |

| Cambio                                                                                                                                 | Descripción                                                                                                                                                                                    | Fecha                |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">AWSSSOReadSolo</a>                                                                                                         | Esta política ahora incluye nuevos permisos para llamar <a href="#">ListDelegatedAdministrators</a> en AWS Organizations.                                                                      | 11 de agosto de 2022 |
| <a href="#">AWSSSOServiceRolePolicy</a>                                                                                                | Ahora esta política incluye nuevos permisos para realizar llamadas a <a href="#">DeleteRolePermissionsBoundary</a> en <a href="#">PutRolePermissionsBoundary</a> .                             | 14 de julio de 2022  |
| <a href="#">AWSSSOServiceRolePolicy</a>                                                                                                | Ahora esta política incluye nuevos permisos para realizar llamadas a <a href="#">ListAWSServiceAccessForOrganization</a> and <a href="#">ListDelegatedAdministrators</a> en AWS Organizations. | 11 de mayo de 2022   |
| <a href="#">AWSSSOMasterAccountAdministrator</a><br><a href="#">AWSSSOMemberAccountAdministrator</a><br><a href="#">AWSSSOReadSolo</a> | Agregue permisos de IAM Access Analyzer para permitir a una entidad principal utilizar las verificaciones de políticas para la validación.                                                     | 28 de abril de 2022  |

| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                                            | Fecha               |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | <p>Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.</p> <p>Para obtener información acerca de las acciones disponibles en el servicio de almacén de identidades de IAM, consulte <a href="#"><u>Referencia de la API del servicio Almacén de identidades de IAM Identity Center</u></a>.</p> | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.                                                                                                                                                                                                                                             | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSODirectoryAdministrator</u></a>     | Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.                                                                                                                                                                                                                                             | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSODirectoryReadOnly</u></a>          | Ahora esta política concede acceso a las acciones de lectura del servicio Almacén de identidades de IAM Identity Center. Este acceso es necesario para recuperar la información de los usuarios y los grupos del servicio Almacén de identidades de IAM Identity Center.                                                                               | 29 de marzo de 2022 |

| Cambio                                                               | Descripción                                                                                                                                          | Fecha               |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSIdentitySyncFullAccess</a>                            | Esta política permite obtener acceso completo a permisos de sincronización de identidades.                                                           | 3 de marzo de 2022  |
| <a href="#">AWSIdentitySyncReadOnlyAccess</a>                        | Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar la configuración de la sincronización de identidades. | 3 de marzo de 2022  |
| <a href="#">AWSSSORReadSolo</a>                                      | Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar los ajustes de configuración de IAM Identity Center.  | 4 de agosto de 2021 |
| IAM Identity Center comenzó a realizar el seguimiento de los cambios | IAM Identity Center comenzó a realizar un seguimiento de los cambios en las políticas AWS gestionadas.                                               | 4 de agosto de 2021 |

## Uso de roles vinculados a servicios para IAM Identity Center

AWS IAM Identity Center utiliza funciones AWS Identity and Access Management vinculadas al [servicio](#) (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a IAM Identity Center. Está predefinido por el Centro de Identidad de IAM e incluye todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Para obtener más información, consulte [Entender los roles vinculados a servicios en IAM Identity Center](#).

Un rol vinculado a servicios simplifica la configuración de IAM Identity Center porque ya no tendrá que agregar manualmente los permisos necesarios. IAM Identity Center define los permisos de su rol vinculado a servicios y, a menos que esté definido de otra manera, solo IAM Identity Center puede



asumir su rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Permisos de roles vinculados a servicios para IAM Identity Center

El Centro de identidad de IAM utiliza la función vinculada al servicio denominada `AWSServiceRoleForSSO` para conceder permisos al Centro de identidad de IAM para gestionar los AWS recursos, incluidas las funciones de IAM, las políticas y el IdP de SAML en su nombre.

La función de `AWSService RoleFor SSO` vinculada al servicio confía en los siguientes servicios para que la asuman:

- IAM Identity Center (prefijo de servicio: `sso`)

La política de permisos de los roles `AWSSSOService RolePolicy` vinculados a un servicio permite al Centro de Identidad de IAM completar lo siguiente en los roles de la ruta `«/aws-reserved/sso.amazonaws.com/»` y con el prefijo de nombre `«SSO_»`: `AWSReserved`

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePermissionsBoundary`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La política de permisos de funciones AWSSSOService RolePolicy vinculadas al servicio permite a IAM Identity Center completar lo siguiente en los proveedores de SAML con el prefijo «\_»: AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en todas las organizaciones:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La política de permisos de funciones AWSSSOService RolePolicy vinculadas al servicio permite a IAM Identity Center realizar las siguientes tareas en todas las funciones de IAM (\*):

- `iam:listRoles`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en «arn:aws:iam: \*:»: role/aws-service-role/ssso.amazonaws.com/AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en «arn:aws:identity-sync: \*:\*:profile/\*»:

- `identity-sync>DeleteSyncProfile`

Para obtener más información [IAM Identity Center actualiza las políticas AWS gestionadas](#) sobre AWSSSOService RolePolicy las actualizaciones de la política de permisos de roles vinculados al servicio, consulte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMRoleProvisioningActions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "IAMRoleReadActions",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource": [
        "*"
      ]
    }
  ],
}
```

```

    {
      "Sid": "IAMRoleCleanupActions",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid": "IAMSLRCleanupActions",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid": "IAMSSAMLProviderCreationAction",
      "Effect": "Allow",
      "Action": [
        "iam:CreateSAMLProvider"
      ],
      "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
      }
    },
  ],
  {

```

```

    "Sid": "IAMSAMLProviderUpdateAction",
    "Effect": "Allow",
    "Action": [
        "iam:UpdateSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
},
{
    "Sid": "IAMSAMLProviderCleanupActions",
    "Effect": "Allow",
    "Action": [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowUnauthAppForDirectory",
    "Effect": "Allow",
    "Action": [
        "ds:UnauthorizeApplication"
    ],
    "Resource": [
        "*"
    ]
},
{

```

```

        "Sid": "AllowDescribeForDirectory",
        "Effect": "Allow",
        "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "AllowDescribeAndListOperationsOnIdentitySource",
        "Effect": "Allow",
        "Action": [
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "AllowDeleteSyncProfile",
        "Effect": "Allow",
        "Action": [
            "identity-sync:DeleteSyncProfile"
        ],
        "Resource": [
            "arn:aws:identity-sync:*:*:profile/*"
        ]
    }
]
}

```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

## Creación de un rol vinculado a servicios para IAM Identity Center

No necesita crear manualmente un rol vinculado a un servicio. Una vez activado, IAM Identity Center crea un rol vinculado al servicio en todas las cuentas de la organización en Organizations. AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre.

### Notas

- Si ha iniciado sesión en la cuenta de AWS Organizations administración, esta utilizará su función con la que ha iniciado sesión actualmente y no la función vinculada al servicio. De este modo se evita la escalada de privilegios.
- Cuando el IAM Identity Center realiza cualquier operación de IAM en la cuenta de AWS Organizations administración, todas las operaciones se realizan con las credenciales del director de IAM. Esto permite que los inicios de sesión CloudTrail proporcionen visibilidad de quién realizó todos los cambios de privilegios en la cuenta de administración.

### Important

Si utilizaba el servicio IAM Identity Center antes del 7 de diciembre de 2017, cuando comenzó a admitir funciones vinculadas al servicio, IAM Identity Center creó la función de inicio de sesión único en su AWSService RoleFor cuenta. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede seguir el mismo proceso para volver a crear el rol en su cuenta.

## Edición de un rol vinculado a servicios para IAM Identity Center

El Centro de Identidad de IAM no le permite editar la función de SSO vinculada al servicio. AWSService RoleFor Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Eliminación de un rol vinculado a servicios para IAM Identity Center

No es necesario eliminar manualmente la función de SSO. AWSService RoleFor Cuando Cuenta de AWS se elimina un elemento de una AWS organización, el Centro de Identidad de IAM limpia automáticamente los recursos y elimina el rol vinculado al servicio. Cuenta de AWS

También puede utilizar la consola de IAM, la CLI de IAM o la API de IAM para eliminar manualmente el rol vinculado a servicios. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

### Note

Si el servicio IAM Identity Center está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos del Centro de Identidad de IAM utilizados por el SSO AWSService RoleFor

1. [Elimina el acceso de usuarios y grupos a un Cuenta de AWS](#) para todos los usuarios y grupos que tengan acceso a la Cuenta de AWS.
2. [Eliminación de conjuntos de permisos de IAM Identity Center](#) que ha asociado con la Cuenta de AWS.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar la función vinculada al servicio de AWSService RoleFor SSO. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Consola de IAM Identity Center y autorización de la API

La consola de IAM Identity Center existente APIs admite la doble autorización, lo que le permite seguir utilizando las operaciones de la API existentes cuando haya más nuevas disponibles. APIs Si ya tiene instancias de IAM Identity Center que se hayan creado antes del 15 de noviembre de 2023 y el 15 de octubre de 2020, puede utilizar las siguientes tablas para determinar qué operaciones de la API se asignan ahora a las operaciones de la API más recientes que se publicaron después de esas fechas.



## Temas

- [Acciones de la API después de noviembre de 2023](#)
- [Acciones de la API después de octubre de 2020](#)

## Acciones de la API después de noviembre de 2023

Las instancias de IAM Identity Center que se crearon antes del 15 de noviembre de 2023 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas.

Las instancias creadas después del 15 de noviembre de 2023 utilizan las [acciones de la API más recientes](#) a efectos de la autorización en la consola de IAM Identity Center.

| Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023 | Acción de la API utilizada después del 15 de noviembre de 2023 |
|-------------------------------------------------------------------------------|----------------------------------------------------------------|
| AssociateProfile                                                              | CreateApplicationAssignment                                    |
| CreateManagedApplicationInstance   CreateApplicationInstance                  | CreateApplication                                              |
| CreateManagedApplicationInstance                                              | PutApplicationAuthenticationMethod                             |
| DeleteApplicationInstance   DeleteManagedApplicationInstance                  | DeleteApplication                                              |
| DeleteSSO                                                                     | DeleteInstance                                                 |
| DisassociateProfile                                                           | DeleteApplicationAssignment                                    |
| GetApplicationTemplate                                                        | DescribeApplicationProvider                                    |
| GetManagedApplicationInstance                                                 | DescribeApplication                                            |
| GetSharedSsoConfiguration                                                     | DescribeInstance                                               |
| ListApplicationInstances                                                      | ListApplications                                               |
| ListApplicationTemplates                                                      | ListApplicationProviders                                       |
| ListDirectoryAssociations                                                     | DescribeInstance                                               |

| Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023                                   | Acción de la API utilizada después del 15 de noviembre de 2023 |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| ListProfileAssociations                                                                                         | ListApplicationAssignments                                     |
| UpdateApplicationInstanceDisplayData   UpdateApplicationInstanceStatus   UpdateManagedApplicationInstanceStatus | UpdateApplication                                              |

## Acciones de la API después de octubre de 2020

Las instancias de IAM Identity Center que se crearon antes del 15 de octubre de 2020 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas. Las instancias creadas después del 15 de octubre de 2020 utilizan las [acciones de la API más recientes](#) a efectos de la autorización en la consola de IAM Identity Center.

| Operation name                         | API actions used before October 15, 2020 | API actions used after October 15, 2020 |
|----------------------------------------|------------------------------------------|-----------------------------------------|
| AssociateProfile                       | AssociateProfile                         | CreateAccountAssignment                 |
| AttachManagedPolicy                    | PutPermissionsPolicy                     | AttachManagedPolicyToPermissionSet      |
| CreatePermissionSet                    | CreatePermissionSet                      | CreatePermissionSet                     |
| DeleteApplicationInstanceForAWSAccount | DeleteApplicationInstance   DeleteTrust  | DeleteAccountAssignment                 |
| DeleteApplicationProfileForAWSAccount  | DeleteProfile                            | DeleteAccountAssignment                 |
| DeletePermissionsPolicy                | DeletePermissionsPolicy                  | DeleteInlinePolicyFromPermissionSet     |
| DeletePermissionSet                    | DeletePermissionSet                      | DeletePermissionSet                     |

| Operation name                                   | API actions used before October 15, 2020           | API actions used after October 15, 2020 |
|--------------------------------------------------|----------------------------------------------------|-----------------------------------------|
| DescribePermissionsPolicies                      | DescribePermissionsPolicies                        | ListManagedPoliciesInPermissionSet      |
| DetachManagedPolicy                              | DeletePermissionsPolicy                            | DetachManagedPolicyFromPermissionSet    |
| DisassociateProfile                              | DisassociateProfile                                | DeleteAccountAssignment                 |
| GetApplicationInstanceForAWSAccount              | GetApplicationInstance                             | ListAccountAssignments                  |
| GetAWSAccountProfileStatus                       | GetProfile                                         | ListPermissionSetsProvisionedToAccount  |
| GetPermissionSet                                 | GetPermissionSet                                   | DescribePermissionSet                   |
| GetPermissionsPolicy                             | GetPermissionsPolicy                               | GetInlinePolicyForPermissionSet         |
| ListAccountsWithProvisionedPermissionSet         | ListApplicationInstances   GetApplicationInstance  | ListAccountsForProvisionedPermissionSet |
| ListAWSAccountProfiles                           | ListProfiles   GetProfile                          | ListPermissionSetsProvisionedToAccount  |
| ListPermissionSets                               | ListPermissionSets                                 | ListPermissionSets                      |
| ListProfileAssociations                          | ListProfileAssociations                            | ListAccountAssignments                  |
| ProvisionApplicationInstanceForAWSAccount        | GetApplicationInstance   CreateApplicationInstance | CreateAccountAssignment                 |
| ProvisionApplicationProfileForAWSAccountInstance | GetProfile   CreateProfile   UpdateProfile         | CreateAccountAssignment                 |
| ProvisionSAMLProvider                            | GetTrust   CreateTrust   UpdateTrust               | CreateAccountAssignment                 |

| Operation name       | API actions used before October 15, 2020 | API actions used after October 15, 2020 |
|----------------------|------------------------------------------|-----------------------------------------|
| PutPermissionsPolicy | PutPermissionsPolicy                     | PutInlinePolicyToPermissionSet          |
| UpdatePermissionSet  | UpdatePermissionSet                      | UpdatePermissionSet                     |

## AWS STS condicionan las claves de contexto del IAM Identity Center

Cuando un [director](#) hace una [solicitud](#) AWS, AWS recopila la información de la solicitud en un contexto de solicitud, que se utiliza para evaluar y autorizar la solicitud. Puede utilizar el elemento `Condition` de una política JSON para comparar las claves de la solicitud de contexto con los valores de claves que especifique en su política. La información de la solicitud proviene de diferentes orígenes, que abarcan la entidad principal que realiza la solicitud, el recurso con el que se realiza la solicitud y los metadatos sobre la solicitud en sí. Las claves de condición específicas del servicio se definen para su uso con un servicio individual. AWS

El IAM Identity Center incluye un proveedor de AWS STS contexto que permite a las aplicaciones AWS gestionadas y a las aplicaciones de terceros añadir valores a las claves de condición definidas por el IAM Identity Center. Estas claves se incluyen en los [roles de IAM](#). Los valores clave se establecen cuando una aplicación pasa un token a. AWS STS La aplicación obtiene el token al que pasa de una AWS STS de las siguientes maneras:

- Durante la autenticación con el IAM Identity Center.
- Tras el intercambio del token con un [emisor de token de confianza](#) para propagar la identidad de forma fiable. En este caso, la aplicación obtiene un token de un emisor de token de confianza y lo cambia por un token del IAM Identity Center.

Estas claves suelen ser utilizadas por aplicaciones que se integran con la propagación de identidades de confianza. En algunos casos, cuando hay valores clave, puede utilizarlas en las políticas de IAM que cree para permitir o denegar permisos.

Por ejemplo, es posible que desee proporcionar acceso condicional a un recurso en función del valor de `UserId`. Este valor indica qué usuario del IAM Identity Center utiliza el rol. El ejemplo es similar

al uso de `SourceId`. Sin embargo, a diferencia de `SourceId`, el valor de `UserId` representa un usuario específico y verificado del almacén de identidades. Este valor está presente en el token que la aplicación obtiene y al que, a continuación, pasa. AWS STS No es una cadena de uso general que pueda contener valores arbitrarios.

## Temas

- [almacén de identidades: `UserId`](#)
- [almacén de identidades: `IdentityStoreArn`](#)
- [centro de identidad: `ApplicationArn`](#)
- [centro de identidad: `CredentialId`](#)
- [centro de identidad: `InstanceArn`](#)

## almacén de identidades: `UserId`

Esta clave de contexto es `UserId` del usuario del IAM Identity Center, que es el sujeto de la afirmación de contexto emitida por el IAM Identity Center. La afirmación de contexto se pasa a. AWS STS Puede utilizar esta clave para comparar el `UserId` del usuario del IAM Identity Center en nombre del que se realiza la solicitud con el identificador del usuario que se especifique en la política.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función mediante cualquier AWS STS `assume-role` comando de la operación AWS CLI o AWS STS `AssumeRole` de la API.
- [Tipo de datos: cadena](#)
- Tipo de valor: valor único

## almacén de identidades: `IdentityStoreArn`

Esta clave de contexto es el ARN del almacén de identidades que está adjunto a la instancia del IAM Identity Center que emitió la afirmación de contexto. También es el almacén de identidades en el que puede buscar los atributos para `identitystore:UserID`. Puede usar esta clave en las políticas para determinar si `identitystore:UserID` proviene de un ARN de almacén de identidades esperado.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función

mediante cualquier AWS STS `assume-role` comando de la operación o de la AWS CLI API. AWS STS `AssumeRole`

- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## centro de identidad: ApplicationArn

Esta clave de contexto es el ARN de la aplicación para la que el IAM Identity Center emitió una afirmación de contexto. Puede usar esta clave en las políticas para determinar si `identitycenter:ApplicationArn` proviene de una aplicación esperada. El uso de esta clave puede ayudar a evitar que una aplicación inesperada acceda a un rol de IAM.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## centro de identidad: CredentialId

Esta clave de contexto es un identificador aleatorio para la credencial de rol con identidad mejorada y se utiliza únicamente para el registro. Como este valor clave es impredecible, le recomendamos que no lo utilice para afirmaciones de contexto en políticas.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [cadena](#)
- Tipo de valor: valor único

## centro de identidad: InstanceArn

Esta clave de contexto es el ARN de la instancia de IAM Identity Center que emitió la afirmación de contexto para `identitystore:UserID`. Puede utilizar esta clave para determinar si

`identitystore:UserID` y la afirmación de contexto provienen de un ARN de instancia de IAM Identity Center esperado.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS AssumeRole API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## Registro y supervisión en IAM Identity Center

Como práctica recomendada, debe supervisar su organización para asegurarse de que los cambios queden registrados. La supervisión permite investigar cualquier modificación inesperada y revertir los cambios no deseados. Actualmente, IAM Identity Center admite dos AWS servicios que le ayudan a supervisar su organización y la actividad que se lleva a cabo en ella: AWS CloudTrail Amazon EventBridge.

### Temas

- [Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail](#)
- [Registrar las llamadas a la API SCIM de IAM Identity Center con AWS CloudTrail](#)
- [Connect los componentes de la aplicación con Amazon EventBridge](#)
- [Registro de errores de sincronización de AD configurable](#)

## Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail

AWS IAM Identity Center está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en el Centro de Identidad de IAM. CloudTrail captura las llamadas a la API del Centro de Identidad de IAM como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de IAM Identity Center y las llamadas de código a las operaciones de la API de IAM Identity Center. Si crea una [ruta](#), puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos del IAM Identity Center. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó al Centro de Identidad de IAM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía del AWS CloudTrail usuario](#).

En la siguiente tabla se resumen los CloudTrail eventos del IAM Identity Center, sus fuentes de CloudTrail eventos y sus coincidencias. APIs Consulte las [referencias de la API del IAM Identity Center](#) para obtener más información sobre. APIs

 Note

Existe un grupo adicional de CloudTrail eventos, denominado inicio de sesión, que se AWS emite al iniciar sesión AWS como usuario del IAM Identity Center. Estos eventos no tienen un público coincidente y APIs, por lo tanto, no aparecen en las referencias de la API.

| CloudTrail eventos                           | Público APIs                                 | Description (Descripción)                                                                                                                                                                                                     | CloudTrail fuentes de eventos                            |
|----------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <a href="#">Centro de identidades de IAM</a> | <a href="#">Centro de identidades de IAM</a> | El Centro de Identidad de IAM APIs permite la gestión de conjuntos de permisos, aplicaciones, emisores de tokens de confianza, asignaciones de cuentas y aplicaciones, instancias del Centro de Identidad de IAM y etiquetas. | sso.amazonaws.com                                        |
| <a href="#">Almacén de identidades</a>       | <a href="#">Tienda de identidades</a>        | El almacén de identidades APIs permite gestionar el ciclo de vida de los usuarios y grupos de su fuerza laboral, así como de las membresías de los grupos de usuarios.                                                        | sso-directory.amazonaws.com, identitystore.amazonaws.com |



| CloudTrail eventos                   | Público APIs                         | Description (Descripción)                                                                                                                                                   | CloudTrail fuentes de eventos               |
|--------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
|                                      |                                      | Además, admiten la administración de los dispositivos MFA de los usuarios.                                                                                                  |                                             |
| <a href="#">OIDC</a>                 | <a href="#">OIDC</a>                 | El OIDC APIs admite la propagación confiable de identidad y el inicio de sesión y los kits de herramientas IDE como AWS CLI usuario del IAM Identity Center ya autenticado. | sso.amazonaws.com , sso-oauth.amazonaws.com |
| <a href="#">AWS portal de acceso</a> | <a href="#">AWS portal de acceso</a> | El portal de AWS acceso APIs admite las operaciones del portal de AWS acceso y los usuarios obtienen las credenciales de las cuentas a través del AWS CLI.                  | sso.amazonaws.com                           |

| CloudTrail eventos          | Público APIs          | Description (Descripción)                                                                                                                                                                                                                               | CloudTrail fuentes de eventos    |
|-----------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <a href="#">SCIM</a>        | <a href="#">SCIM</a>  | El SCIM permite APIs el aprovisionamiento de usuarios, grupos y membresías a grupos mediante el protocolo SCIM. Para obtener más información, consulte <a href="#">Registrar las llamadas a la API SCIM de IAM Identity Center con AWS CloudTrail</a> . | identitystore-scim.amazonaws.com |
| <a href="#">AWS Sign-In</a> | No tiene API pública. | AWS Emite CloudTrail eventos de inicio de sesión para la autenticación de los usuarios y los flujos de federación al Centro de Identidad de IAM.                                                                                                        | signin.amazonaws.com             |

## Temas

- [CloudTrail casos de uso del IAM Identity Center](#)
- [La información del centro de identidad de IAM se encuentra en CloudTrail](#)

## CloudTrail casos de uso del IAM Identity Center

Los CloudTrail eventos que emite el Centro de Identidad de IAM pueden ser valiosos para una variedad de casos de uso. Las organizaciones pueden usar estos registros de eventos para monitorear y auditar el acceso de los usuarios y la actividad en su AWS entorno. Esto puede ayudar a los casos de uso relacionados con el cumplimiento, ya que los registros recopilan detalles sobre quién accede a qué recursos y cuándo. También puede utilizar los CloudTrail datos para

investigar incidentes, lo que permite a los equipos analizar las acciones de los usuarios y rastrear los comportamientos sospechosos. Además, el historial de eventos puede respaldar las iniciativas de solución de problemas, ya que proporciona visibilidad de los cambios realizados en los permisos y las configuraciones de los usuarios a lo largo del tiempo.

En las siguientes secciones se describen los casos de uso fundamentales que sirven de base a sus flujos de trabajo, como la auditoría, la investigación de incidentes y la solución de problemas.

Identificar al usuario en los eventos iniciados por CloudTrail los usuarios del IAM Identity Center

El Centro de Identidad de IAM emite dos CloudTrail campos que le permiten identificar al usuario del Centro de Identidad de IAM detrás de los CloudTrail eventos, como iniciar sesión en el Centro de Identidad de IAM o usar el portal de AWS acceso AWS CLI, incluida la administración de los dispositivos de MFA:

- **userId**: el identificador de usuario único e inmutable del almacén de identidades de una instancia de IAM Identity Center.
- **identityStoreArn**: el nombre de recurso de Amazon (ARN) del almacén de identidades que contiene el usuario.

Los **identityStoreArn** campos **userId** y se muestran en el **onBehalfOf** elemento anidado dentro del elemento, como se muestra en el [userIdentity](#) siguiente ejemplo de registro de eventos. CloudTrail Este registro de eventos muestra estos dos campos en un evento en el que el tipo de **userIdentity** es «IdentityCenterUser». También puede encontrar estos campos en los eventos de los usuarios autenticados de IAM Identity Center en los que el tipo de **userIdentity** es «Unknown». Sus flujos de trabajo deben aceptar ambos valores de tipo.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

 Tip

Le recomendamos que utilice `userId` y `identityStoreArn` para identificar al usuario responsable de los eventos del IAM Identity Center CloudTrail. Los campos `principalId` y `userName` y del elemento `userIdentity` ya no están disponibles. Si sus flujos de trabajo, como la auditoría o la respuesta a incidentes, dependen de tener acceso a ellos `username`, tiene dos opciones:

- Recupere el nombre de usuario del directorio de IAM Identity Center como se explica en [El nombre de usuario en los eventos de inicio de sesión CloudTrail](#).
- Obtenga el `UserName` que IAM Identity Center emite en el elemento `additionalEventData` en Iniciar sesión. Esta opción no requiere acceso al directorio de IAM Identity Center. Para obtener más información, consulte [El nombre de usuario en los eventos de inicio de sesión CloudTrail](#).

Para recuperar los detalles de un usuario, incluido el campo `username`, consulte el almacén de identidades con el ID de usuario y el ID del almacén de identidades como parámetros. Puede realizar esta acción mediante la solicitud de la API [DescribeUser](#) o mediante la CLI. El siguiente comando de la CLI es un ejemplo. Puede omitir el parámetro `region` si la instancia de IAM Identity Center se encuentra en la región predeterminada de la CLI.

```
aws identitystore describe-user \  
--identity-store-id d-1234567890 \  
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \  
--region your-region-id
```

Para determinar el valor del identificador del almacén de identidades para el comando de la CLI del ejemplo anterior, puede extraer el identificador del almacén de identidades del valor `identityStoreArn`. En el ARN de ejemplo `arn:aws:identitystore::111122223333:identitystore/d-1234567890`, el ID del almacén de identidades es `d-1234567890`. Como alternativa, puede localizar el ID del almacén de identidades accediendo a la pestaña Identity Store de la sección Configuración de la consola de IAM Identity Center.

Si va a automatizar la búsqueda de usuarios en el directorio de IAM Identity Center, le recomendamos que calcule la frecuencia de las búsquedas de usuarios y que tenga en cuenta el límite máximo de [IAM Identity Center en la API del almacén de identidades](#). El almacenamiento

en caché de los atributos de usuario recuperados puede ayudarle a mantenerse dentro del límite máximo.

## Correlación de eventos de usuario dentro de la misma sesión de usuario

El [AuthWorkflowID](#) campo emitido en los eventos de inicio de sesión permite rastrear todos los CloudTrail eventos asociados a una secuencia de inicio de sesión antes del comienzo de una sesión de usuario del IAM Identity Center.

Para las acciones de los usuarios dentro del portal de AWS acceso, el `credentialId` valor se establece en el ID de la sesión del usuario del Centro de Identidad de IAM utilizada para solicitar la acción. Puede utilizar este valor para identificar CloudTrail los eventos iniciados dentro de la misma sesión de usuario autenticada del IAM Identity Center en el AWS portal de acceso.

### Note

No se puede utilizar `credentialId` para correlacionar los eventos de inicio de sesión con los eventos posteriores, como el uso del portal de acceso de AWS . El valor del campo `credentialId` emitido en los eventos de inicio de sesión tiene un uso interno y le recomendamos que no confíe en él. El valor del `credentialId` campo emitido para los [eventos del portal de acceso de AWS](#) invocados con OIDC es igual al ID del token de acceso.

## Identificar los detalles de la sesión de fondo del usuario en los eventos iniciados por los usuarios del IAM Identity Center CloudTrail

El siguiente CloudTrail evento captura el proceso de intercambio de tokens OAuth 2.0, en el que un token de acceso existente (`elsubjectToken`) que representa la sesión interactiva del usuario se intercambia por un token de actualización (`elrequestedTokenType`). El token de actualización permite que cualquier tarea de larga duración que haya iniciado continúe ejecutándose con los permisos del usuario, incluso después de cerrar sesión.

En el caso de las [sesiones en segundo plano de los usuarios](#) del IAM Identity Center, el CloudTrail evento incluye un elemento adicional denominado «`resource` el `requestParameters` elemento». El parámetro `resource` contiene el nombre de recurso de Amazon (ARN) del trabajo que se ejecuta en segundo plano. Este elemento solo está presente en los registros de CloudTrail eventos y no se incluye en las respuestas del SDK o la API de [CreateTokenWithIAM](#) Identity Center.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

## Correlación de usuarios entre IAM Identity Center y directorios externos

IAM Identity Center proporciona dos atributos de usuario que puede utilizar para correlacionar un usuario de su directorio con el mismo usuario de un directorio externo (por ejemplo, Microsoft Active Directory y Okta Universal Directory).

- **externalId**: el identificador externo de un usuario de IAM Identity Center. Se recomienda asignar este identificador a un identificador de usuario inmutable en el directorio externo. Tenga en cuenta que el Centro de identidades de IAM no emite este valor en CloudTrail.
- **username**: un valor proporcionado por el cliente con el que los usuarios suelen iniciar sesión. El valor puede cambiar (por ejemplo, con una actualización de SCIM). Tenga en cuenta que cuando la fuente de identidad es Directory Service, el nombre de usuario que emite el Centro de Identidad de IAM CloudTrail coincide con el nombre de usuario que introduce para autenticarse. No es necesario que el nombre de usuario coincida exactamente con el nombre de usuario del directorio de IAM Identity Center.

Si tiene acceso a los CloudTrail eventos pero no al directorio del Centro de Identidad de IAM, puede utilizar el nombre de usuario que aparece en el elemento al iniciar sesión.

**additionalEventData** Para obtener más información sobre el nombre de usuario en **additionalEventData**, consulte [El nombre de usuario en los eventos de inicio de sesión CloudTrail](#).

La asignación de estos dos atributos de usuario a los atributos de usuario correspondientes en un directorio externo se define en IAM Identity Center cuando el origen de identidad es Directory Service. Para obtener información, consulte [Asignaciones de los atributos entre IAM Identity Center y el directorio de proveedores de identidad externos](#). Externo, IdPs que proporciona a los usuarios

con SCIM su propio mapeo. Incluso si utiliza el directorio de IAM Identity Center como origen de identidad, puede utilizar el atributo `externalId` para hacer una referencia cruzada de las entidades principales de seguridad con su directorio externo.

En la siguiente sección se explica cómo buscar a un usuario de IAM Identity Center mediante los atributos `username` y `externalId` del usuario.

### Visualización de un rol de IAM Identity Center por `username` y `externalId`

Para recuperar los atributos de usuario del directorio de IAM Identity Center para un nombre de usuario conocido, solicite primero el correspondiente `userId` mediante la solicitud de la API [GetUserId](#) y, a continuación, emita una solicitud de la API [DescribeUser](#), como se muestra en el ejemplo anterior. En el siguiente ejemplo se muestra cómo se puede recuperar un `userId` del almacén de identidades para un nombre de usuario específico. Puede omitir el parámetro `region` si su instancia de IAM Identity Center se encuentra en la región predeterminada con la CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Del mismo modo, puede utilizar el mismo mecanismo cuando conoce el atributo `externalId`. Actualice la ruta del atributo del ejemplo anterior con el valor `externalId` y el valor del atributo con la información específica de `externalId` que está buscando.

### Visualización del identificador seguro (SID) de un usuario en Microsoft Active Directory (AD) y `externalId`

En algunos casos, el IAM Identity Center emite el SID de un usuario en el `principalId` campo de los CloudTrail eventos, como los que emiten el portal de AWS acceso y el OIDC. APIs Estos casos se están eliminando gradualmente. Recomendamos que sus flujos de trabajo utilicen el atributo `AD objectguid` cuando necesite un identificador de usuario único de AD. Puede encontrar este valor en el atributo `externalId` del directorio de IAM Identity Center. Sin embargo, si sus flujos de trabajo requieren el uso del SID, recupere el valor de AD, ya que no está disponible en el Centro de identidades de IAM. APIs

[Correlación de eventos de usuario dentro de la misma sesión de usuario](#) describe cómo puede utilizar los campos `username` y `externalId` para correlacionar un usuario de IAM Identity Center con un usuario coincidente en un directorio externo. De forma predeterminada, IAM Identity Center asigna `externalId` al atributo `objectguid` de AD y esta asignación es fija. IAM Identity Center ofrece a los administradores la flexibilidad de mapear `username` de forma diferente a la que se asigna por defecto a `userprincipalname` en AD.

Puede ver estas asignaciones en la consola de IAM Identity Center. Vaya a la pestaña Origen de identidad de Configuración y seleccione Administrar la sincronización en el menú Acciones. En la sección Administrar la sincronización, seleccione el botón Ver asignaciones de atributos.

Si bien puede utilizar cualquier identificador de usuario único de AD disponible en IAM Identity Center para buscar un usuario en AD, le recomendamos que utilice `objectguid` en sus consultas, ya que es un identificador inmutable. El siguiente ejemplo muestra cómo consultar Microsoft AD con Powershell para recuperar un usuario utilizando el valor `objectguid` del usuario de `16809ecc-7225-4c20-ad98-30094aefdbca`. Una respuesta correcta a esta consulta incluye el SID del usuario.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

```
Get-ADUser `
-Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
-Properties *
```

La información del centro de identidad de IAM se encuentra en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en el Centro de Identidad de IAM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

 Note

Para obtener más información sobre la evolución de la identificación de los usuarios y el seguimiento de las acciones de los usuarios en CloudTrail los eventos, consulte la sección [Cambios importantes en CloudTrail los eventos del IAM Identity Center](#) en el blog AWS de seguridad.



Para obtener un registro continuo de los eventos en su centro de identidad Cuenta de AWS, incluidos los eventos del IAM Identity Center, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Cuando el CloudTrail registro está activado en su cuenta Cuenta de AWS, las llamadas a la API realizadas a las acciones del Centro de Identidad de IAM se registran en los archivos de registro. Los registros del IAM Identity Center se escriben junto con otros registros de AWS servicio en un archivo de registro. CloudTrail determina cuándo crear y escribir en un nuevo archivo en función del período de tiempo y del tamaño del archivo.

CloudTrail eventos para el centro de identidad de IAM compatible APIs

En las siguientes secciones se proporciona información sobre los CloudTrail eventos asociados a lo siguiente APIs que admite el Centro de identidades de IAM:

- [API de IAM Identity Center](#)
- [API del almacén de identidades](#)
- [API de OIDC](#)
- [AWS API del portal de acceso](#)
- [API de SCIM](#)

## CloudTrail eventos de las operaciones de la API de IAM Identity Center

La siguiente lista contiene los CloudTrail eventos que las operaciones públicas del IAM Identity Center emiten con la fuente de `sso.amazonaws.com` eventos. Para obtener más información sobre las operaciones de la API para IAM Identity Center, consulte [IAM Identity Center API Reference](#).

Puede encontrar eventos adicionales en las operaciones de la API CloudTrail de la consola de IAM Identity Center en las que se basa la consola. Para obtener más información sobre estas consolas APIs, consulte la [Referencia de autorización de servicios](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
-

[DeleteApplicationGrant](#)

- 

[DeleteInlinePolicyFromPermissionSet](#)

- 

[DeleteInstance](#)

- 

[DeleteInstanceAccessControlAttributeConfiguration](#)

- 

[DeletePermissionsBoundaryFromPermissionSet](#)

- 

[DeletePermissionSet](#)

- 

[DeleteTrustedTokenIssuer](#)

- 

[DescribeAccountAssignmentCreationStatus](#)[S](#)

- 

[DescribeAccountAssignmentDeletionStatus](#)

- 

[DescribeApplication](#)

- 

[DescribeApplicationAssignment](#)

- 

[DescribeApplicationProvider](#)

- 

[DescribeInstance](#)

- 

[DescribeInstanceAccessControlAttributeConfiguration](#)

-

[DescribePermissionSet](#)

- [DescribePermissionSetProvisioningStatus](#)
- [DescribeTrustedTokenIssuer](#)
- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
- [GetPermissionsBoundaryForPermissionSet](#)
- [ListAccountAssignmentCreationStatus](#)
- [ListAccountAssignmentDeletionStatus](#)
- [ListAccountAssignments](#)
- [ListAccountAssignmentsForPrincipal](#)
- [ListAccountsForProvisionedPermissionSet](#)

- [ListApplicationAccessScopes](#)
- [ListApplicationAssignments](#)
- [ListApplicationAssignmentsForPrincipal](#)
- [ListApplicationAuthenticationMethods](#)
- [ListApplicationGrants](#)
- [ListApplicationProviders](#)
- [ListApplications](#)
- [ListCustomerManagedPolicyReferencesInPermissionSet](#)
- [ListInstances](#)
- [ListManagedPoliciesInPermissionSet](#)
- [ListPermissionSetProvisioningStatus](#)
- [ListPermissionSets](#)
- [ListPermissionSetsProvisionedToAccount](#)
- [ListTagsForResource](#)
- [ListTrustedTokenIssuers](#)
-

[ProvisionPermissionSet](#)

- 

[PutApplicationAccessScope](#)

- 

[PutApplicationAssignmentConfiguration](#)

- 

[PutApplicationAuthenticationMethod](#)

- 

[PutApplicationGrant](#)

- 

[PutInlinePolicyToPermissionSet](#)

- 

[PutPermissionsBoundaryToPermissionSet](#)

- 

[TagResource](#)

- 

[UntagResource](#)

- 

[UpdateApplication](#)

- 

[UpdateInstance](#)

- 

[UpdateInstanceAccessControlAttributeConfiguration](#)

- 

[UpdatePermissionSet](#)

- 

[UpdateTrustedTokenIssuer](#)

CloudTrail eventos de las operaciones de la API de Identity Store

La siguiente lista contiene los CloudTrail eventos que las operaciones públicas del almacén de identidades emiten con la fuente de `identitystore.amazonaws.com` eventos. Para obtener más

información sobre las operaciones de la API del almacén de identidades, consulte [Identity Store API Reference](#).

Puede encontrar eventos adicionales en las operaciones CloudTrail de la API de la consola de Identity Store con la fuente de `sso-directory.amazonaws.com` eventos. Son APIs compatibles con la consola y el portal de AWS acceso. Si necesita detectar la aparición de una operación concreta, como añadir un miembro a un grupo, le recomendamos que considere utilizar tanto las operaciones de API públicas como las de consola. Para obtener más información sobre estas consolas APIs, consulte la [Referencia de autorización de servicio](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

## CloudTrail eventos de las operaciones de la API de OIDC

La siguiente lista contiene los CloudTrail eventos que emiten las operaciones públicas del OIDC. Para obtener más información sobre estas operaciones de la API de OIDC, consulte [OIDC API Reference](#).

- [CreateToken](#) (origen del evento sso.amazonaws.com)
- [CreateTokenWithIAM](#) (origen del evento sso-oauth.amazonaws.com)

## CloudTrail eventos de las operaciones de la AWS API del portal de acceso

La siguiente lista contiene los CloudTrail eventos que las operaciones de la API del portal de AWS acceso emiten con la fuente del sso.amazonaws.com evento. Las operaciones de API que se indican como no disponibles en la API pública respaldan las operaciones del portal de AWS acceso. El uso de la AWS CLI puede provocar la emisión de CloudTrail eventos tanto de las operaciones de la API del portal de AWS acceso público como de aquellos que no están disponibles en la API pública. Para obtener más información sobre las operaciones de la API del portal de AWS acceso público, consulta la [referencia de la API del portal de AWS acceso](#).

- [Authenticate](#)(No disponible en la API pública. Proporciona el inicio de sesión en el portal de AWS acceso.)
- [Federate](#) (No disponible en la API pública. Proporciona la federación en las aplicaciones).
- [ListAccountRoles](#)
- [ListAccounts](#)
- [ListApplications](#)(No disponible en la API pública. Proporciona los recursos asignados a los usuarios para mostrarlos en el portal de AWS acceso.)
- [ListProfilesForApplication](#)(No está disponible en la API pública. Proporciona metadatos de la aplicación para mostrarlos en el portal de AWS acceso.)
- [GetRoleCredentials](#)
- [Logout](#)

## CloudTrail eventos de las operaciones de la API SCIM

Para obtener más información sobre las operaciones de la API de SCIM públicas, consulte [AWS access portal API Reference](#).



## Información de identidad en los eventos del IAM Identity Center CloudTrail

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.
- Si la solicitud la realizó un usuario de IAM Identity Center. Si es así, los `identityStoreArn` campos `userId` y están disponibles en los CloudTrail eventos para identificar al usuario del Centro de Identidad de IAM que inició la solicitud. Para obtener más información, consulte [Identificar al usuario en los eventos iniciados por CloudTrail los usuarios del IAM Identity Center](#).

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

### Note

Actualmente, el Centro de identidades de IAM no emite CloudTrail eventos para el inicio de sesión de los usuarios en aplicaciones web AWS gestionadas (por ejemplo, Amazon SageMaker AI Studio) con la API de [OIDC](#). Estas aplicaciones web son un subconjunto de un conjunto más amplio de [the section called “AWS aplicaciones gestionadas”](#), que también incluye aplicaciones no web, como Amazon Athena SQL y Concesiones de acceso a Amazon S3.

## Descripción de los CloudTrail eventos del Centro de Identidad de IAM

Un registro de seguimiento es una configuración que permite la entrega de eventos a un bucket de Amazon S3 que especifique. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail los eventos no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico. Obtén información sobre el [contenido de un CloudTrail registro](#) en la Guía del CloudTrail usuario.

En este ejemplo, se muestra una entrada de CloudTrail registro que captura una `DescribePermissionsPolicies` acción realizada por un usuario de IAM (samadams) que interactúa con el IAM Identity Center:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIIJM2K4example",
        "userName": "samadams"
      },
      "eventTime": "2017-11-29T22:39:43Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "DescribePermissionsPolicies",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "permissionSetId": "ps-79a0dde74b95ed05"
      },
      "responseElements": null,
      "requestID": "319ac6a1-d556-11e7-a34f-69a333106015",
      "eventID": "a93a952b-13dd-4ae5-a156-d3ad6220b071",
      "readOnly": true,
      "resources": [

      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Este ejemplo muestra una entrada de CloudTrail registro que captura una `ListApplications` acción realizada por un usuario del Centro de Identidad de IAM en el portal de acceso: AWS

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "eventTime": "2017-11-29T18:48:28Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "ListApplications",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
      "eventID": "e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Este ejemplo muestra una entrada de CloudTrail registro que captura una CreateToken acción realizada por un usuario del IAM Identity Center que se autentica con el servicio OIDC del IAM Identity Center:

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
},
"eventTime": "2020-06-16T01:31:15Z",
"eventSource": "sso.amazonaws.com",
"eventName": "CreateToken",
"awsRegion": "us-east-1",
"sourceIPAddress": "203.0.113.0",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
"requestParameters": {
  "clientId": "clientid1234example",
  "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "grantType": "urn:ietf:params:oauth:grant-type:device_code",
  "deviceCode": "devicecode1234example"
},
"responseElements": {
  "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "tokenType": "Bearer",
  "expiresIn": 28800,
  "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "IdentityStoreId",
    "ARN": "d-1234567890"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

## Explicación de los eventos de inicio de sesión de IAM Identity Center

AWS CloudTrail registra los eventos de inicio de sesión correctos y fallidos para todas las fuentes de identidad del IAM Identity Center. Las identidades de origen de IAM Identity Center y Active Directory (AD Connector y AWS Managed Microsoft AD) incluyen eventos de inicio de sesión adicionales que

se capturan cada vez que se le pide a un usuario que resuelva un desafío o factor de credenciales específico, además del estado de esa solicitud de verificación de credenciales en particular. Solo después de que un usuario haya completado todos los desafíos de credenciales requeridos, el usuario iniciará sesión, lo que provocará que se registre un evento `UserAuthentication`.

En la siguiente tabla se muestran los nombres de los CloudTrail eventos de inicio de sesión del IAM Identity Center, su finalidad y su aplicabilidad a las distintas fuentes de identidad.

| Nombre de evento                    | Propósito del evento                                                                                                                                                                                                                                                                      | Aplicabilidad de la fuente de identidad                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <code>CredentialChallenge</code>    | Se utiliza para notificar que IAM Identity Center ha solicitado al usuario que resuelva un desafío de credenciales específico y puntualiza el <code>CredentialType</code> que se requiere (por ejemplo, <code>PASSWORD</code> o <code>TOTP</code> ).                                      | Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD |
| <code>CredentialVerification</code> | Se utiliza para notificar que el usuario ha intentado resolver una solicitud de <code>CredentialChallenge</code> específica y precisa si la credencial se ha realizado correctamente o no.                                                                                                | Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD |
| <code>UserAuthentication</code>     | Se utiliza para notificar que todos los requisitos de autenticación con los que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctamente. Si los usuarios no completan correctamente los desafíos de credenciales requeridos, no se registrará | Todas las fuentes de identidad                                                    |

| Nombre de evento | Propósito del evento | Aplicabilidad de la fuente de identidad |
|------------------|----------------------|-----------------------------------------|
|------------------|----------------------|-----------------------------------------|

ningún evento de *UserAuthentication* .

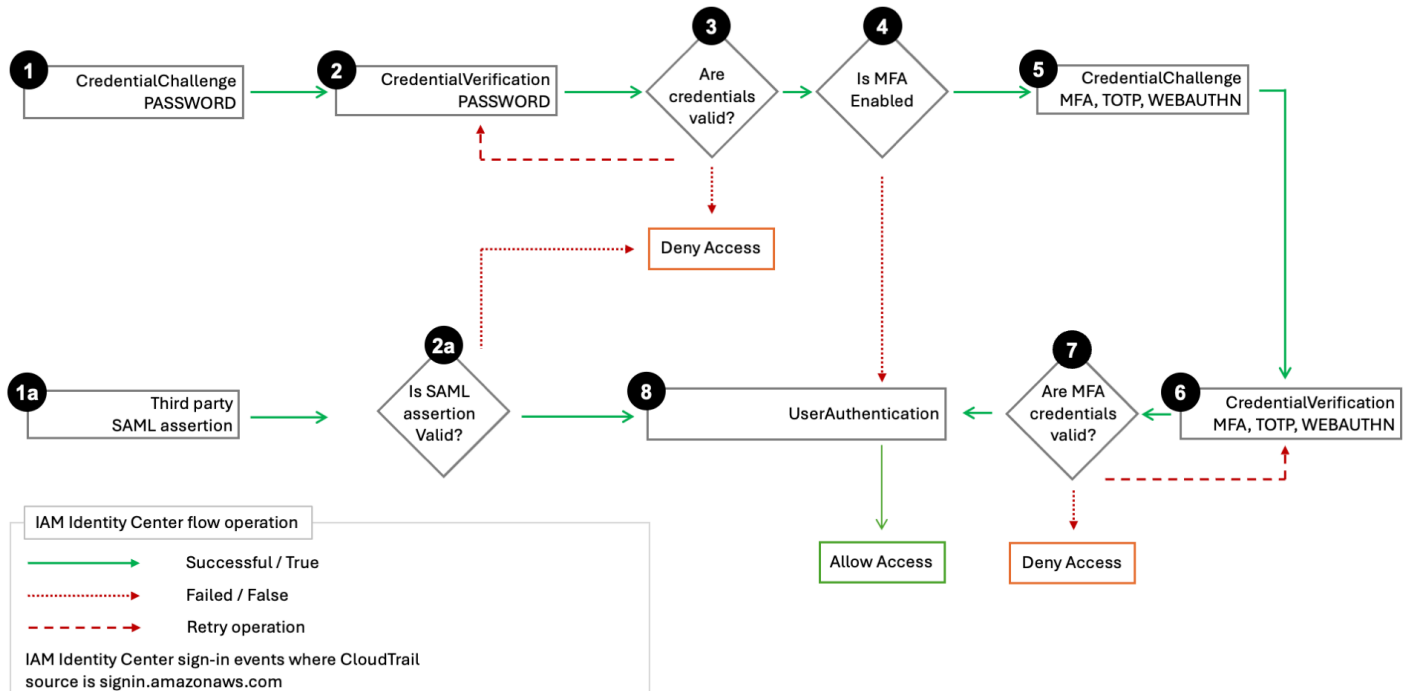
En la siguiente tabla, se muestran otros campos de datos de eventos útiles incluidos en eventos de inicio de sesión CloudTrail específicos.

| Campo          | Propósito del evento                                                                                                                                                                                                | Aplicabilidad al evento de inicio de sesión                     | Valores de ejemplo                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AuthWorkflowID | Se utiliza para correlacionar todos los eventos emitidos en una secuencia de inicio de sesión completa. Por cada inicio de sesión de usuario, IAM Identity Center puede emitir varios eventos.                      | CredentialChallenge, CredentialVerification, UserAuthentication | «AuthWorkflowID»: «9de74b32-8362-4a01-a524-de21df59fd83»                                                                                                         |
| CredentialType | Se utiliza para especificar la credencial o el factor que se ha cuestionado. Los eventos de UserAuthentication incluirán todos los valores de CredentialType que se hayan verificado correctamente a lo largo de la | CredentialChallenge, CredentialVerification, UserAuthentication | CredentialType«: «PASSWORD» o «: «PASSWORD, TOTP» (los valores posibles incluyen: PASSWORD, TOTP, WEBAUTHN, CredentialType EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP) |

| Campo                    | Propósito del evento                                                                                                                                                   | Aplicabilidad al evento de inicio de sesión | Valores de ejemplo                                       |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|----------------------------------------------------------|
|                          | secuencia de inicio de sesión del usuario.                                                                                                                             |                                             |                                                          |
| DeviceEnrollmentRequired | Se utiliza para especificar que el usuario debe registrar un dispositivo de MFA durante el inicio de sesión y que el usuario ha completado correctamente la solicitud. | UserAuthentication                          | "«: «verdadero» DeviceEnrollmentRequired"                |
| LoginTo                  | Se utiliza para especificar la ubicación de redireccionamiento tras una secuencia de inicio de sesión correcta.                                                        | UserAuthentication                          | "LoginTo": "https://mydirectory.awsapps.com/start/....." |

## CloudTrail eventos en los flujos de inicio de sesión del IAM Identity Center

El siguiente diagrama describe el flujo de inicio de sesión y los CloudTrail eventos que emite el inicio de sesión.



El diagrama muestra un flujo de inicio de sesión con contraseña y un flujo de inicio de sesión federado.

El flujo de inicio de sesión con contraseña, que consta de los pasos 1 a 8, muestra los pasos durante el proceso de inicio de sesión con nombre de usuario y contraseña. IAM Identity Center establece `userIdentity.additionalEventData.CredentialType` como «PASSWORD», e IAM Identity Center sigue el ciclo de desafío-respuesta de las credenciales y lo vuelve a intentar si es necesario.

El número de pasos depende del tipo de [inicio de sesión y de la presencia de la autenticación multifactor \(MFA\)](#). El proceso inicial da como resultado tres o cinco CloudTrail eventos y `UserAuthentication` finaliza la secuencia para que la autenticación se realice correctamente. Los intentos fallidos de autenticación con contraseña provocan CloudTrail eventos adicionales, ya que el Centro de Identidad de IAM vuelve a emitir la autenticación `CredentialChallenge` normal o, si está habilitada, la autenticación MFA.

El flujo de inicio de sesión con contraseña también cubre el escenario en el que un usuario de IAM Identity Center recién creado con una llamada a la API `CreateUser` inicia sesión con una contraseña de un solo uso (OTP). El tipo de credencial en este escenario es «EMAIL\_OTP».



El flujo de inicio de sesión federado, que consta de los pasos 1a, 2a y 8, muestra los pasos principales del proceso de autenticación federada, en los que un [proveedor de identidades proporciona una aserción de SAML](#), la valida IAM Identity Center y, si es correcta, se obtiene como resultado `UserAuthentication`. IAM Identity Center no invoca la secuencia de autenticación MFA interna en los pasos 3 a 7 porque un proveedor de identidades federado externo es responsable de toda la autenticación de credenciales de usuario.

El nombre de usuario en los eventos de inicio de sesión CloudTrail

IAM Identity Center emite el campo `UserName` situado debajo del elemento `additionalEventData` una vez por cada inicio de sesión correcto de un usuario de IAM Identity Center. En la siguiente lista se describen los dos eventos de inicio de sesión incluidos en el ámbito de aplicación y las condiciones en las que se producen. Solo una de las condiciones puede cumplirse cuando un usuario inicia sesión.

- `CredentialChallenge`
  - Cuando `CredentialType` es «PASSWORD»: se aplica a la autenticación por contraseña con Directory Service o Directorio de IAM Identity Center.
  - Cuando `CredentialType` es «EMAIL\_OTP»: solo se aplica Directorio de IAM Identity Center cuando un usuario creado con una llamada a la `CreateUser` API intenta iniciar sesión por primera vez y recibe una contraseña de un solo uso para iniciar sesión con esa contraseña una vez.
- `UserAuthentication`
  - Cuando `CredentialType` es «EXTERNAL\_IDP»: se aplica a la autenticación con un IdP externo.

El valor de `UserName` para que las autenticaciones se realicen correctamente es el siguiente:

- Cuando el origen de identidad es un IdP externo, el valor es igual al valor `nameID` de la aserción SAML entrante. Este valor es igual al campo `UserName` de Directorio de IAM Identity Center.
- Cuando la fuente de identidad es un Directorio de IAM Identity Center, el valor emitido es igual al `UserName` campo de este directorio.
- Cuando la fuente de identidad es la Directory Service, el valor emitido es igual al nombre de usuario que el usuario introduce durante la autenticación. Por ejemplo, un usuario que tiene el nombre de usuario `anyuser@company.com` puede autenticarse con

anyuseranyuser@company.com, o ycompany.com/anyuser, en cada caso, el valor introducido se emite CloudTrail respectivamente.

## Enmascaramiento de seguridad de los intentos incorrectos con el nombre de usuario

El `UserName` campo contiene la cadena `HIDDEN_DUE_TO_SECURITY_REASONS` cuando el evento registrado es un error de inicio de sesión en la consola provocado por una introducción incorrecta del nombre de usuario. CloudTrail en este caso, no graba el contenido porque el texto podría contener información confidencial, como se describe en los siguientes ejemplos:

- Un usuario escribe por error una contraseña en el campo de nombre de usuario.
- Un usuario escribe por error el nombre de una cuenta de correo electrónico personal, un identificador de inicio de sesión en un banco u otro identificador privado.

### Tip

Le recomendamos que utilice `userId` y `identityStoreArn` para identificar al usuario responsable de los CloudTrail eventos del IAM Identity Center. Si necesita usar el campo `userName`, puede usar el valor de `userName` en el elemento `additionalEventData` que se emite una vez por cada inicio de sesión correcto.

Para obtener información adicional sobre cómo usar el campo `UserName`, consulte [Correlación de eventos de usuario dentro de la misma sesión de usuario](#).

## Ejemplos de eventos para escenarios de inicio de sesión en IAM Identity Center

Los siguientes ejemplos ilustran las secuencias de CloudTrail eventos típicas generadas durante varios escenarios de inicio de AWS sesión. Estos ejemplos sirven como patrones de referencia para ayudarle a interpretar los registros de autenticación, identificar los problemas de seguridad y comprobar que las políticas de autenticación funcionan correctamente.

### Temas

- [Inicio de sesión correcto al autenticarse solo con contraseña](#)
- [Inicio de sesión correcto al autenticarse con un proveedor de identidad externo](#)
- [Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación con contraseña temporal de un solo uso \(TOTP\).](#)

- [Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado](#)
- [Error al iniciar sesión debido a una autenticación de contraseña incorrecta](#)

## Inicio de sesión correcto al autenticarse solo con contraseña

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión exitoso solo con contraseña.

### CredentialChallenge (Contraseña)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:33:58Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  },
  "requestID": "5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID": "27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
```

```

    "managementEvent":true,
    "eventCategory":"Management",
    "serviceEventDetails":{
      "CredentialChallenge":"Success"
    }
  }
}

```

## CredentialVerificationCorrecto (contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
    "CredentialType":"PASSWORD"
  },
  "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "recipientAccountId":"111122223333",

```

```

    "serviceEventDetails":{
      "CredentialVerification":"Success"
    }
  }
}

```

## UserAuthentication Correcto (solo contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo":"https://d-1234567890.awsapps.com/start/?state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIc50BAA6ftz73M6LsfLWDlf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType":"PASSWORD"
  },
  "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
  "readOnly":false,
  "eventType":"AwsServiceEvent",

```

```

    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "UserAuthentication":"Success"
    }
  }
}

```

Inicio de sesión correcto al autenticarse con un proveedor de identidad externo

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión correcto cuando se autentica mediante el protocolo SAML con un proveedor de identidad externo.

UserAuthentication Correcto (proveedor de identidad externo)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo":"https://d-1234567890.awsapps.com/start/?state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIc50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-

```

```
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
  "CredentialType": "EXTERNAL_IDP",
  "UserName": "bobsmith@example.com"
},
"requestID": "f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
"eventID": "e959a95a-2b33-478d-906c-4fe303e8a9f1",
"readOnly": false,
"eventType": "AwsServiceEvent",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333",
"serviceEventDetails": {
  "UserAuthentication": "Success"
}
}
```

Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación con contraseña temporal de un solo uso (TOTP).

La siguiente secuencia de eventos captura un ejemplo en el que se requería una autenticación multifactorial durante el inicio de sesión y el usuario inició sesión correctamente con una contraseña y una aplicación de autenticación TOTP.

### CredentialChallenge (Contraseña)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime": "2020-12-08T20:40:13Z",
"eventSource": "signin.amazonaws.com",
"eventName": "CredentialChallenge",
```

```

"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
  "CredentialType":"PASSWORD",
  "UserName":"bobsmith@example.com"
},
"requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
"eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

### CredentialVerificationCorrecto (contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:20Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",

```



```

    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType": "PASSWORD"
    },
    "requestID": "92c4ac90-0d9b-452d-95d5-728487612f5e",
    "eventID": "4533fd49-6669-4d0b-b272-a0b2139309a8",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "CredentialVerification": "Success"
    }
  }
}

```

## CredentialChallenge (TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime": "2020-12-08T20:40:20Z",
"eventSource": "signin.amazonaws.com",
"eventName": "CredentialChallenge",
"awsRegion": "us-east-1",
"sourceIPAddress": "203.0.113.0",

```

```

    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
        "CredentialType": "TOTP"
    },
    "requestID": "92c4ac90-0d9b-452d-95d5-728487612f5e",
    "eventID": "29202f08-f240-40cc-b789-c0cea8a27847",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "CredentialChallenge": "Success"
    }
}

```

## Exitoso CredentialVerification (TOTP)

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",
        "accessKeyId": "",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
    },
    "eventTime": "2020-12-08T20:40:27Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",

```

```

"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
  "CredentialType":"TOTP"
},
"requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
"eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialVerification":"Success"
}
}

```

## Exitoso UserAuthentication (contraseña + TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:27Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,

```

```

"additionalEventData":{
  "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
  "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMLui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
  "CredentialType":"PASSWORD,TOTP"
},
"requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
"eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "UserAuthentication":"Success"
}
}

```

Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado

La siguiente secuencia de eventos demuestra una autenticación de contraseña correcta en la que el usuario debía registrarse y completar correctamente la autenticación multifactor (MFA) antes de finalizar su proceso de inicio de sesión.

### CredentialChallenge (Contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    }
  }
}

```

```

    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-09T01:24:02Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialChallenge",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "CredentialType":"PASSWORD",
    "UserName":"bobsmith@example.com"
  },
  "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
  "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "recipientAccountId":"111122223333",
  "serviceEventDetails":{
    "CredentialChallenge":"Success"
  }
}

```

### CredentialVerificationCorrecto (contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    }
  },

```

```

    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-09T01:24:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "CredentialType":"PASSWORD"
  },
  "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
  "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "recipientAccountId":"111122223333",
  "serviceEventDetails":{
    "CredentialVerification":"Success"
  }
}

```

Exitoso UserAuthentication (se requiere contraseña y registro en MFA)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
}

```

```

    "eventTime": "2020-12-09T01:24:14Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo": "https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNNQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiquYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType": "PASSWORD",
      "DeviceEnrollmentRequired": "true"
    },
    "requestID": "74d24604-a365-4237-8c4a-350795494b92",
    "eventID": "a15bf257-7f37-46c0-b67c-fea5fa6166be",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "UserAuthentication": "Success"
    }
  }
}

```

## Error al iniciar sesión debido a una autenticación de contraseña incorrecta

La siguiente secuencia de eventos muestra un intento de autenticación en el que el usuario ingresó correctamente su nombre de usuario, pero no pasó el paso de verificación de la contraseña, lo que provocó un inicio de sesión incorrecto.

### CredentialChallenge (Contraseña)

```
{
```

```

"eventVersion":"1.08",
"userIdentity":{
  "type":"Unknown",
  "arn":"",
  "accountId":"111122223333",
  "accessKeyId":"",
},
"eventTime":"2020-12-08T18:56:15Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialChallenge",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
  "CredentialType":"PASSWORD",
  "UserName":"bobsmith@example.com"
},
"requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
"eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

## Error CredentialVerification (contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
  },

```



```
"eventTime":"2020-12-08T18:56:21Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialVerification",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{"
  "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
  "CredentialType":"PASSWORD"
},
"requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
"eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{"
  "CredentialVerification":"Failure"
}
}
```

## Registrar las llamadas a la API SCIM de IAM Identity Center con AWS CloudTrail

[IAM Identity Center SCIM](#) está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un. Servicio de AWS CloudTrail captura las llamadas a la API del SCIM como eventos. Con la información recopilada por CloudTrail, puede determinar la información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

### Note

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Sin embargo, es posible que tenga que rotar su token de acceso para ver los eventos de SCIM, si su token se creó antes de septiembre de 2024.

Para obtener más información, consulte [Rotar un token de acceso](#).

SCIM admite el registro de las siguientes operaciones como eventos en CloudTrail:

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroup](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

## Ejemplos CloudTrail de eventos

Los siguientes ejemplos muestran los registros de CloudTrail eventos típicos generados durante las operaciones de SCIM con el IAM Identity Center. Estos ejemplos muestran la estructura y el contenido de los eventos para que las operaciones se realicen correctamente y los escenarios de error más comunes, lo que le ayuda a entender cómo interpretar los CloudTrail registros a la hora de solucionar problemas de aprovisionamiento del SCIM.

### Operación de **CreateUser** exitosa

Este CloudTrail evento muestra una `CreateUser` operación realizada correctamente a través de la API SCIM. El evento captura tanto los parámetros de la solicitud (ocultando la información confidencial) como los elementos de respuesta, incluido el ID del usuario recién creado. Este tipo de evento se genera cuando un proveedor de identidades aprovisiona correctamente un nuevo usuario a IAM Identity Center mediante el protocolo SCIM.

```
{
```

```

"eventVersion": "1.10",
"userIdentity": {
  "type": "WebIdentityUser",
  "accountId": "123456789012",
  "accessKeyId": "xxxx"
},
"eventTime": "xxxx",
"eventSource": "identitystore-scim.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "us-east-1",
"sourceIPAddress": "xx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": {
  "meta" : {
    "created" : "Oct 10, 2024, 1:23:45 PM",
    "lastModified" : "Oct 10, 2024, 1:23:45 PM",
    "resourceType" : "User"
  },
  "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
  "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "name": {
    "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "active": true,
  "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
  "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
}

```

```

},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Operación de **PatchGroup** fallida: falta el atributo de ruta obligatorio

Este CloudTrail evento muestra una PatchGroup operación fallida que dio lugar a un ValidationException mensaje "Missing path in PATCH request" de error. El error se produjo porque la operación PATCH requiere un atributo de ruta para especificar qué atributo de grupo se debe modificar, pero este atributo no aparecía en la solicitud.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ]
    }
  },

```

```

    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ],
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

Operación de **CreateGroup** fallida: el nombre del grupo ya existe

Este CloudTrail evento muestra una CreateGroup operación fallida que dio lugar a un mensaje de error `ConflictException` con el mensaje de error `"Duplicate GroupDisplayName"`. Este error se produce al intentar crear un grupo con un nombre para mostrar que ya existe en IAM Identity Center. El proveedor de identidades debe utilizar un nombre de grupo único o actualizar el grupo existente en lugar de crear otro nuevo.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",

```

```
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}
```

### Operación de **PatchUser** fallida: no se admiten varias direcciones de correo electrónico

Este CloudTrail evento muestra una PatchUser operación fallida que dio lugar a un mensaje de error ValidationException con el mensaje de error "List attribute emails exceeds allowed limit of 1". Este error se produce al intentar asignar varias direcciones de correo electrónico a un usuario, ya que IAM Identity Center solo admite una dirección de correo electrónico por usuario. El proveedor de identidades debe configurar el mapeo SCIM para enviar solo una dirección de correo electrónico para cada usuario.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
}
```

```

"requestParameters": {
  "httpBody": {
    "operations": [
      {
        "op": "REPLACE",
        "path": "emails",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ],
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

## Errores comunes de validación de la API de SCIM en IAM Identity Center

Los siguientes mensajes de error de validación suelen aparecer en CloudTrail los eventos cuando se utiliza la API SCIM con el IAM Identity Center. Estos errores de validación suelen producirse durante las operaciones de aprovisionamiento de usuarios y grupos.

Para obtener una guía detallada sobre cómo resolver estos errores y configurar correctamente el aprovisionamiento de SCIM, consulte este [artículo de AWS re:Post](#).

- El correo electrónico con el atributo de la lista supera el límite permitido de 1
- El límite permitido de direcciones de atributos de lista es de 1
- Se detectó un error de validación: el valor de `*name.familyName*` no cumplía la restricción: el miembro debe cumplir el patrón de expresión regular: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

- Se detectaron dos errores de validación: el valor de 'name.familyName' no pudo cumplir la restricción: el miembro debe tener una longitud mayor o igual a 1; el valor de 'name.familyName' no pudo cumplir la restricción: el miembro debe cumplir el patrón de expresión regular: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`
- Se detectaron dos errores de validación: el valor de 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' no cumplía la restricción: el miembro debe tener una longitud mayor o igual a 1; el valor en 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' no pudo cumplir la restricción: el miembro debe cumplir con la expresión regular patrón: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`,
- JSON no válido de RequestBody
- Formato de filtro no válido

## Connect los componentes de la aplicación con Amazon EventBridge

Puede integrar IAM Identity Center con [Amazon EventBridge](#) para generar eventos que inicien notificaciones administrativas o invocar flujos de trabajo automatizados en respuesta a acciones específicas del IAM Identity Center registradas en eventos. CloudTrail

Por ejemplo, puede configurar [EventBridge reglas](#) para detectar cuándo un usuario elimina una aplicación o cuándo el Centro de Identidad de IAM crea un grupo nuevo. [Según su caso de uso, puede dirigir estos eventos a un tema de Amazon SNS para notificarlos a los administradores o invocar una automatización adicional mediante Step AWS Lambda Functions u otros EventBridge servicios compatibles.](#)

## Registro de errores de sincronización de AD configurable

Puede activar el registro en las configuraciones de su sincronización de Active Directory (AD) configurable para recibir registros con información sobre los errores que pueden producirse durante el proceso de sincronización. Con estos registros, puede supervisar si hay algún problema con la sincronización de AD configurable y tomar las medidas necesarias. Puede enviar sus registros a un grupo de registros de Amazon CloudWatch Logs, a un depósito de Amazon Simple Storage Service (Amazon S3) o a un Amazon Data Firehose, y se admite la entrega entre cuentas para los depósitos de Amazon S3 y Firehose.

[Para obtener más información sobre las limitaciones, los permisos y los registros vendidos, consulte Habilitar el registro desde. Servicios de AWS](#)



 Note

Se le cobrará el registro. Para obtener más información, consulta [Vended Logs](#) en la página de [CloudWatch precios de Amazon](#).

## Para habilitar los registros de errores de la sincronización de AD configurable

1. Inicie sesión en la [consola del IAM Identity Center](#).
2. Seleccione Configuración.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Seleccione Agregar entrega de registros y uno de los siguientes tipos de destino.
  - a. Elige Amazon CloudWatch Logs. A continuación, seleccione o introduzca el grupo de registro de destino.
  - b. Seleccione A Amazon S3. A continuación, elija o introduzca el bucket de destino.
  - c. Seleccione A Firehose. A continuación, seleccione o introduzca el flujo de entrega de destino.
5. Seleccione Enviar.

## Para los registros de errores de sincronización de AD configurable

1. Inicie sesión en la [consola del IAM Identity Center](#).
2. Seleccione Configuración.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Seleccione Eliminar para el destino que desea eliminar.
5. Seleccione Enviar.

## Campos de registro de errores de sincronización de AD configurable

Consulte la siguiente lista para ver los posibles campos del registro de errores.

## `sync_profile_name`

El nombre del perfil de sincronización.

## `error_code`

El código de error que representa el tipo de error que se ha producido.

## `error_message`

Un mensaje que contiene información detallada sobre el error que se ha producido.

## `sync_source`

La fuente de sincronización es el lugar desde el que se sincronizan las entidades. En el caso del IAM Identity Center, se trata de un Active Directory (AD) gestionado por Directory Service. La fuente de sincronización contiene el dominio y el ARN del directorio afectado.

## `sync_target`

El destino de sincronización es el destino en el que se guardan las entidades. En el caso del IAM Identity Center, se trata de un almacén de identidades. El destino de sincronización contiene el ARN del almacén de identidades afectado.

## `source_entity_id`

Un identificador único para la entidad que está causando el error. En el caso del IAM Identity Center, este es el SID de la entidad.

## `source_entity_type`

El tipo de entidad que está causando el error. El valor puede ser USER o GROUP.

## `eventTimestamp`

La fecha y hora en que se produjo el error.

## Ejemplos de registros de errores de sincronización de AD configurable

Ejemplo 1: Un registro de errores de una contraseña caducada de un directorio de AD

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "InvalidDirectoryCredentials",
```

```

    "error_message": "The password for your AD directory has expired. Please reset
the password to allow Identity Sync to access the directory."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "eventTimestamp": "1683355579981"
}

```

Ejemplo 2: Un registro de errores para un usuario con un nombre de usuario que no es único

```

{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "ConflictError",
    "error_message": "The source entity has a username conflict with the sync
target. Please verify that the source identity has a unique username in the target."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "sync_target": {
    "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
  },
  "source_entity_id": "SID-1234",
  "source_entity_type": "USER",
  "eventTimestamp": "1683355579981"
}

```

## Validación de la conformidad en IAM Identity Center

Los auditores externos evalúan la seguridad y el cumplimiento de Servicios de AWS dichos programas, por ejemplo AWS IAM Identity Center , como parte de varios programas de AWS cumplimiento.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa](#) de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

## Estándares de conformidad admitidos

IAM Identity Center ha sido sometido a auditorías para los siguientes estándares y puede utilizarse en soluciones para las que se exija certificación de conformidad.



AWS [ha ampliado su programa de cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud \(HIPAA\)](#) para incluir el Centro de Identidad de IAM como un servicio que cumple con los requisitos de la HIPAA.

AWS ofrece un [documento técnico centrado en la HIPAA](#) para los clientes que desean obtener más información sobre cómo procesar y almacenar la información de salud. Servicios de AWS Para obtener más información, consulte [Conformidad con HIPAA](#).



El Programa de Asesores Registrados de Seguridad de la Información (IRAP) permite a los clientes del Gobierno australiano garantizar que existen controles apropiados, así como determinar el modelo de responsabilidad adecuado para abordar los requisitos del Manual de Seguridad de la Información (ISM) del Gobierno australiano, elaborado por el Centro Australiano de Ciberseguridad (ACSC). Para obtener más información, consulte [Recursos de IRAP](#).



IAM Identity Center dispone de una declaración de conformidad para el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) versión 3.2 de nivel de proveedor de servicios 1.

Los clientes que utilizan AWS productos y servicios para almacenar, procesar o transmitir datos de titulares de tarjetas pueden utilizar las siguientes fuentes de identidad en el Centro de Identidad de IAM para gestionar su propia certificación de conformidad con la PCI DSS:

- Active Directory
- Proveedor de identidades externo

La fuente de identidad de IAM Identity Center actualmente no cumple con el estándar PCI DSS.

Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Compliance Package, consulte [PCI](#) DSS nivel 1.



Los informes de control de organizaciones y sistemas (SOC) son informes de análisis independientes de terceros que muestran cómo IAM Identity Center cumple los controles y objetivos clave de conformidad. Estos informes ayudan tanto a sus auditores como a usted a comprender cómo los controles respaldan las operaciones y la conformidad. Existen 3 tipos de informes de SOC:

- AWS Informe SOC 1: [Descargar con Artifact AWS](#)
- AWS SOC 2: Informe de seguridad, disponibilidad y confidencialidad: [descarga con Artifact AWS](#)
- [AWS SOC 3: Informe de seguridad, disponibilidad y confidencialidad](#)

El IAM Identity Center está dentro del ámbito de aplicación de los AWS informes SOC 1, SOC 2 y SOC 3. Para obtener más información, consulte [Conformidad con SOC](#).

## Resiliencia en IAM Identity Center

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura global.AWS](#)

Para obtener más información sobre AWS IAM Identity Center la resiliencia, consulte [Diseño de resiliencia y comportamiento regional](#).

# Seguridad de la infraestructura en IAM Identity Center

Como servicio gestionado, AWS IAM Identity Center está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utilice las llamadas a la API AWS publicadas para acceder al IAM Identity Center a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

# Protección de datos en IAM Identity Center

El [modelo de responsabilidad AWS compartida](#) se aplica a la protección de datos en AWS IAM Identity Center. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la AWS nube. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de datos, consulte [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación del blog [AWS Shared Responsibility Model and GDPR](#) en el Blog de seguridad de AWS .

Recomendamos que proteja sus datos de las siguientes formas:

- Utilice la autenticación multifactor (MFA) con IAM Identity Center.
- Use TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS IAM Identity Center u otros AWS servicios que utilizan la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de diagnóstico.

## Cifrado en tránsito

IAM Identity Center protege los datos en tránsito, a medida que viajan hacia y desde el servicio, cifrando automáticamente todos los datos entre redes mediante el protocolo de cifrado seguridad de la capa de transporte (TLS) 1.2 o TLS 1.3. Las solicitudes HTTPS directas autenticadas con IAM y enviadas al Centro de Identidad de IAM APIs, a la API Identity Store o a la API de OIDC se firman mediante el [algoritmo AWS Signature versión 4](#) para establecer una conexión segura.



## Privacidad de datos

Con IAM Identity Center, mantendrá el control de los datos de su organización. Las identidades de usuario y grupo almacenadas en el Centro de Identidad de IAM se comparten con otros AWS servicios, como [las aplicaciones AWS gestionadas](#), solo si las habilita con el Centro de Identidad de IAM y si dichos servicios las necesitan.

Para obtener información adicional, consulte las [preguntas frecuentes sobre la privacidad de los datos de AWS](#).

## Retención de datos

IAM Identity Center almacena sus datos, como las identidades de usuarios y grupos, y los metadatos hasta que los elimine del servicio. Al eliminar una instancia de IAM Identity Center, también se eliminan los datos que contiene.

## Cifrado en reposo

IAM Identity Center proporciona cifrado para proteger los datos en reposo de los clientes usando los siguientes tipos de claves:

- Claves propiedad de AWS (tipo de clave predeterminado): el Centro de identidad de IAM utiliza estas claves de forma predeterminada para cifrar automáticamente los datos. No puede ver, gestionar, auditar su uso ni utilizar las claves AWS propias para otros fines. IAM Identity Center gestiona completamente la administración de claves para mantener sus datos seguros, sin que tenga que realizar ninguna acción. Para obtener más información, consulte [AWS owned keys](#) en la [Guía para desarrolladores de AWS Key Management Service](#).
- Claves administradas por el cliente: en las instancias de organización de IAM Identity Center, puede elegir una clave simétrica administrada por el cliente para cifrar el resto de los datos de identidad de su personal, como los atributos de usuario y grupo. Usted crea, posee y administra estas claves de cifrado. Como usted tiene el control total de esta capa de cifrado, puede realizar tareas como las siguientes:
  - Establecer y mantener políticas clave para restringir el acceso a la clave solo a los directores de IAM que necesiten acceder, como el IAM Identity Center, y [AWS aplicaciones gestionadas](#) al mismo tiempo AWS Organizations a sus administradores.
  - Establecer y mantener las políticas de IAM para el acceso a la clave, incluido el acceso entre cuentas

- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Auditar el acceso a sus datos que requiere un acceso a la clave
- Adición de etiquetas de
- Crear alias de clave
- Programar la eliminación de claves

Para obtener información sobre cómo implementar una clave KMS administrada por el cliente en IAM Identity Center, consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#). Para obtener más información acerca de las claves administradas por el cliente, consulte [customer managed key](#) en la Guía para desarrolladores de AWS Key Management Service .

 Note

El Centro de Identidad de IAM permite automáticamente el cifrado en reposo mediante claves KMS AWS propias para proteger los datos de los clientes sin coste alguno. Sin embargo, se aplican AWS KMS cargos cuando se utiliza una clave gestionada por el cliente. Para obtener más información acerca de los precios, consulte [Precios de AWS Key Management Service](#).

Consideraciones a la hora de implementar claves administradas por el cliente:

- Claves dedicadas: recomendamos crear una nueva clave de KMS dedicada y administrada por el cliente para cada instancia del IAM Identity Center, en lugar de reutilizar una clave existente. Este enfoque proporciona una separación de funciones más clara, simplifica la gestión del control de acceso y facilita las auditorías de seguridad. Tener una clave dedicada también reduce el riesgo al limitar el impacto de los cambios clave a una sola instancia del IAM Identity Center.
- Uso del Centro de Identidad de IAM en varias instancias Regiones de AWS: si planea replicar su instancia del Centro de Identidad de IAM en varias instancias Regiones de AWS, necesitará usar una clave KMS administrada por el cliente para el cifrado en reposo. El tipo de clave KMS de AWS propiedad predeterminada no se admite en un centro de identidad de IAM multirregional. Para obtener más información, consulte [Uso del Centro de Identidad de IAM en varios Regiones de AWS](#).

**Note**

IAM Identity Center utiliza el [cifrado de sobre](#) para cifrar los datos de identidad de su personal. Su clave de KMS desempeña el rol de clave de empaquetado que cifra la clave de datos que realmente se utiliza para cifrar los datos.

Para obtener más información sobre AWS KMS, consulte [¿Qué es el servicio de administración de AWS claves?](#)

## Contexto de cifrado de IAM Identity Center

Un [contexto de cifrado](#) es un conjunto opcional de pares clave-valor no secretos que contienen información contextual adicional sobre los datos. AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud. Para obtener más información sobre el cifrado, consulte la [Guía para desarrolladores de AWS KMS](#).

El Centro de identidades de IAM utiliza las siguientes claves de contexto de cifrado: `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn` y `tenant-key-id`. [Por ejemplo, el AWS KMS siguiente contexto de cifrado puede aparecer en las operaciones de API invocadas por la API de IAM Identity Center.](#)

```
"encryptionContext": {  
  "tenant-key-id": "ssoins-1234567890abcdef",  
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"  
}
```

El siguiente contexto de cifrado puede aparecer en las operaciones de AWS KMS API invocadas por la [API Identity Store](#).

```
"encryptionContext": {  
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",  
  "aws:identitystore:identitystore-arn":  
    "arn:aws:identitystore:::123456789012:identitystore/d-1234567890"  
}
```

## Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente

Puede utilizar el contexto de cifrado en políticas de claves y políticas de IAM como condiciones para controlar el acceso a su clave simétrica administrada por el cliente. Algunas de las plantillas de políticas de claves en [Instrucciones de política de claves de KMS avanzadas](#) incluyen estas condiciones para garantizar que la clave se utilice únicamente con una instancia específica de IAM Identity Center.

## Supervisión de claves de cifrado para IAM Identity Center

Cuando utilizas una clave de KMS gestionada por el cliente con tu instancia del Centro de Identidad de IAM, puedes utilizar [AWS CloudTrailAmazon CloudWatch Logs](#) para realizar un seguimiento de las solicitudes que envía el Centro de Identidad de IAM. AWS KMS En ella se enumeran las operaciones de la API de KMS a las que llama el Centro de Identidad de IAM. [Paso 2: prepare las instrucciones de política de claves de KMS](#) CloudTrail los eventos de estas operaciones de API contienen el contexto de cifrado, que le permite supervisar las operaciones de la AWS KMS API a las que recurre su instancia del IAM Identity Center para acceder a los datos cifrados por la clave gestionada por el cliente.

Ejemplo de contexto de cifrado en el CloudTrail caso de una operación de AWS KMS API:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxxxx"
    }
  }
}
```

## AWS el almacenamiento, el cifrado y la eliminación de los atributos de identidad del IAM Identity Center por parte de las aplicaciones gestionadas

Algunas aplicaciones AWS gestionadas con las que se despliega AWS IAM Identity Center, como AWS Systems Manager y Amazon CodeCatalyst, almacenan atributos específicos de usuarios y grupos del IAM Identity Center en su propio almacén de datos. El cifrado en reposo con una clave KMS gestionada por el cliente en el Centro de Identidad de IAM no se extiende a los atributos de

usuario y grupo del Centro de Identidad de IAM almacenados en AWS las aplicaciones gestionadas. AWS las aplicaciones gestionadas admiten distintos métodos de cifrado para los datos que almacenan. Por último, al eliminar los atributos de usuario y grupo en el Centro de Identidad de IAM, estas aplicaciones AWS gestionadas pueden seguir almacenando esta información después de su eliminación en el Centro de Identidad de IAM. Consulte la guía del usuario de las aplicaciones AWS gestionadas para obtener información sobre el cifrado y la seguridad de los datos almacenados en las aplicaciones.

## Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center

Las claves administradas por el cliente son AWS claves del Servicio de administración de claves que usted crea, posee y administra. Para implementar una clave KMS gestionada por el cliente para el cifrado en reposo en el Centro de Identidad de AWS IAM, siga estos pasos:

### Important

Algunas aplicaciones AWS gestionadas no se pueden utilizar con el centro de identidad de AWS IAM configurado con una clave KMS gestionada por el cliente. Consulte [AWS aplicaciones gestionadas que puede utilizar con IAM Identity Center](#).

1. [Paso 1: identifique los casos de uso de su organización](#): con el fin de definir los permisos correctos para el uso de la clave KMS, debe identificar los casos de uso relevantes en su organización. Los permisos clave de KMS consisten en instrucciones de política de claves de KMS y políticas basadas en la identidad que funcionan de forma conjunta para permitir que los responsables de IAM correspondientes utilicen la clave de KMS para sus casos de uso específicos.
2. [Paso 2: prepare las instrucciones de política de claves de KMS](#): elija las plantillas de instrucciones de políticas de claves de KMS pertinentes en función de los casos de uso identificados en el paso 1 y rellene los identificadores obligatorios y los nombres de las entidades principales de IAM. Comience con las instrucciones de política de claves de KMS básicas y, si sus políticas de seguridad lo requieren, perfecciónelas como se describe en las declaraciones de política de claves de KMS avanzadas.
3. [Paso 3: cree una clave de KMS administrada por el cliente](#)- Cree una clave de KMS en AWS KMS que cumpla con los requisitos del centro de identidad de IAM y añada a la política clave de KMS las declaraciones de política clave de KMS preparadas en el paso 2.

4. [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#): elija las plantillas de instrucciones de políticas de IAM pertinentes en función de los casos de uso identificados en el paso 1 y prepárelas para su uso rellenando el ARN de clave. A continuación, permita que los directores de IAM de cada caso de uso específico utilicen la clave de KMS en todas las cuentas añadiendo las instrucciones de política de IAM preparadas a las políticas de IAM de las entidades principales.
5. [Paso 5: configure la clave de KMS en IAM Identity Center](#): active la clave de KMS administrada por el cliente en su instancia de IAM Identity Center para usarla como cifrado en reposo.

## Paso 1: identifique los casos de uso de su organización

Antes de crear y configurar su clave de KMS administrada por el cliente, identifique sus casos de uso y prepare los permisos de clave de KMS necesarios. Consulte la [Guía para desarrolladores de KMS de AWS](#) para obtener más información sobre la política de claves de KMS.

Los directores de IAM que llamen al servicio del Centro de Identidad de IAM necesitan permisos. APIs Por ejemplo, se puede autorizar a un administrador delegado a utilizarlos APIs mediante una política de conjuntos de permisos. Cuando el Centro de Identidad de IAM se configura con una clave gestionada por el cliente, los directores de IAM también deben tener permisos para usar la API de KMS a través del servicio del Centro de Identidad de IAM. APIs Estos permisos de la API de KMS se definen en dos lugares: en la política de claves de KMS y en las políticas de IAM asociadas a las entidades principales de IAM.

Los permisos clave de KMS consisten en:

1. Instrucciones de políticas de claves de KMS que se especifican en la clave de KMS durante su creación en [Paso 3: cree una clave de KMS administrada por el cliente](#).
2. Instrucciones de política de IAM para los directores de IAM que se especifican en [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#) después de crear la clave de KMS.

En la siguiente tabla se especifican los casos de uso relevantes y las entidades principales de IAM que necesitan permisos para usar la clave de KMS.

| Caso de uso                                                                                                                                                                                                                                                     | Las entidades principales de IAM que necesitan permisos para usar la clave de KMS                                                                                                                                                                                                   | Obligatorio/ opcional |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Uso del Centro de Identidad de IAM AWS                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>Administradores del centro de AWS identidad de IAM</li> <li>Servicio IAM Identity Center y servicio de almacén de identidades asociado</li> </ul>                                                                                            | Obligatorio           |
| Uso de aplicaciones AWS gestionadas con IAM Identity Center                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>Administradores de aplicaciones AWS gestionadas</li> <li>AWS aplicaciones gestionadas</li> <li><a href="#">Funciones de servicio</a> que las aplicaciones AWS gestionadas asumen para llamar al servicio IAM Identity Center APIs</li> </ul> | Opcional              |
| Se utiliza AWS Control Tower en la instancia del AWS IAM Identity Center que habilitó                                                                                                                                                                           | <ul style="list-style-type: none"> <li>AWS Control Tower administradores</li> </ul>                                                                                                                                                                                                 | Opcional              |
| SSO en instancias de Amazon EC2 AWS con IAM Identity Center                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>Los directores de IAM están autorizados a realizar el SSO en las instancias de Amazon EC2</li> </ul>                                                                                                                                         | Opcional              |
| Cualquier otro caso de uso que realice llamadas al servicio del Centro de Identidad de IAM APIs con los principios de IAM, como aplicaciones administradas por el cliente, conjuntos de permisos, flujos de trabajo de aprovisionamiento o funciones AWS Lambda | <ul style="list-style-type: none"> <li>Estos flujos de trabajo utilizan los principios de IAM para llamar al servicio del Centro de Identidad de IAM APIs</li> </ul>                                                                                                                | Opcional              |

 Note

Los principales de IAM que figuran en la tabla requieren permisos de la API de KMS. AWS Sin embargo, para proteger los datos de sus usuarios y grupos en el Centro de identidades de IAM, solo los servicios de IAM Identity Center e Identity Store llaman directamente a la API de KMS. AWS

## Paso 2: prepare las instrucciones de política de claves de KMS

Tras identificar los casos de uso relevantes para su organización, puede preparar las instrucciones de política de claves de KMS correspondientes.

1. Elija las instrucciones de política de claves de KMS que coincidan con los casos de uso de su organización. Comience con las plantillas de políticas básicas. Si necesita políticas más específicas en función de sus requisitos de seguridad, puede modificar las instrucciones de políticas mediante los ejemplos que se muestran en [Instrucciones de política de claves de KMS avanzadas](#). Para obtener orientación sobre esta decisión, consulte [Consideraciones a la hora de elegir las principales instrucciones de política de claves de KMS básicas o avanzadas](#). Además, cada sección de referencia en [Instrucciones básicas de KMS y políticas de IAM](#) incluye consideraciones relevantes.
2. Copie las políticas relevantes y envíelas a un editor e inserte los identificadores necesarios y los nombres de las entidades principales de IAM en las instrucciones de política de claves de KMS. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios](#).

A continuación se presentan las plantillas de políticas de referencia para cada caso de uso. Para utilizar una clave KMS, solo se necesita el primer conjunto de permisos del Centro de Identidad de AWS IAM. Le recomendamos que consulte las subsecciones correspondientes para obtener información adicional sobre casos de uso específicos.

- [Instrucciones de política de claves básicas de KMS para el uso de IAM Identity Center \(obligatorias\)](#)
- [Declaraciones básicas de política de IAM y clave de KMS para el uso de aplicaciones administradas AWS](#)
- [Declaración clave básica de KMS para el uso de AWS Control Tower](#)



- [Declaraciones básicas de política de IAM y clave de KMS para el uso del IAM Identity Center en las instancias de Amazon EC2](#)
- [Instrucciones básicas de políticas de IAM y de claves de KMS para el uso de flujos de trabajo personalizados con IAM Identity Center](#)

#### Important

Tenga cuidado al modificar las políticas de claves de KMS para las claves que ya utiliza IAM Identity Center. Si bien IAM Identity Center valida los permisos de cifrado y descifrado al configurar inicialmente una clave de KMS, no puede verificar los cambios de política posteriores. La eliminación inadvertida de los permisos necesarios podría interrumpir el funcionamiento normal de IAM Identity Center. Para obtener instrucciones sobre la solución de errores comunes relacionados con las claves administradas por el cliente en IAM Identity Center, consulte [Solucione los problemas de las claves administradas por el cliente en AWS IAM Identity Center](#).

#### Note

IAM Identity Center y su almacén de identidades asociado requieren permisos de nivel de servicio para utilizar la clave de KMS administrada por el cliente. Este requisito se extiende a las aplicaciones AWS gestionadas que llaman al servicio del Centro de Identidad de IAM APIs mediante credenciales de servicio. Para otros casos de uso en los que APIs se llama al servicio del Centro de Identidad de IAM con [sesiones de acceso directo](#), solo el responsable de IAM que lo inicia (por ejemplo, un administrador) necesita permisos clave de KMS. En particular, los usuarios finales que utilizan el portal de AWS acceso y las aplicaciones AWS gestionadas no necesitan permisos clave de KMS directos, ya que se conceden a través de los servicios correspondientes.

## Paso 3: cree una clave de KMS administrada por el cliente

Puede crear una clave gestionada por el cliente mediante la consola AWS de gestión o el AWS KMS APIs. Al crear la clave, añada las instrucciones de política de claves de KMS que preparó en el paso 2 a la política de claves de KMS. Para obtener instrucciones detalladas, incluida la orientación sobre la política de claves de KMS predeterminada, consulte [AWS Key Management Service en la Guía para desarrolladores](#).

La clave debe cumplir los siguientes requisitos:

- La clave KMS debe estar en la misma AWS región que la instancia del IAM Identity Center
- Puede crear una clave de una región o multirregional. Sin embargo, si piensa utilizar el Centro de identidad de IAM en varias ocasiones, Regiones de AWS debe crear una clave KMS multirregional. No puede convertir una clave KMS de una sola región en una de varias regiones, por lo que le recomendamos empezar con una clave de KMS de varias regiones, a menos que tenga requisitos específicos para utilizar una clave de KMS de una sola región.
- La clave de KMS debe ser una clave simétrica configurada para el uso de «cifrado y descifrado»
- La clave KMS debe estar en la misma cuenta de AWS Organizations administración que la instancia de la organización del IAM Identity Center

 Note

Si tiene previsto replicar esta clave de KMS en las regiones en las que desee replicar su centro de identidad de IAM, le recomendamos que primero complete la configuración de esta sección y, a continuación, siga las instrucciones de [the section called “Replique el centro de identidad de IAM en una región adicional”](#)

## Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS

Cualquier administrador de IAM que utilice el servicio del Centro de Identidad de IAM APIs desde otra AWS cuenta, como los administradores delegados del Centro de Identidad de IAM, también necesita una declaración de política de IAM que permita utilizar la clave KMS a través de estas cuentas. APIs

Para cada caso de uso identificado en el paso 1:

1. Busque las plantillas de instrucciones de políticas de IAM pertinentes en Instrucciones básicas de políticas de IAM y de claves de KMS.
2. Copie las plantillas en un editor y rellene la clave ARN, que ahora está disponible tras la creación de la clave de KMS en el paso 3. Para obtener ayuda para encontrar el ARN de clave, consulte [¿Dónde encontrar los identificadores necesarios.](#)
3. En el Consola de administración de AWS, busque la política de IAM del principal de IAM asociado al caso de uso. La ubicación de esta política varía según el caso de uso y la forma en que se concede el acceso.

- Si el acceso se concede directamente en IAM, puede localizar las entidades principales de IAM, como los roles de IAM, en la consola de IAM.
  - Si el acceso se concedió en IAM Identity Center, puede localizar el conjunto de permisos correspondiente en la consola de IAM Identity Center.
4. Añada las instrucciones de política de IAM específicas de cada caso de uso al rol de IAM y guarde el cambio.

 Note

Las políticas de IAM descritas aquí son políticas basadas en identidades. Si bien estas políticas se pueden asociar a los usuarios, grupos y roles de IAM, recomendamos el uso de roles de IAM siempre que sea posible. Para obtener más información acerca de los roles de IAM, consulte Roles de IAM en la Guía del usuario de IAM.

## Configuración adicional en algunas aplicaciones gestionadas AWS

Algunas aplicaciones AWS gestionadas requieren que configure un rol de servicio para permitir que las aplicaciones utilicen el servicio APIs IAM Identity Center. Si su organización utiliza aplicaciones AWS gestionadas con el Centro de identidades de IAM, complete los siguientes pasos para cada aplicación implementada:

1. Consulte la guía del usuario de la aplicación para confirmar si los permisos se han actualizado a fin de incluir los permisos relacionados con las claves del KMS para el uso de la aplicación con IAM Identity Center.
2. Si es así, actualice los permisos tal y como se indica en la guía del usuario de la aplicación para evitar interrumpir las operaciones de la aplicación.

 Note

Si no está seguro de si una aplicación AWS gestionada utiliza estos permisos, le recomendamos que consulte las guías de usuario de todas las aplicaciones AWS gestionadas implementadas. Solo necesita realizar esta configuración una vez para cada aplicación que la requiera.

## Paso 5: configure la clave de KMS en IAM Identity Center

### Important

Antes de continuar con este paso:

- Compruebe que las aplicaciones AWS administradas sean compatibles con las claves de KMS administradas por el cliente. Para obtener una lista de aplicaciones compatibles, consulte [AWS managed applications that you can use with IAM Identity Center](#). Si tiene aplicaciones incompatibles, no continúe.
- Configure los permisos necesarios para usar la clave de KMS. Sin los permisos adecuados, este paso puede provocar errores o interrumpir la administración de IAM Identity Center, el uso de aplicaciones administradas por AWS y otros casos de uso que requieran permisos clave de KMS. Para obtener más información, consulte [Paso 1: identifique los casos de uso de su organización](#).
- Asegúrese de que los permisos para las aplicaciones AWS administradas y las aplicaciones administradas por el cliente que utilizan el servicio IAM Identity Center APIs con funciones de IAM también permitan el uso de la clave KMS a través del servicio IAM Identity Center. APIs Algunas aplicaciones AWS gestionadas requieren la configuración de permisos, como un rol de servicio, para su uso. APIs Consulte la guía del usuario de cada aplicación AWS administrada implementada para confirmar si necesita agregar permisos clave de KMS específicos.

Especificación de una clave de KMS al habilitar una nueva instancia de organización de IAM Identity Center

Al habilitar una nueva instancia de organización de IAM Identity Center, puede especificar una clave de KMS administrada por el cliente durante la configuración. Esto garantiza que la instancia utilice su clave de cifrado en reposo desde el principio. Antes de comenzar, consulte [Consideraciones sobre las claves de KMS administradas por el cliente y las políticas de claves de KMS avanzadas](#).

1. En la página Habilitar IAM Identity Center, amplíe la sección Cifrado en reposo.
2. Elija Manage Encryption (Administrar cifrado).
3. Elija Claves administradas por el cliente.
4. Para Clave de KMS, realice una de las siguientes operaciones:

- a. Seleccione la opción Seleccionar una de sus claves de KMS y seleccione la clave que ha creado en la lista desplegable.
  - b. Seleccione Introducir el ARN de la clave de KMS e introduzca el ARN completo de la clave.
5. Seleccione Save.
6. Seleccione Habilitar para completar la configuración.

Para más información, consulte [Activar IAM Identity Center](#).

## Cambio de la configuración de claves de una instancia de organización existente de IAM Identity Center

Puede cambiar la clave de KMS administrada por el cliente por otra clave o cambiar a una clave de propiedad de AWS en cualquier momento.

### Console

Para cambiar su configuración de clave de KMS

1. Abra la consola del IAM Identity Center en <https://console.aws.amazon.com/singlesignon/>.
2. En el panel de navegación, seleccione Configuración.
3. Elija la pestaña Configuración adicional.
4. Seleccione Administrar cifrado.
5. Seleccione una de las siguientes opciones:
  - a. Clave administrada por el cliente: seleccione una clave administrada por el cliente diferente en el menú desplegable o introduzca un ARN de clave nuevo.
  - b. AWS clave propia: cambie a la opción de cifrado predeterminada.
6. Seleccione Save.

### AWS CLI

Para cambiar una instancia de organización existente de IAM Identity Center para que utilice la clave administrada por el cliente de KMS

```
aws sso-admin update-instance \  
--instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  

```

```
--encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Para cambiar una instancia de organización existente de IAM Identity Center para que utilice una clave de propiedad de AWS

```
aws sso-admin update-instance \  
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
    --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

### Consideraciones clave administradas por el cliente

- La actualización de la configuración de claves de KMS para el funcionamiento de IAM Identity Center no afecta a las sesiones de usuario activas en su IAM Identity Center. Puede seguir utilizando el portal de AWS acceso, la consola del IAM Identity Center y el servicio IAM Identity Center APIs durante este proceso.
- Al cambiar a una nueva clave de KMS, IAM Identity Center comprueba que puede utilizarla correctamente para el cifrado y el descifrado. Si cometió un error durante la configuración de la política de claves o la política de IAM, la consola mostrará un mensaje de error explicativo y la clave de KMS anterior seguirá utilizándose.
- La rotación anual predeterminada de claves de KMS se realizará automáticamente. Puede consultar la [Guía para desarrolladores de AWS KMS](#) para obtener información sobre temas como la [rotación de claves](#), la [supervisión de las claves de AWS KMS](#) y el [control del acceso a la eliminación de claves](#).

#### Important

Si la clave de KMS gestionada por el cliente que utiliza su instancia de IAM Identity Center se elimina, deshabilita o no se puede acceder a ella debido a una política de claves de KMS incorrecta, los usuarios de su personal y los administradores de IAM Identity Center no podrán utilizar IAM Identity Center. La pérdida de acceso puede ser temporal (se puede corregir una política de claves) o permanente (no se puede restaurar una clave eliminada), según las circunstancias. Le recomendamos que [restrinja el acceso](#) a las operaciones críticas, como eliminar o deshabilitar la clave de KMS. Además, recomendamos que su organización establezca [AWS procedimientos de acceso innovadores para garantizar que](#)

[sus usuarios privilegiados puedan acceder](#) AWS en caso de que el IAM Identity Center no esté accesible.

## ¿Dónde encontrar los identificadores necesarios

Al configurar los permisos para la clave de KMS administrada por el cliente, necesitará identificadores de recursos de AWS específicos para completar las plantillas de instrucciones de políticas de claves y de políticas de IAM. Inserte los identificadores necesarios (por ejemplo, el identificador de la organización) y los nombres de entidades principales de IAM en las instrucciones de política de claves de KMS.

A continuación, encontrará una guía para localizar estos identificadores en la consola de AWS administración.

### Nombre de recurso de Amazon (ARN) de IAM Identity Center y ARN de Identity Store

Una instancia de IAM Identity Center es un AWS recurso con su propio ARN único, como `arn:aws:sso::instance/ssoins-1234567890abcdef`. El ARN sigue el patrón documentado en la sección de tipos de recursos de IAM Identity Center de la Referencia de autorizaciones de servicios.

Cada instancia de IAM Identity Center tiene un almacén de identidades asociado que almacena las identidades de los usuarios y los grupos. Un almacén de identidades tiene un identificador único denominado ID de almacén de identidades (por ejemplo, `d-123456789a`). El ARN sigue el patrón documentado en la sección de tipos de recursos de Identity Store de la [Referencia de autorizaciones de servicios](#).

Puede encontrar los valores del ARN y del ID de almacén de identidades en la página de configuración de su IAM Identity Center. El ID de almacén de identidades se encuentra en la pestaña Origen de identidad.

### AWS Organizations ID

Si desea especificar un ID de organización (por ejemplo, `o-exampleorg1`) en su política de claves, puede encontrar su valor en la página de configuración de las consolas de IAM Identity Center y Organizations. El ARN sigue el patrón documentado en la sección de tipos de recursos de Organizations de la Referencia de autorizaciones de servicios.

### ARN de clave de KMS

Puede encontrar el ARN de una clave KMS en la AWS KMS consola. Elija Claves administradas por el cliente a la izquierda, haga clic en la clave cuyo ARN desee buscar y la verá en la sección Configuración general. El ARN sigue el patrón documentado en la sección de tipos de AWS KMS recursos de la Referencia de autorización de servicio.

Consulte la Guía para AWS Key Management Service desarrolladores para obtener más información sobre las políticas clave AWS KMS y la solución de problemas relacionados con AWS KMS los permisos. Para obtener más información acerca de las políticas de IAM y su representación en JSON, consulte la Guía del usuario de IAM.

## Instrucciones básicas de KMS y políticas de IAM

Las políticas básicas basadas en la identidad y las claves de KMS que se proporcionan aquí sirven de base para los requisitos comunes. También le recomendamos que revise [Instrucciones de política de claves de KMS avanzadas](#) que proporciona controles de acceso más detallados, como garantizar que solo una instancia específica de IAM Identity Center o una aplicación administrada por AWS pueda acceder a la clave KMS. Antes de utilizar las instrucciones de políticas de claves de KMS avanzadas, revise las [Consideraciones a la hora de elegir las principales instrucciones de política de claves de KMS básicas o avanzadas](#).

En las secciones siguientes, se incluyen instrucciones de política de referencia para cada caso de uso. Amplíe las secciones que se adapten a sus casos de uso y copie las principales declaraciones de políticas de KMS. A continuación, vuelva a [Paso 2: prepare las instrucciones de política de claves de KMS](#).

Instrucciones de política de claves básicas de KMS para el uso de IAM Identity Center (obligatorias)

Utilice la siguiente plantilla de instrucción de políticas de claves de KMS en [Paso 2: prepare las instrucciones de política de claves de KMS](#) para permitir que IAM Identity Center, su almacén de identidades asociado y los administradores de IAM Identity Center utilicen la clave de KMS.

- En el elemento principal de las declaraciones de política del administrador, especifique los principales de las AWS cuentas de administración del Centro de Identidad de IAM, que son la cuenta de administración de la AWS organización y la cuenta de administración delegada, utilizando el formato «arn:aws:iam: :111122223333:root».
- En el PrincipalArn elemento, sustituya el ejemplo por las funciones de IAM de los administradores del IAM Identity Center. ARNs

Puede especificar:



- ARN de rol de IAM específico:

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
```

- Patrón comodín (recomendado):

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*
```

El uso del comodín (\*) evita la pérdida de acceso si el conjunto de permisos se elimina y se vuelve a crear, ya que Identity Center genera nuevos identificadores únicos para los conjuntos de permisos recreados. Para ver un ejemplo de implementación, consulte [Ejemplo de políticas de confianza personalizadas](#)

- En el SourceAccount elemento, especifique el ID de cuenta del IAM Identity Center.
- Identity Store tiene su propia entidad principal de servicio, `identitystore.amazonaws.com`, a la que se le debe permitir usar la clave de KMS.
- Estas declaraciones de política permiten que las instancias del Centro de Identidad de IAM de una AWS cuenta específica utilicen la clave KMS. Para restringir el acceso a una instancia específica de IAM Identity Center, consulte [Instrucciones de política de claves de KMS avanzadas](#). Solo puede tener una instancia del IAM Identity Center para cada AWS cuenta.

## Instrucciones de política de claves de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      },
    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      },
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
  }
}

```

```

    }
  },
  {
    "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "sso.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "identitystore.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "identitystore.amazonaws.com",
        "sso.amazonaws.com"
      ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  }
]
}

```

Utilice la siguiente plantilla de instrucción de políticas de IAM en [the section called “Paso 4: configure las políticas de IAM”](#) para permitir que los administradores de IAM Identity Center utilicen la clave de KMS.

- Sustituya el ARN de clave de ejemplo del elemento Resource por el ARN de clave de KMS real. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios?](#).
- Estas declaraciones de política de IAM conceden acceso a la clave de KMS al director de IAM, pero no restringen el AWS servicio que puede realizar la solicitud. La política de claves de KMS suele proporcionar estas restricciones de servicio. Sin embargo, puede añadir un contexto de cifrado a esta política de IAM para limitar el uso a una instancia específica de Identity Center. Consulte [Instrucciones de política de claves de KMS avanzadas](#) para obtener más información.

Las instrucciones de política de IAM son obligatorias para los administradores delegados de IAM Identity Center

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  {
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",
    "Effect": "Allow",
    "Action": "kms:ListAliases",
    "Resource": "*"
  }
]
```

## Declaraciones básicas de política de IAM y clave de KMS para el uso de aplicaciones administradas AWS

### Note

Algunas aplicaciones AWS administradas no se pueden usar con el centro de identidad de IAM configurado con una clave de KMS administrada por el cliente. Para obtener más información, consulte [AWS managed applications that work with IAM Identity Center](#).

Utilice la siguiente plantilla de declaración de política clave de KMS [Paso 2: prepare las instrucciones de política de claves de KMS](#) para permitir que tanto las aplicaciones AWS gestionadas como sus administradores utilicen la clave de KMS.

- Introduzca su AWS Organizations ID en el PrincipalOrg ID y SourceOrgId las condiciones. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios](#).
- Estas declaraciones de política permiten a cualquiera de sus aplicaciones AWS gestionadas y a todos los responsables de IAM (administradores de aplicaciones) de la AWS organización utilizar kms: Decrypt mediante IAM Identity Center e Identity Store. Para restringir estas instrucciones de política a aplicaciones administradas por AWS , cuentas o instancias del IAM Identity Center específicas, consulte [Instrucciones de política de claves de KMS avanzadas](#).

Puede restringir el acceso a administradores de aplicaciones específicos sustituyendo \* por las entidades principales de IAM específicas. Para protegerse de los cambios en el nombre del rol de IAM al volver a crear conjuntos de permisos, utilice el enfoque de [Ejemplo de políticas de confianza personalizadas](#). Para obtener más información, consulte [Consideraciones a la hora de elegir las principales instrucciones de política de claves de KMS básicas o avanzadas](#).

### Instrucciones de política de claves de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
]
}

```

Utilice la siguiente plantilla de instrucción de política de IAM en [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#) para permitir que los administradores de las aplicaciones administradas por AWS utilicen la clave KMS de una cuenta de miembro.

- Sustituya el ARN de ejemplo del elemento Recurso por el ARN de clave de KMS real. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios?](#).
- Algunas aplicaciones AWS gestionadas requieren que configure los permisos para el servicio IAM Identity Center. APIs Antes de configurar una clave administrada por el cliente en IAM Identity Center, compruebe que estos permisos también permiten el uso de la clave de KMS. Para conocer los requisitos específicos de permisos clave de KMS, consulte la documentación de cada aplicación administrada por AWS que haya implementado.

Declaraciones de política de IAM obligatorias para los administradores de aplicaciones AWS gestionadas:



```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid":
    "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

## Declaración clave básica de KMS para el uso de AWS Control Tower

Utilice las siguientes plantillas de declaraciones clave de KMS [Paso 2: prepare las instrucciones de política de claves de KMS](#) para permitir que los administradores AWS de la Torre de Control usen la clave de KMS.

- En el elemento principal, especifique los principios de IAM utilizados para acceder al servicio del Centro de identidad de IAM. APIs Para obtener más información sobre las entidades principales de IAM, consulte [Cómo especificar una entidad principal](#) en la Guía del usuario de IAM.
- Estas declaraciones de política permiten a los administradores de la Torre de AWS Control utilizar la clave KMS en cualquiera de sus instancias del IAM Identity Center. Sin embargo, AWS Control Tower restringe el acceso a la instancia organizativa de IAM Identity Center en la misma AWS organización. Debido a esta restricción, restringir aún más la clave KMS a una instancia específica del IAM Identity Center no tiene ningún beneficio práctico, como se describe en. [Instrucciones de política de claves de KMS avanzadas](#)
- Para evitar que se produzcan cambios en el nombre de las funciones de IAM cuando se vuelvan a crear conjuntos de permisos, utilice el enfoque descrito en la. [Ejemplo de políticas de confianza personalizadas](#)

## Instrucción de la política de claves de KMS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

AWS Control Tower no admite la administración delegada y, por lo tanto, no es necesario configurar una política de IAM para sus administradores.

**⚠ Important**

La declaración de política anterior abarca las operaciones AWS Control Tower gestionadas por el servicio, como la inscripción automática de cuentas, en las que AWS Control Tower asume la función. `AWSControlTowerAdmin` Sin embargo, para las operaciones iniciadas por el cliente, como el aprovisionamiento de cuentas a través de Account Factory o las llamadas AWS Control Tower APIs directas, AWS Control Tower utiliza [sesiones de acceso directo \(FAS\)](#) y opera bajo la propia función de IAM del cliente. Esto significa que la función de IAM que utilizas para iniciar estas operaciones también necesita `kms:Decrypt` permisos en la clave de KMS administrada por el cliente.

Agregue las siguientes declaraciones de política clave de KMS junto con las `AWSControlTowerAdmin` declaraciones anteriores. `MyControlTowerRole` Sustitúyalo por el ARN del rol de IAM con el que utilizas para interactuar AWS Control Tower, como un rol de conjunto de permisos del Centro de Identidad de IAM (por ejemplo, `AWSReservedSSO_PermissionSetName_*`), un rol de IAM personalizado para la automatización o cualquier otro rol que se utilice para llamar o. AWS Control Tower AWS Service Catalog APIs

Declaración de política clave de KMS para las operaciones iniciadas por el cliente: AWS Control Tower

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityCenterForControlTower",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    }
  ],
}
```

```
{
  "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityStoreForControlTower",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
  }
}
```

Declaraciones básicas de política de IAM y clave de KMS para el uso del IAM Identity Center en las instancias de Amazon EC2

Utilice la siguiente plantilla de declaración de política clave de KMS [Paso 2: prepare las instrucciones de política de claves de KMS](#) para permitir a los usuarios de inicio de sesión único (SSO) en las instancias de Amazon EC2 utilizar la clave de KMS en todas las cuentas.

- Especifique las entidades principales de IAM que se utilizan para acceder a IAM Identity Center en el campo Entidad principal. Para obtener más información sobre las entidades principales de IAM, consulte [Cómo especificar una entidad principal](#) en la Guía del usuario de IAM.
- Esta instrucción de política permite que cualquiera de sus instancias de IAM Identity Center utilice la clave de KMS. Para restringir el acceso a una instancia específica de IAM Identity Center, consulte [Instrucciones de política de claves de KMS avanzadas](#).
- Para protegerse de los cambios en el nombre del rol de IAM al volver a crear conjuntos de permisos, utilice el enfoque descrito en el ejemplo de política de confianza personalizada.

### Instrucción de política de claves de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Utilice la siguiente plantilla de declaración de política de IAM [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#) para permitir que el SSO de las instancias EC2 utilice la clave de KMS.

Adjunte la declaración de política de IAM al conjunto de permisos existente en el Centro de identidades de IAM que está utilizando para permitir el acceso SSO a las instancias de Amazon EC2. Para ver ejemplos de políticas de IAM, consulte [Conexiones del protocolo de escritorio remoto](#) en la Guía del usuario de AWS Systems Manager.

- Sustituya el ARN de ejemplo del elemento Recurso por el ARN de clave de KMS real. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios?](#).

Política de IAM del conjunto de permisos:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Instrucciones básicas de políticas de IAM y de claves de KMS para el uso de flujos de trabajo personalizados con IAM Identity Center

Utilice las siguientes plantillas de declaraciones de políticas clave de KMS [Paso 2: prepare las instrucciones de política de claves de KMS](#) para permitir que los flujos de trabajo personalizados, como las aplicaciones administradas por el cliente, en la cuenta de administración o la AWS Organizations cuenta de administración delegada utilicen la clave de KMS. Tenga en cuenta que la federación de SAML en las aplicaciones administradas por el cliente no requiere permisos clave de KMS.

- En el elemento principal, especifique los principios de IAM que se utilizan para acceder al servicio del Centro de identidad de IAM. APIs Para obtener más información sobre las entidades principales de IAM, consulte [Cómo especificar una entidad principal](#) en la Guía del usuario de IAM.

- Estas instrucciones de política permiten que su flujo de trabajo utilice la clave de KMS en cualquiera de sus instancias de IAM Identity Center. Para restringir el acceso a una instancia específica de IAM Identity Center, consulte [Instrucciones de política de claves de KMS avanzadas](#).
- Para protegerse de los cambios en el nombre de las funciones de IAM cuando se recrean los conjuntos de permisos, utilice el enfoque descrito en el [Ejemplo de políticas de confianza personalizadas](#)

Instrucción de la política de claves de KMS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

```
]
}
```

Utilice la siguiente plantilla de instrucción de políticas de IAM en [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#) para permitir que la entidad principal de IAM asociada al flujo de trabajo personalizado utilice la clave de KMS en todas las cuentas. Añada la instrucción de política de IAM a la entidad principal de IAM.

- Sustituya el ARN de ejemplo del elemento Recurso por el ARN de clave de KMS real. Si necesita ayuda para encontrar los valores de los identificadores a los que se hace referencia, consulte [¿Dónde encontrar los identificadores necesarios?](#).

Instrucción de política de IAM (necesaria solo para el uso entre cuentas):

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

## Ejemplos de declaraciones de políticas clave de KMS para casos de uso comunes

### Centro de identidad de IAM con administradores delegados y AWS aplicaciones gestionadas

Esta sección contiene ejemplos de las principales declaraciones de política del KMS que puede utilizar para una instancia del IAM Identity Center que tenga administradores delegados y aplicaciones gestionadas. AWS



**⚠ Important**

En las declaraciones de política clave de KMS se parte del supuesto de que su instancia del Centro de Identidad de IAM no se utilizará en ningún otro caso de uso que requiera permisos de clave de KMS. Para confirmarlo, puedes revisar todos los [casos de uso](#). Además, para confirmar si las aplicaciones AWS gestionadas requieren una configuración adicional, consulte [the section called “Configuración adicional en algunas aplicaciones AWS administradas”](#)

Copie las declaraciones de política clave de KMS que aparecen debajo de la tabla y agréguelas a su política de clave de KMS. En este ejemplo se utilizan los siguientes valores de ejemplo:

- 111122223333- ID de cuenta de la instancia del IAM Identity Center
- 444455556666- ID de cuenta de administración delegada
- o-a1b2c3d4e5- ID de AWS organización
- `arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*`- Un patrón comodín de la función de IAM de un administrador del Centro de Identidad de IAM proporcionada a partir del conjunto de permisos. *Admin* Este rol contiene el código de región de la región principal (us-east-1 en este ejemplo).
- `arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*`- Un patrón comodín de una función de IAM de un administrador delegado del Centro de Identidad de IAM proporcionada a partir del conjunto de permisos. *DelegatedAdmin* Este rol contiene el código de región de la región principal (us-east-1 en este ejemplo).

Si la función de IAM no se generó a partir de un conjunto de permisos, la función de IAM tendrá el aspecto de una función normal, por ejemplo. `arn:aws:iam::111122223333:role/idcadmin`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```

        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
    ],
    },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
                "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
            ]
        }
    },
    "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [

```

```

        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
    ]
},
"StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",
    "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
}
},
{
    "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
                "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
            ]
        }
    }
},
{
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "sso.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",

```

```

    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIdentityStoreToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "identitystore.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "identitystore.amazonaws.com",
      "sso.amazonaws.com"
    ]
  },
  "Action": "kms:DescribeKey",

```

```

    "Resource": "*"
  },

  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",

```

```

        "kms:EncryptionContext:aws:sso:instance-arn": "*"
    },
    "Bool": {
        "aws:PrincipalIsAWSService": "true"
    },
    "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
    }
}
},
{
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "identitystore.*.amazonaws.com",
            "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "Bool": {
            "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
            "aws:SourceOrgID": "o-a1b2c3d4e5"
        }
    }
}
]
}

```

## Instrucciones de política de claves de KMS avanzadas

Utilice las instrucciones de política de claves de KMS avanzadas para implementar controles de acceso más detallados para su clave de KMS administrada por el cliente. Estas políticas se basan en [Instrucciones básicas de KMS y políticas de IAM](#) al agregar condiciones de contexto de cifrado y restricciones específicas del servicio. Antes de decidir si va a utilizar las instrucciones de política de claves de KMS avanzadas, asegúrese de revisar las consideraciones pertinentes.

## Uso del contexto de cifrado para restringir el acceso

Puede restringir el uso de claves de KMS a una instancia específica de IAM Identity Center especificando una condición de contexto de cifrado en sus instrucciones de política de claves. Las instrucciones de políticas de claves de referencia ya incluyen este contexto con un valor genérico. Sustituya el comodín «\*» por un ARN de instancia de Identity Center y un ARN de Identity Store específicos para garantizar que la clave solo funcione con la instancia deseada. También puede añadir las mismas condiciones de contexto de cifrado a la política de IAM configurada para el uso de la clave de KMS entre cuentas.

### Centro de identidades

```
"StringEquals": {  
  "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/  
ssoins-1234567890abcdef"  
}
```

### Almacén de identidades

```
"StringEquals": {  
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":  
  "arn:aws:identitystore:::111122223333:identitystore/d-1234567890"  
}
```

Si necesita ayuda para encontrar estos identificadores, consulte. [¿Dónde encontrar los identificadores necesarios](#)

#### Note

Solo puede usar una clave de KMS administrada por el cliente con una instancia de organización de IAM Identity Center. La clave administrada por el cliente debe estar ubicada en la cuenta de administración de la AWS organización, lo que ayuda a garantizar que la clave se utilice con una única instancia de IAM Identity Center. Sin embargo, el mecanismo de contexto de cifrado proporciona una protección técnica independiente contra el uso de una sola instancia. También puede usar la clave de condición `aws:SourceArn` en las instrucciones de política de claves de KMS destinadas a las entidades principales de servicio de Identity Center e Identity Store.

## Consideraciones para implementar las condiciones del contexto de cifrado

Antes de implementar las condiciones del contexto de cifrado, revise estos requisitos:

- **DescribeKey acción.** El contexto de cifrado no se puede aplicar a la acción «kms:DescribeKey», que pueden utilizar los administradores del IAM Identity Center. Al configurar su política de claves de KMS, excluya el contexto de cifrado para esta acción específica a fin de garantizar el correcto funcionamiento de su instancia de IAM Identity Center.
- **Configuración de una instancia nueva.** Si habilita una nueva instancia de IAM Identity Center con una clave de KMS administrada por el cliente, consulte [Consideraciones sobre las claves de KMS administradas por el cliente y las políticas de claves de KMS avanzadas](#).
- **Cambios en el origen de identidad.** Al cambiar el origen de identidad a Active Directory o desde Active Directory, se debe prestar especial atención al contexto de cifrado. Consulte [Consideraciones para cambiar la fuente de identidad](#).

## Plantillas de política de

Seleccione entre estas plantillas de políticas avanzadas en función de sus requisitos de seguridad. Equilibre los controles de acceso detallados con la sobrecarga administrativa que suponen.

Los temas que se tratan aquí:

- [Instrucciones de política de KMS para el uso de solo lectura de una instancia específica de IAM Identity Center](#). En esta sección se muestra el uso del contexto de cifrado para el acceso de solo lectura a IAM Identity Center.
- [Se han perfeccionado las principales declaraciones de política de KMS para el uso de aplicaciones gestionadas AWS](#). En esta sección se muestra cómo refinar las políticas de claves de KMS para las aplicaciones AWS administradas mediante el contexto de cifrado y la información de la aplicación, como el principal del servicio de la aplicación, el ARN de la aplicación y el ID de AWS cuenta.

## Instrucciones de política de KMS para el uso de solo lectura de una instancia específica de IAM Identity Center

Esta política permite a los [auditores de seguridad](#) y al resto del personal que solo necesita acceso de lectura a IAM Identity Center utilizar la clave de KMS.

Para usar esta política:



1. Sustituya las entidades principales de IAM de administrador de solo lectura del ejemplo por las entidades principales de IAM de administrador actuales
2. Sustituya el ARN de la instancia de IAM Identity Center de ejemplo por el ARN de la instancia real
3. Sustituya el ARN de Identity Store de ejemplo por el ARN actual de Identity Store
4. Si se utiliza la [administración delegada](#), consulte [Paso 4: configure las políticas de IAM para el uso entre cuentas de la clave de KMS](#)

Si necesita ayuda para encontrar los valores de estos identificadores, consulte. [¿Dónde encontrar los identificadores necesarios](#)

Una vez que haya actualizado la plantilla con sus valores, vuelva a [Paso 2: prepare las instrucciones de política de claves de KMS](#) para preparar otras instrucciones de política de claves de KMS, según sea necesario.

La acción de kms: descifrar por sí sola no restringe el acceso a las operaciones de solo lectura. La política de IAM debe imponer el acceso de solo lectura al servicio del Centro de identidad de IAM. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        }
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
```

```
"Principal": {
  "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
},
"Action": "kms:Decrypt",
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",
    "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  }
}
}
```

Se han perfeccionado las principales declaraciones de política de KMS para el uso de aplicaciones gestionadas AWS

Estas plantillas de políticas proporcionan un control más detallado sobre qué aplicaciones AWS administradas pueden usar su clave de KMS.

 Note

Algunas aplicaciones AWS administradas no se pueden usar con el Centro de identidad de IAM configurado con una clave de KMS administrada por el cliente. Consulte [Aplicaciones administradas por AWS que puede utilizar con IAM Identity Center](#).

[Declaraciones básicas de política de IAM y clave de KMS para el uso de aplicaciones administradas AWS](#) Permiten que cualquier aplicación AWS gestionada de cualquier cuenta de la misma AWS organización utilice la clave KMS. Utilice estas políticas refinadas para restringir el acceso de la siguiente manera:

- Entidad principal del servicio de aplicaciones
- Instancia de aplicación ARNs
- AWS account IDs
- Contexto de cifrado para instancias específicas de IAM Identity Center

 Note

Un principal de servicio es un identificador único de un AWS servicio, normalmente con el formato `servicename.amazonaws.com` (por ejemplo, `elasticmapreduce.amazonaws.com` para Amazon EMR).

## Restricción por cuenta

Esta plantilla de declaración de política clave de KMS permite que una aplicación AWS gestionada en cuentas específicas utilice la clave de KMS mediante una instancia específica del IAM Identity Center. AWS

Para usar esta política:

1. Sustituya la entidad principal de servicio de ejemplo por la entidad principal de servicio de la aplicación actual
2. Sustituya la cuenta IDs de ejemplo por la cuenta real en la IDs que se AWS implementan las aplicaciones gestionadas
3. Sustituya el ARN de Identity Store de ejemplo por el ARN actual de Identity Store
4. Sustituya el ARN de la instancia de IAM Identity Center de ejemplo por el ARN de la instancia real

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        }
      }
    }
  ]
}
```

```

    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso::instance/
ssoins-1234567890abcdef"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  },
  {
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      }
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  }
]
}

```

## Restricción por instancia de aplicación

Esta plantilla de declaración de política clave de KMS permite que una instancia de aplicación AWS gestionada específica utilice la clave de KMS mediante una instancia específica del IAM Identity Center.

Para usar esta política:

1. Sustituya la entidad principal de servicio de ejemplo por la entidad principal de servicio de la aplicación actual
2. Sustituya el ARN de la aplicación de ejemplo por el ARN de la instancia de aplicación real
3. Sustituya el ARN de Identity Store de ejemplo por el ARN actual de Identity Store
4. Sustituya el ARN de la instancia de IAM Identity Center de ejemplo por el ARN de la instancia real

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ],
  {
```

```

    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

## Consideraciones sobre las claves de KMS administradas por el cliente y las políticas de claves de KMS avanzadas

Al implementar claves de KMS administradas por el cliente con IAM Identity Center, tenga en cuenta estos factores que afectan a la configuración, la seguridad y el mantenimiento continuo de la configuración de cifrado.

Consideraciones a la hora de elegir las principales instrucciones de política de claves de KMS básicas o avanzadas

Al decidir si desea hacer que los permisos de clave de KMS sean más específicos usando [Instrucciones de política de claves de KMS avanzadas](#), tenga en cuenta la sobrecarga de administración y las necesidades de seguridad de su organización. Las instrucciones de políticas más específicas proporcionan un control más detallado sobre quién puede usar la clave y con qué fines; sin embargo, requieren un mantenimiento continuo a medida que evoluciona la configuración de IAM Identity Center. Por ejemplo, si restringe el uso de la clave KMS a implementaciones de aplicaciones AWS gestionadas específicas, tendrá que actualizar la política clave siempre que su

organización desee implementar o anular el despliegue de una aplicación. Las políticas menos restrictivas reducen la carga administrativa, pero pueden conceder permisos más amplios de los necesarios para cumplir sus requisitos de seguridad.

Consideraciones para habilitar una nueva instancia de IAM Identity Center con una clave de KMS administrada por el cliente

Estas consideraciones se aplican si utiliza el contexto de cifrado, tal como se describe en [Instrucciones de política de claves de KMS avanzadas](#) para restringir el uso de la clave de KMS a una instancia específica de IAM Identity Center.

Al habilitar una nueva instancia del Centro de Identidad de IAM con una clave de KMS administrada por el cliente, el Centro de Identidad de IAM y el Almacén de identidades no estarán disponibles hasta ARNs después de la configuración. Dispone de las opciones siguientes:

- Usa patrones de ARN genéricos de forma temporal y, a continuación, sustitúyelos por completos una ARNs vez que la instancia esté habilitada. Recuerde cambiar de operador a StringEquals StringLike operador según sea necesario.
  - Para IAM Identity Center SPN: «arn:\${Partition}:sso:::instance/\*».
  - Para Identity Store SPN: «arn:\${Partition}:identitystore:::\${Account}:identitystore/\*».
- Utilice «purpose:KEY\_CONFIGURATION» en el ARN temporalmente. Esto solo funciona para la habilitación de instancias, por ejemplo, y debe sustituirse por el ARN real para que la instancia de IAM Identity Center funcione normalmente. La ventaja de este enfoque es que no puede olvidar reemplazarlo una vez habilitada la instancia.
  - Para el SPN de IAM Identity Center, utilice: «arn:\${Partition}:sso:::instance/purpose:KEY\_CONFIGURATION»
  - Para el SPN de Identity Store, utilice: «arn:\${Partition}:identitystore:::\${Account}:identitystore/purpose:KEY\_CONFIGURATION».

 Important

No aplique esta configuración a una clave de KMS que ya esté en uso en una instancia de IAM Identity Center existente, ya que podría interrumpir su funcionamiento normal.

- Omita la condición del contexto de cifrado de la política de claves de KMS hasta que la instancia esté habilitada.

# Recursos de etiquetado AWS IAM Identity Center

Una etiqueta es una etiqueta de atributo personalizada que se agrega a un AWS recurso para facilitar la identificación, la organización y la búsqueda de los recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta pueden tener 128 caracteres como máximo y distingue entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Los valores de etiqueta pueden tener una longitud de hasta 256 caracteres y, al igual que las claves de etiqueta, distinguen mayúsculas y minúsculas. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía.

Las etiquetas ayudan a identificar y organizar AWS los recursos. Muchos AWS servicios admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, puede asignar la misma etiqueta a un conjunto de permisos específico en su instancia de IAM Identity Center. Para obtener más información sobre las estrategias de etiquetado, consulte [Etiquetado de AWS recursos](#) en la Referencia general de AWS guía y Prácticas recomendadas de [etiquetado](#).

Además de identificar, organizar y rastrear tus AWS recursos con etiquetas, puedes utilizarlas en las políticas de IAM para controlar quién puede ver tus recursos e interactuar con ellos. Para obtener más información sobre el uso de etiquetas para controlar el acceso, consulte [Controlar el acceso a AWS los recursos mediante etiquetas](#) en la Guía del usuario de IAM. Por ejemplo, puede permitir que un usuario actualice un conjunto de permisos de IAM Identity Center, pero solo si este conjunto tiene una etiqueta de `owner` con un valor del nombre de ese usuario.

Solo puede aplicar etiquetas a conjuntos de permisos. No puede aplicar etiquetas a las funciones correspondientes en las que crea el Centro de Identidad de IAM. Cuentas de AWS Puede utilizar la consola del Centro de Identidad de IAM AWS CLI o el Centro de Identidad de IAM APIs para añadir, editar o eliminar las etiquetas de un conjunto de permisos.

En las siguientes secciones se ofrece más información acerca de las etiquetas para IAM Identity Center.

Temas



- [Restricciones de las etiquetas](#)
- [Administre las etiquetas a través de la consola de IAM Identity Center](#)
- [AWS CLI ejemplos](#)
- [Administre etiquetas mediante el uso de la API de IAM Identity Center](#)

## Restricciones de las etiquetas

Las siguientes restricciones básicas se aplican a las etiquetas en recursos de IAM Identity Center:

- El número máximo de etiquetas que puede asignar a un recurso es 50.
- La longitud máxima de la clave es de 128 caracteres Unicode.
- La longitud máxima del valor es de 256 caracteres Unicode.
- Los caracteres válidos para una clave y un valor de etiqueta son:  
a-z, A-Z, 0-9, espacio y los siguientes caracteres: `_ . : / = + - y @`
- Las claves y los valores distinguen entre mayúsculas y minúsculas.
- No utilice `aws :` como prefijo para claves, ya que está reservado para AWS .

## Administre las etiquetas a través de la consola de IAM Identity Center

Puede utilizar la consola de IAM Identity Center para agregar, editar y eliminar etiquetas asociadas a sus conjuntos de instancias o permisos.

Para administrar etiquetas de conjuntos de permisos para una consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#)
2. Elija Conjuntos de permisos.
3. Elija el nombre del conjunto de permisos que tiene las etiquetas que desea administrar.
4. En la pestaña Permisos de la sección Etiquetas, realice una de las siguientes acciones y, a continuación, continúe con el paso siguiente:
  - a. Si ya hay etiquetas asignadas a este conjunto de permisos, elija Edite etiquetas.
  - b. Si no hay ninguna etiqueta asignada a este conjunto de permisos, elija Agregar etiquetas.

5. Para cada etiqueta nueva, escriba los valores en las columnas Clave y Valor (opcional). Cuando haya finalizado, elija Guardar cambios.

Para eliminar una etiqueta, seleccione la X en la columna Eliminar situada junto a la etiqueta que desea eliminar.

Para administrar de etiquetas para una instancia de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. Elija la pestaña Etiquetas.
4. Para cada etiqueta, escriba los valores en los campos Clave y Valor (opcional). Cuando haya terminado, seleccione el botón Agregar nueva etiqueta.

Para eliminar una etiqueta, seleccione el botón Eliminar junto a la etiqueta que desee eliminar.

## AWS CLI ejemplos

AWS CLI Proporciona comandos que puede usar para administrar las etiquetas que asigna a su conjunto de permisos.

### Asignación de etiquetas

Utilice los siguientes comandos para asignar etiquetas a su conjunto de permisos.

Example Comando **tag-resource** para un conjunto de permisos

Asigne etiquetas a un conjunto de permisos mediante el uso de [tag-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test
```

Este comando incluye los siguientes parámetros:

- `instance-arn`: el nombre de recurso de Amazon (ARN) de la instancia de IAM Identity Center en la que se ejecutará la operación.

- **resource-arn**: el ARN del recurso con las etiquetas que se van a enumerar.
- **tags**: los pares de clave-valor de las etiquetas.

Para asignar varias etiquetas a la vez, especifíquelas en una lista separada por comas:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

## Visualización de etiquetas

Utilice los siguientes comandos para visualizar las etiquetas que ha asignado a su conjunto de permisos.

Example Comando **list-tags-for-resource** para un conjunto de permisos

Visualice las etiquetas que están asignadas a un conjunto de permisos mediante el uso de [list-tags-for-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

## Eliminación de etiquetas

Utilice los siguientes comandos para eliminar etiquetas de un conjunto de permisos.

Example Comando **untag-resource** para un conjunto de permisos

Elimine etiquetas de un conjunto de permisos mediante el uso de [untag-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin untag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tag-keys Stage CostCenter Owner
```

Para el parámetro **--tag-keys**, especifique una o más claves de etiquetas y no incluya los valores de etiqueta.

## Cómo aplicar etiquetas al crear un conjunto de permisos

Utilice los siguientes comandos para asignar etiquetas al crear un conjunto de permisos.

Example Comando **create-permission-set** con etiquetas

Cuando se crea un conjunto de permisos a través del comando [create-permission-set](#), es posible especificar etiquetas con el parámetro `--tags`:

```
$ aws sso-admin create-permission-set \  
> --instance-arn sso-instance-arn \  
> --name permission=set-name \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

## Administre etiquetas mediante el uso de la API de IAM Identity Center

Utilice las siguientes acciones de la API para asignar, ver y eliminar etiquetas para un conjunto de permisos o instancia de IAM Identity Center.

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

# Integración de AWS CLI con IAM Identity Center

AWS La integración de la versión 2 de la interfaz de línea de comandos (CLI) con IAM Identity Center simplifica el proceso de inicio de sesión. Los desarrolladores pueden iniciar sesión directamente en el IAM Identity Center AWS CLI con las mismas credenciales de Active Directory o IAM Identity Center que utilizan normalmente para iniciar sesión en el IAM Identity Center y acceder a las cuentas y funciones que se les asignen. Por ejemplo, después de que un administrador configure el Centro de identidades de IAM para que utilice Active Directory para la autenticación, el desarrollador puede iniciar sesión AWS CLI directamente en él con sus credenciales de Active Directory.

AWS La integración de CLI con IAM Identity Center ofrece las siguientes ventajas:

- Las empresas pueden permitir que sus desarrolladores inicien sesión con las credenciales de IAM Identity Center o Active Directory conectando IAM Identity Center a su Active Directory mediante Directory Service.
- Los desarrolladores pueden iniciar sesión desde la CLI para un acceso más rápido.
- Los desarrolladores pueden enumerar las cuentas y los roles a los que tienen acceso asignado y cambiar de una cuenta a otra.
- Los desarrolladores pueden generar y guardar automáticamente perfiles de rol con nombre en su configuración de la CLI y hacer referencia a ellos en la CLI para ejecutar comandos en las cuentas y roles deseados.
- La CLI administra automáticamente las credenciales a corto plazo para que los desarrolladores puedan iniciar y permanecer en la CLI de forma segura y sin interrupciones, y ejecutar scripts de larga duración.

## Cómo integrar AWS CLI con IAM Identity Center

Para utilizar la integración de AWS CLI con IAM Identity Center, descargue, instale y configure la AWS Command Line Interface versión 2. Para ver los pasos detallados sobre cómo descargar e integrar el AWS CLI IAM Identity Center, consulte [Configuración de la AWS CLI para usar IAM Identity Center](#) en la Guía del AWS Command Line Interface usuario.

# Consideraciones para el acceso Consola de administración de AWS privado

Si su organización utiliza la función de acceso Consola de administración de AWS privado, debe tener en cuenta cómo iniciarán sesión sus usuarios en el Centro de identidades de IAM.

Una política de puntos finales de VPC restringe el inicio de sesión en la consola de administración, lo que impide que los usuarios inicien sesión en la que no Cuentas de AWS están autorizados a acceder. Para obtener más información, consulte [Acceso privado a Consola de administración de AWS](#) en la Guía del usuario de Consola de administración de AWS .

Los puntos de conexión de VPC bloquean el inicio de sesión en IAM Identity Center

Sin embargo, es importante tener en cuenta que el uso de puntos de conexión de VPC bloqueará el inicio de sesión en IAM Identity Center. Esto ocurre cuando un usuario ya ha iniciado sesión en la consola de administración a través del punto de conexión de VPC. Para garantizar que sus usuarios puedan seguir iniciando sesión en el IAM Identity Center, deben utilizar el punto de conexión público para iniciar sesión en AWS en lugar del punto de conexión de VPC.

# Cuotas y límites de IAM Identity Center

En las siguientes tablas se describen las cuotas de IAM Identity Center. Las solicitudes de aumento de cuota deben provenir de una cuenta de administración o de administrador delegado. Para solicitar un aumento de cuota, consulte [Solicitar un aumento de cuota](#).

## Note

Recomendamos utilizar la AWS CLI y APIs administrar el Centro de identidad de IAM si tiene más de 50 000 usuarios, 10 000 grupos o 500 conjuntos de permisos. Para obtener más información acerca de la CLI, consulte [Integración de AWS CLI con IAM Identity Center](#). Para obtener más información APIs, consulte [Bienvenido a la referencia de la API del Centro de Identidad de IAM](#).

## Cuotas de aplicaciones

| Recurso                                                                                  | Cuota predeterminada    | Se puede aumentar |
|------------------------------------------------------------------------------------------|-------------------------|-------------------|
| Tamaño del archivo de los certificados SAML de proveedores de servicios (en formato PEM) | 2 KB                    | No                |
| Límite de aserción de SAML                                                               | 50 000 caracteres       | No                |
| Límite de tamaño de archivo del certificado de IdP cargado en el IAM Identity Center     | 2500 caracteres (UTF-8) | No                |
| Ámbitos de acceso por aplicación                                                         | 25                      | No                |

## Cuenta de AWS cuotas

| Recurso                                                                                            | Cuota predeterminada                                                                                                                                        | Se puede aumentar |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Número de conjuntos de permisos permitidos en IAM Identity Center                                  | 3500                                                                                                                                                        | Sí                |
| Número de conjuntos de permisos aprovisionados permitidos por Cuenta de AWS                        | 500                                                                                                                                                         | Sí                |
| Número de políticas insertadas por conjunto de permisos                                            | 1                                                                                                                                                           | No                |
| Número de políticas AWS administradas y administradas por el cliente por conjunto de permisos      | 25 <sup>1</sup>                                                                                                                                             | No                |
| Tamaño máximo de la política insertada por conjunto de permisos                                    | 32 768 bytes.<br><br>El tamaño máximo de los caracteres que no son espacios en blanco en la política insertada por conjunto de permisos es de 10 240 bytes. | No                |
| Número de funciones de IAM (conjuntos de permisos) Cuenta de AWS que se pueden actualizar a la vez | 1                                                                                                                                                           | No                |

<sup>1</sup>AWS Identity and Access Management (IAM) establece una cuota de 10 políticas gestionadas por función. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas



gestionadas asociadas a una función de IAM en la consola de Service Quotas para cada uno de los Cuentas de AWS lugares en los que desee implementar el conjunto de permisos.

 Note

[Administre Cuentas de AWS con conjuntos de permisos](#) se aprovisionan Cuentas de AWS como funciones de IAM o utilizan las funciones de IAM existentes y, por lo tanto Cuentas de AWS, respetan las cuotas de IAM. Para obtener más información sobre las cuotas asociadas a los roles de IAM, consulte [Cuotas de IAM y STS](#).

## Cuotas de Active Directory

| Recurso                                                                 | Cuota predeterminada | Se puede aumentar |
|-------------------------------------------------------------------------|----------------------|-------------------|
| Número de directorios conectados que se puede tener de forma simultánea | 1                    | No                |

## Cuotas de almacén de identidades de IAM Identity Center

| Recurso                                                                                | Cuota predeterminada | Se puede aumentar |
|----------------------------------------------------------------------------------------|----------------------|-------------------|
| Número de usuarios admitidos en IAM Identity Center                                    | 200 000              | Sí                |
| Número de grupos admitidos en IAM Identity Center                                      | 100000               | Sí                |
| Número de grupos únicos que se pueden utilizar para evaluar los permisos de un usuario | 1 000                | No                |

# Límites de solicitudes de IAM Identity Center

| Recurso                         | Cuota predeterminada                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Centro de identidad de IAM APIs | <p>APIs Los <a href="#">centros de identidad de IAM</a> tienen un límite de aceleración colectivo de 20 transacciones por segundo (TPS). Por ejemplo APIs, puede abrir un caso de soporte para solicitar un aumento del límite. La API de <a href="#">CreateAccountAssignment</a> escritura tiene un límite de 15 llamadas asíncronas pendientes. Este límite no se puede aumentar.</p> |
| Almacén de identidades APIs     | <p><a href="#">Identity Store APIs</a> tiene un límite máximo de 20 transacciones por segundo (TPS) por API. Este límite se aplica a cada instancia de Identity Store. Puede abrir un caso de soporte para solicitar un aumento del límite.</p>                                                                                                                                         |
| SCIM APIs                       | <p>Los <a href="#">SCIM APIs</a> tienen límites de 25 transacciones por segundo (TPS) para escritura APIs y 40 TPS para lectura. APIs Estos límites se aplican a cada instancia de Identity Store. Puede abrir un caso de soporte para solicitar un aumento del límite.</p>                                                                                                             |

Si su instancia de IAM Identity Center está habilitada en varias Regiones de AWS, los límites máximos se aplicarán por igual a cada región habilitada. Por ejemplo, tendría un límite máximo de 20 TPS en el almacén de identidades de cada región APIs habilitada. [Para obtener más información sobre qué operaciones de API están disponibles en otras regiones, consulte la tabla correspondiente.](#)

## Cuotas de solicitud de servicio de OIDC

| Recurso                                                                                                                                                                         | Límite predeterminado (solicitudes por segundo) | Se puede aumentar                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------|
| <p>Solicita una tarifa desde una dirección remota para registrar un OAuth cliente público</p> <p>Se aplica a: <a href="#">RegisterClient</a></p>                                | 20                                              | Sí                                  |
| <p>Tasa de solicitudes de un cliente público registrado en el servicio OIDC</p> <p>Se aplica a: <a href="#">CreateToken</a>, <a href="#">StartDeviceAuthorization</a></p>       | 80                                              | Sí                                  |
| <p>Tasa de solicitudes de todos los clientes públicos registrados en la misma instancia de IAM Identity Center</p> <p>Se aplica a: <a href="#">CreateToken</a></p>              | 250                                             | Sí                                  |
| <p>Tasa de solicitudes desde una aplicación de IAM Identity Center registrada en la instancia de IAM Identity Center</p> <p>Se aplica a: <a href="#">CreateTokenWithIAM</a></p> | 80                                              | Sí                                  |
| <p>Tasa de generación de tokens de todas las aplicaciones de IAM Identity Center registradas en la misma instancia de</p>                                                       | 10                                              | Póngase en contacto con AWS Support |

| Recurso                                                                                                       | Límite predeterminado (solicitudes por segundo) | Se puede aumentar |
|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------|
| IAM Identity Center con la concesión del portador JWT<br><br><a href="#">Se aplica a: IAM CreateTokenWith</a> |                                                 |                   |

Si su instancia del IAM Identity Center está habilitada en varias Regiones de AWS, las tarifas de solicitud anteriores se aplican por igual a cada región habilitada. Por ejemplo, si la tasa de solicitudes permitida para registrar un OAuth cliente público desde una dirección remota es de 20 solicitudes por segundo, este rendimiento está disponible en cada región habilitada. Para obtener más información sobre qué operaciones de API están disponibles en otras regiones, consulta la [tabla](#) correspondiente.

## Cuotas adicionales

| Recurso                                                                                                     | Cuota predeterminada | Se puede aumentar |
|-------------------------------------------------------------------------------------------------------------|----------------------|-------------------|
| Número total de Cuentas de AWS aplicaciones que se pueden configurar* **                                    | 3 000                | Sí                |
| Total de instancias de IAM Identity Center por cuenta                                                       | 1                    | No                |
| Total de emisores de tokens de confianza                                                                    | 10                   | No                |
| Número total de grupos que se pueden asignar a un conjunto de permisos por Cuenta de AWS aplicación o a una | 100                  | No                |
| Número total de instancias Regiones de AWS habilitad                                                        | 3                    | Sí                |

| Recurso                                           | Cuota predeterminada | Se puede aumentar |
|---------------------------------------------------|----------------------|-------------------|
| as para una sola instancia de IAM Identity Center |                      |                   |

Por ejemplo, puede configurar 2750 cuentas y 250 aplicaciones, lo que da como resultado un total de 3000 cuentas y aplicaciones.

\*\* La operación de la API [ProvisionPermissionSet](#) puede aprovisionar un conjunto de permisos mediante la opción ALL\_PROVISIONED\_ACCOUNTS de, como máximo, 3500 Cuentas de AWS. Si necesita aprovisionar un conjunto de permisos de más de 3500 Cuentas de AWS, puede utilizar la operación de la API ProvisionPermissionSet con la opción AWS\_ACCOUNT, que aprovisiona el conjunto de permisos en una sola Cuenta de AWS. Puede realizar hasta tres llamadas simultáneas a ProvisionPermissionSet.

# Resolución de problemas de IAM Identity Center

La siguiente información puede ayudarle a solucionar algunos problemas comunes que puede encontrarse a la hora de configurar o utilizar la consola de IAM Identity Center.

## Problemas al crear una instancia de cuenta de IAM Identity Center

Es posible que se apliquen varias restricciones al crear una instancia de cuenta de IAM Identity Center. Si no puede crear una instancia de cuenta a través de la consola del IAM Identity Center o de la experiencia de configuración de una aplicación AWS gestionada compatible, compruebe los siguientes casos de uso:

- Marque otras Regiones de AWS Cuenta de AWS en las que esté intentando crear la instancia de cuenta. Tiene un límite de una instancia de IAM Identity Center por Cuenta de AWS. Para habilitar la aplicación, cambie a la Región de AWS instancia de IAM Identity Center o cambie a una cuenta sin una instancia de IAM Identity Center.
- Si su organización habilitó IAM Identity Center antes del 14 de septiembre de 2023, es posible que su administrador tenga que activar la creación de instancias de cuenta. Trabaje con el administrador para habilitar la creación de instancias de cuenta desde la consola de IAM Identity Center en la cuenta de administración.
- Es posible que el administrador haya creado una política de control de servicio para limitar la creación de instancias de cuenta de IAM Identity Center. Trabaje con el administrador para agregar su cuenta a la lista de permitidos.

## Recibe un error al intentar ver la lista de aplicaciones en la nube que están preconfiguradas para funcionar con IAM Identity Center

El siguiente error se produce cuando tienes una política que lo permite, `sso:ListApplications` pero no otros centros de identidad de IAM. APIs Actualice la política para resolver este error.

El `ListApplications` permiso autoriza varios: APIs

- La API `ListApplications`.
- Una API interna similar a la API `ListApplicationProviders` utilizada en la consola de IAM Identity Center.

Para ayudar a resolver la duplicación, la API interna ahora también autoriza el uso de la acción `ListApplicationProviders`. Para permitir la API pública `ListApplications`, pero denegar la API interna, la política debe incluir una instrucción que deniegue la acción `ListApplicationProviders`:

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplications",  
    "Resource": "<instanceArn>" // (or "*" for all instances)  
  }  
]
```

Para permitir la API interna, pero denegar `ListApplications`, la política tiene que permitir solo `ListApplicationProviders`. La API `ListApplications` se deniega si no se permite explícitamente.

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Cuando se actualicen sus políticas, póngase en contacto con nosotros Soporte para que eliminen esta medida proactiva.

# Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center

El Centro de Identidad de IAM ofrece una experiencia de depuración basada en la web para las afirmaciones de SAML creadas y enviadas por el Centro de Identidad de IAM, incluidos los atributos de estas afirmaciones, al acceder a Cuentas de AWS las aplicaciones de SAML desde el portal de acceso. AWS Para visualizar los detalles de una confirmación de SAML que genera IAM Identity Center, siga estos pasos:

1. Inicie sesión en el portal de acceso. AWS
2. Mientras está conectado al portal, mantenga pulsada la tecla Mayúscula, elija el mosaico de aplicaciones y suelte la tecla Mayúscula.
3. Revise la información de la página titulada You are now in administrator mode (Ahora está en modo administrador). Para conservar esta información y poder consultarla en el futuro, elija Copy XML (Copiar XML) y pegue el contenido en otro lugar.
4. Seleccione Enviar a <application> para continuar. Esta opción envía la confirmación al proveedor del servicio.

## Note

Es posible que algunas configuraciones de navegadores y sistemas operativos no admitan este procedimiento. Este procedimiento se ha probado en Windows 10 con los navegadores Firefox, Chrome y Edge.

## Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo

Si su proveedor de identidades (IdP) está configurado para aprovisionar usuarios al IAM Identity Center mediante la sincronización SCIM, es posible que se produzcan errores de sincronización durante el proceso de aprovisionamiento de usuarios. Esto puede indicar que la configuración de usuario de su IdP no es compatible con los requisitos del IAM Identity Center. Cuando esto suceda, el SCIM del IAM Identity Center APIs devolverá mensajes de error que proporcionan información sobre la causa raíz del problema. Puede localizar estos mensajes de error en los registros o en la



interfaz de usuario de su IdP. Como alternativa, puede encontrar información más detallada sobre los errores de aprovisionamiento en los [registros de AWS CloudTrail](#).

Para más información sobre la implementación del SCIM de IAM Identity Center, incluidas las especificaciones de los parámetros y operaciones obligatorios, opcionales y no admitidos para los objetos de usuario, consulte la [Guía para desarrolladores de la implementación del SCIM de IAM Identity Center](#) en la Guía para desarrolladores de SCIM.

Los siguientes motivos son algunos de los más comunes de este error:

1. El objeto de usuario del IdP carece de un nombre (de pila), un apellido (apellido) o and/or un nombre para mostrar.

Mensaje de error: «Se detectaron 2 errores de validación: el valor at '*name.givenName*' no pudo cumplir la restricción: el miembro debe cumplir con el patrón de expresión regular: [\ p {L}\ p {M}\ p {N}\ p {P}\ t\n\ r] +; el valor en '*name.givenName*' no pudo cumplir la restricción: el miembro debe tener una longitud mayor o igual a 1»

- Solución: agregue un nombre (de pila), un apellido y un nombre para el objeto de usuario. Además, asegúrese de que las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP estén configuradas para enviar valores no vacíos a todos estos atributos.
2. Se está enviando al usuario más de un valor para un único atributo (también conocidos como “atributos de valores múltiples”). Por ejemplo, el usuario puede tener un número de teléfono fijo y laboral especificado en el IdP, o varios correos electrónicos o direcciones físicas, y su IdP está configurado para intentar sincronizar varios o todos los valores de ese atributo.

Mensaje de error: «El atributo de la lista *emails* supera el límite permitido de 1»

- Opciones de solución:
  - i. Actualice las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP para enviar solo un valor único para un atributo determinado. Por ejemplo, configure una asignación que envíe solo el número de teléfono laboral de cada usuario.
  - ii. Si los atributos adicionales se pueden eliminar de forma segura del objeto de usuario del IdP, puede eliminar los valores adicionales y dejar uno o cero valores establecidos para ese atributo del usuario.

- iii. Si el atributo no es necesario para realizar ninguna acción AWS, elimine la asignación de ese atributo de las asignaciones de aprovisionamiento de SCIM para objetos de usuario en su IdP.
3. Su IdP intenta hacer coincidir a los usuarios del objetivo (en este caso, IAM Identity Center) en función de varios atributos. Como se garantiza que los nombres de usuario sean únicos en una instancia determinada de IAM Identity Center, solo tiene que especificar `username` como atributo utilizado para la coincidencia.
  - Solución: asegúrese de que la configuración de SCIM de su IdP utilice solo un atributo para coincidir con los usuarios de IAM Identity Center. Por ejemplo, la asignación de `username` o `userPrincipalName` del IdP al atributo `userName` de SCIM para el aprovisionamiento en IAM Identity Center será correcto y suficiente para la mayoría de las implementaciones.

## Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo

Si tiene problemas de sincronización del IAM Identity Center al aprovisionar usuarios o grupos en un proveedor de identidades (IdP) externo, podría deberse a que los usuarios o grupos de su IdP externo no tengan valores de atributos únicos. Es posible que aparezca el siguiente mensaje de error en el IdP externo:

Se negó a crear un nuevo recurso duplicado

Este problema se puede producir en el siguiente escenario:

- Escenario 1
  - Está utilizando atributos no únicos personalizados en su IdP externo para los atributos que deben ser únicos en el IAM Identity Center. Los usuarios o grupos existentes del IAM Identity Center no se sincronizan con su IdP.
- Escenario 2
  - Intenta crear usuarios con atributos duplicados para los atributos que deben ser únicos en el IAM Identity Center.
    - Por ejemplo, crea o tiene un usuario existente del IAM Identity Center con los siguientes atributos:
      - Nombre de usuario: Jane Doe
      - Dirección de correo electrónico principal: `jane_doe@example.com`

- A continuación, intente crear otro usuario en su IdP externo con los siguientes atributos:
  - Nombre de usuario: Richard Doe
  - Dirección de correo electrónico principal: jane\_doe@example.com
  - El IdP externo intenta sincronizar y crear el usuario en el IAM Identity Center. Sin embargo, estas acciones fallan porque ambos usuarios tienen valores duplicados para una dirección de correo electrónico principal que debe ser única.

El nombre de usuario, la dirección de correo electrónico principal y el identificador externo deben ser únicos para que los usuarios del IdP externo se sincronicen correctamente con IAM Identity Center. Del mismo modo, el nombre del grupo debe ser único para que los grupos de IdP externos se sincronicen correctamente con el IAM Identity Center.

La solución consiste en revisar los atributos de la fuente de identidad y asegurarse de que son únicos.

## Los usuarios no pueden iniciar sesión cuando su nombre de usuario está en formato UPN

Es posible que los usuarios no puedan iniciar sesión en el portal de AWS acceso en función del formato que utilizan para introducir su nombre de usuario en la página de inicio de sesión. En la mayoría de los casos, los usuarios pueden iniciar sesión en el portal de usuarios con su nombre de usuario normal, su nombre de inicio de sesión de nivel inferior (DOMAIN\UserName) o su nombre de inicio de sesión UPN (). UserName@Corp.Example.com La excepción a esto se produce cuando IAM Identity Center utiliza un directorio conectado que se ha habilitado con MFA y el modo de verificación se ha establecido en Context-aware o en Always-on. En este escenario, los usuarios deben iniciar sesión con su nombre de inicio de sesión de nivel inferior (DOMAIN\). UserName Para obtener más información, consulte [MFA para usuarios de Identity Center](#). Para obtener información general sobre los formatos de nombre de usuario que se utilizan para iniciar sesión en Active Directory, consulte [Formatos de nombre de usuario](#) en el sitio web de documentación de Microsoft.

## Al modificar un rol de IAM, aparece el error: “No se puede realizar la operación en el rol protegido”.

Al revisar las funciones de IAM en una cuenta, es posible que veas que los nombres de las funciones comienzan por «SSO\_». AWSReserved Se trata de los roles que el servicio de IAM Identity Center

ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta. Si se intenta modificar estos roles desde la consola de IAM, se producirá el siguiente error:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoLeName_Here' -  
this role is only modifiable by AWS'
```

Estas funciones solo se pueden modificar desde la consola de administración de IAM Identity Center, que se encuentra en la cuenta de administración de AWS Organizations. Una vez modificado, puede transferir los cambios a las cuentas de AWS a las que esté asignado.

## Los usuarios del directorio no pueden restablecer su contraseña

Cuando un usuario del directorio restablece su contraseña mediante la opción ¿Ha olvidado su contraseña? al iniciar sesión en el portal de AWS acceso, su nueva contraseña debe cumplir con la política de contraseñas predeterminada, tal como se describe en [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#)

Si un usuario introduce una contraseña que cumple con la política y, a continuación, recibe el error `We couldn't update your password`, compruebe si AWS CloudTrail se ha registrado el error. Para ello, busque en la consola del historial de eventos o CloudTrail utilice el siguiente filtro:

```
"UpdatePassword"
```

Si el mensaje indica lo siguiente, es posible que deba ponerse en contacto con el servicio de asistencia:

```
"errorCode": "InternalFailure",  
"errorMessage": "An unknown error occurred"
```

Otra posible causa de este problema está en la convención de nomenclatura que se aplicó al valor del nombre de usuario. Las convenciones de nomenclatura deben seguir patrones específicos, como `“surname.givenName”`. Sin embargo, algunos nombres de usuario pueden ser bastante largos o contener caracteres especiales, lo que puede provocar que se eliminen caracteres en la llamada a la API y, por lo tanto, se produzca un error. Puede intentar restablecer la contraseña con un usuario de prueba de la misma manera para comprobar si es así.

Si el problema persiste, póngase en contacto con el [centro de soporte de AWS](#).

## En un conjunto de permisos se hace referencia a mi usuario, pero no puede acceder a las cuentas o aplicaciones asignadas

Este problema se puede producir si utilizas el Sistema de administración de identidades entre dominios (SCIM) para el aprovisionamiento automático con un proveedor de identidad externo. En concreto, cuando se elimina un usuario o el grupo al que pertenecía el usuario y se vuelve a crear con el mismo nombre de usuario (para los usuarios) o nombre (para los grupos) en el proveedor de identidad, se crea un nuevo identificador interno único para el nuevo usuario o grupo en IAM Identity Center. Sin embargo, IAM Identity Center aún conserva una referencia al identificador anterior en su base de datos de permisos, de modo que el nombre del usuario o grupo sigue apareciendo en la interfaz de usuario, pero se produce un error en el acceso. Esto se debe a que el ID de usuario o grupo subyacente al que hace referencia la interfaz de usuario ya no existe.

Para restablecer el Cuenta de AWS acceso en este caso, puede eliminar el acceso del usuario o grupo anterior de los Cuenta de AWS lugares a los que estaba asignado originalmente y, a continuación, volver a asignar el acceso al usuario o grupo. Esto actualiza el conjunto de permisos con el identificador correcto para el nuevo usuario o grupo. Del mismo modo, para restablecer el acceso a la aplicación, puede eliminar el acceso del usuario o grupo de la lista de usuarios asignados a esa aplicación y, a continuación, volver a agregar el usuario o grupo.

También puede comprobar si se AWS CloudTrail ha registrado el error buscando en los CloudTrail registros los eventos de sincronización de SCIM que hagan referencia al nombre del usuario o grupo en cuestión.

## No puedo configurar correctamente mi aplicación del catálogo de aplicaciones

Si ha agregado una aplicación del catálogo de aplicaciones en IAM Identity Center, tenga en cuenta que cada proveedor de servicios proporciona su propia documentación detallada. Puede acceder a esta información desde la pestaña Configuración de la aplicación en la consola de IAM Identity Center.

Si el problema está relacionado con la configuración de la confianza entre la aplicación del proveedor de servicios y IAM Identity Center, consulte el manual de instrucciones para conocer los pasos a seguir para la resolución de problemas.

## Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo

Este error puede producirse por varios motivos, pero uno de los más comunes es la falta de coincidencia entre la información del usuario incluida en la solicitud de SAML y la información del usuario en IAM Identity Center.

Para que un usuario de IAM Identity Center inicie sesión correctamente al utilizar un IdP externo como fuente de identidad, debe cumplirse lo siguiente:

- El formato de nameID de SAML (configurado en su proveedor de identidad) debe ser “correo electrónico”
- El valor de nameID debe ser una cadena con el formato correcto (RFC2822) (user@domain.com)
- El valor del nameID debe coincidir exactamente con el nombre de usuario de un usuario existente en IAM Identity Center (no importa si la dirección de correo electrónico en IAM Identity Center coincide o no; la coincidencia entrante se basa en el nombre de usuario)
- La implementación de la federación SAML 2.0 en IAM Identity Center solo admite una confirmación en la respuesta de SAML entre el proveedor de identidades y IAM Identity Center. No admite las confirmaciones de SAML cifradas.
- Si los [Atributos para controlar el acceso](#) están habilitados en su cuenta de IAM Identity Center, se aplican las siguientes confirmaciones:
  - El número de atributos asignados en la solicitud de SAML debe ser 50 o inferior.
  - La solicitud de SAML no debe contener atributos con varios valores.
  - La solicitud de SAML no debe contener varios atributos con el mismo nombre.
  - El atributo no debe contener XML estructurado como valor.
  - El formato del nombre debe ser un formato especificado por SAML y no un formato genérico.

### Note

IAM Identity Center no crea usuarios o grupos “justo a tiempo” para nuevos usuarios o grupos mediante la federación SAML. Esto significa que el usuario debe haber sido creado previamente en IAM Identity Center, ya sea de forma manual o mediante un aprovisionamiento automático, para poder iniciar sesión en IAM Identity Center.

Este error también se puede producir cuando el punto de conexión del Servicio de Consumidor de Aserción (ACS) configurado en su proveedor de identidad no coincide con la URL de ACS proporcionada por su instancia de IAM Identity Center. Asegúrese de que estos 2 valores coincidan exactamente.

Además, puede solucionar aún más los errores de inicio de sesión de un proveedor de identidad externo consultando AWS CloudTrail y filtrando el nombre del evento Login. ExternalId PDirectory

## Error: “No se pudieron habilitar los atributos del control de acceso”

Este error se puede producir si el usuario que habilita ABAC no tiene los permisos de `iam:UpdateAssumeRolePolicy` necesarios para habilitar [Atributos para controlar el acceso](#).

## El mensaje “El navegador no es compatible” aparece cuando intento registrar un dispositivo para MFA

WebAuthn actualmente es compatible con los navegadores web Google Chrome, Mozilla Firefox, Microsoft Edge y Apple Safari, así como con las plataformas Windows 10 y Android. Algunos componentes de la WebAuthn compatibilidad pueden variar, como la compatibilidad con el autenticador de plataforma en los navegadores macOS e iOS. Si los usuarios intentan registrar WebAuthn dispositivos en un navegador o una plataforma no compatibles, verán determinadas opciones que no son compatibles o recibirán un mensaje de error que indica que no se admiten todos los métodos compatibles. En estos casos, consulte [FIDO2: Autenticación web \(WebAuthn\)](#) para obtener más información sobre browser/platform el soporte. Para obtener más información sobre WebAuthn el Centro de identidades de IAM, consulte [FIDO2 autenticadores](#).

## El grupo “Usuarios de dominio” de Active Directory no se sincroniza correctamente con IAM Identity Center

El grupo de usuarios de dominio de Active Directory es el “grupo principal” predeterminado para los objetos de usuario de AD. IAM Identity Center no puede leer los grupos principales de Active Directory ni sus membresías. Al asignar el acceso a los recursos o aplicaciones de IAM Identity Center, utilice grupos distintos del grupo de usuarios del dominio (u otros grupos asignados como grupos principales) para que la membresía a los grupos se refleje correctamente en el almacén de identidades de IAM Identity Center.

## Error de credenciales de MFA no válidas

Este error se puede producir cuando un usuario intenta iniciar sesión en IAM Identity Center con una cuenta de un proveedor de identidad externo (por ejemplo, Okta o Microsoft Entra ID) antes de que su cuenta esté completamente aprovisionada en IAM Identity Center mediante el protocolo SCIM. Una vez que la cuenta de usuario se aprovisiona en IAM Identity Center, este problema debería resolverse. Confirme que la cuenta se haya aprovisionado en IAM Identity Center. Si no es así, compruebe los registros de aprovisionamiento en el proveedor de identidades externo.

## El mensaje “Se ha producido un error inesperado” aparece cuando intento registrarme o iniciar sesión con una aplicación de autenticación

Los sistemas de contraseña temporal de un solo uso (TOTP) basados en el tiempo, como los que utiliza IAM Identity Center en combinación con las aplicaciones de autenticación basadas en código, se basan en la sincronización horaria entre el cliente y el servidor. Asegúrese de que el dispositivo en el que está instalada la aplicación de autenticación esté sincronizado correctamente con una fuente horaria fiable o configure manualmente la hora del dispositivo para que coincida con una fuente fiable, como el NIST (<https://www.time.gov/>) u otras equivalentes. local/regional

## Aparece el mensaje de error “No es usted, somos nosotros” cuando intento iniciar sesión en IAM Identity Center

Este error indica que hay un problema de configuración con su instancia de IAM Identity Center o con el proveedor de identidades (IdP) externo que IAM Identity Center utiliza como fuente de identidad. Le recomendamos que realice las siguientes acciones:

- Compruebe la configuración de fecha y hora del dispositivo que utiliza para iniciar sesión. Recomendamos que establezca que la fecha y la hora se ajusten automáticamente. Si no está disponible, le recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.
- Compruebe que el certificado de IdP cargado en el IAM Identity Center es el mismo que el que proporcionó su IdP. Para comprobar el certificado desde la consola del IAM Identity Center, vaya a Configuración. En la pestaña Fuente de identidad, elija Acción y, a continuación, Administrar



autenticación. Si los certificados del IdP y del IAM Identity Center no coinciden, importe un certificado nuevo al IAM Identity Center.

- Asegúrese de que el formato NameID del archivo de metadatos de su proveedor de identidad sea el siguiente:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Si utiliza AD Connector de AWS Directory Service como proveedor de identidad, compruebe que las credenciales de la cuenta de servicio son correctas y no han caducado. Consulte [Actualización de las credenciales de su cuenta de servicio de Conector de AD en AWS Directory Service](#) para obtener más información.

## Mis usuarios no reciben correos electrónicos de IAM Identity Center

Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Su sistema de correo electrónico se debe configurar de manera que acepte los mensajes con estas direcciones de correo electrónico como remitente y no los trate como correo basura o spam.

## Error: no puedes delete/modify/remove/assign acceder a los conjuntos de permisos aprovisionados en la cuenta de administración

Este mensaje indica que la característica [Administración delegada](#) está habilitada y que la operación que intentó anteriormente solo la puede realizar correctamente una persona con permisos de cuenta de administración en AWS Organizations. Para resolver este problema, inicie sesión como usuario con estos permisos e intente volver a realizar la tarea o asigne esta tarea a alguien que cuente con los permisos correctos. Para obtener más información, consulte [Registro de una cuenta de miembro](#).

## Error: no se encontró el token de sesión o no es válido

Este error puede producirse cuando un cliente, como un navegador web AWS Toolkit AWS CLI, o intenta utilizar una sesión revocada o invalidada en el servidor. Para corregir este problema, vuelva a la aplicación de cliente o al sitio web e inténtelo de nuevo, incluso vuelva a iniciar sesión si se le solicita. A veces, esto puede requerir que también canceles las solicitudes pendientes, como un intento de conexión pendiente desde tu AWS Toolkit IDE.

# Los miembros del grupo de dominios de confianza no se sincronizan con el Centro de Identidad de IAM

Si un grupo de seguridad se sincroniza correctamente con el Centro de Identidad de IAM, pero sus miembros de un dominio local de confianza no aparecen en el Centro de Identidad de IAM, esto puede deberse a que el grupo reside en Foreign Security Principal ( ) AWS Managed Microsoft AD y contiene a Foreign Security Principal (FSPs), que representa a los usuarios de un dominio de confianza.

Pruebe los siguientes pasos para solucionar un error:

- Sincronice los grupos directamente desde el dominio de confianza: en lugar de sincronizar un grupo AWS Managed Microsoft AD que contiene miembros de varios dominios, cree y sincronice el grupo directamente desde el dominio local de confianza. Este enfoque funciona porque IAM Identity Center puede acceder a los objetos de usuario reales del dominio de origen.
- Compruebe los permisos de la cuenta de servicio: asegúrese de que la cuenta de servicio del Centro de Identidad de IAM tenga los permisos `ReadProperties` y `ListContents` permisos necesarios para los objetos de usuario del dominio de confianza.

## Solucione los problemas de las claves administradas por el cliente en AWS IAM Identity Center

En este tema se describen los errores más comunes relacionados con las claves gestionadas por el cliente que se pueden encontrar al utilizarlas AWS IAM Identity Center y se proporcionan los pasos de solución de problemas para resolverlos.

### Acceso denegado: problema con el permiso de descifrado de KMS

Error: «El usuario xxxxxxxx no está autorizado a realizar la operación de kms: descifrado en el recurso asociado a este texto cifrado porque ninguna política basada en la identidad permite la acción de descifrado» kms:

El usuario o la entidad principal de IAM carecen del permiso de kms:Decrypt necesario en su política de IAM o en la política de claves de KMS.

Solución de problemas con: AWS CloudTrail

1. Busque `kms.amazonaws.com` eventos en CloudTrail
2. Busque el nombre del evento `Decrypt`
3. Revise los campos `errorCode` y `errorMessage`
4. Compruebe `userIdentity` para confirmar qué entidad principal intentó realizar la operación

Para resolver este problema, conceda al usuario o a la entidad principal de IAM permisos de acceso `kms:Decrypt` en su política de IAM y en la política de claves de KMS. Para obtener más información, consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).

## AWS errores de inicio de sesión en aplicaciones gestionadas con una clave KMS gestionada por el cliente habilitada en el IAM Identity Center

Si ningún usuario del Identity Center puede iniciar sesión en las aplicaciones AWS gestionadas y usted tiene habilitada una clave de KMS gestionada por el cliente en su instancia del Identity Center de IAM, compruebe que la política de claves de KMS concede a las aplicaciones AWS gestionadas permisos para utilizar la clave de KMS gestionada por el cliente. Para obtener más información, consulte [Instrucciones básicas de KMS y políticas de IAM](#).

## AWS Se produce un error en la asignación and/or de usuarios durante la instalación de aplicaciones gestionadas con una clave KMS gestionada por el cliente y habilitada en el IAM Identity Center

Error: «El usuario xxxxxxxx no está autorizado a realizar la operación de `kms:descifrado` en el recurso asociado a este texto cifrado porque ninguna política basada en la identidad permite la acción de descifrado» `kms:`

El usuario o la entidad principal de IAM carecen del permiso de `kms:Decrypt` necesario en su política de IAM o en la política de claves de KMS.

Solución de problemas con: CloudTrail

1. Busque el nombre del evento `Decrypt`
2. Revise los campos `errorCode` y `errorMessage`
3. Compruebe `userIdentity` para confirmar qué entidad principal intentó realizar la operación

Para resolver este problema, conceda al usuario o a la entidad principal de IAM permisos de acceso `kms:Decrypt` en su política de IAM y en la política de claves de KMS. Para obtener más información, consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).

## Problema de permisos de KMS: configurar la clave administrada por el cliente con AWS IAM Identity Center

El usuario o la entidad principal de IAM carece de uno o más de los permisos de KMS necesarios (`kms:Decrypt`, `kms:Encrypt`, `kms:GenerateDataKey`, `kms:DescribeKey`) al habilitar la clave administrada por el cliente.

Solución de problemas con CloudTrail:

1. Busque `Decrypt`, `Encrypt`, `GenerateDataKey` o eventos `DescribeKey`
2. Revise los campos `errorCode` y `errorMessage`
3. Compruebe `userIdentity` para confirmar qué entidad principal intentó realizar la operación

Para resolver este problema, conceda todos los permisos de KMS necesarios al usuario o a la entidad principal de IAM en su política basada en la identidad o en la política de claves de KMS. Para obtener más información, consulte [Implementación de claves KMS administradas por el cliente en AWS IAM Identity Center](#).

## AWS errores de inicio de sesión en el portal de acceso con una clave KMS gestionada por el cliente y habilitada en el IAM Identity Center

Error: «Código de error: 0001: el acceso IdentityCenter al servicio está bloqueado. Ponte en contacto con tu IdentityCenter administrador para conocer los pasos adicionales».

Si los usuarios no pueden iniciar sesión en el portal de AWS acceso y tienes habilitada una clave KMS gestionada por el cliente en tu instancia del IAM Identity Center, comprueba que la política de claves de KMS concede los permisos necesarios para Identity Center e Identity Store. Para obtener más información, consulte [Instrucciones básicas de KMS y políticas de IAM](#).

# Solucione los problemas de configuración multirregional en AWS IAM Identity Center

En este tema se describen los errores más comunes relacionados con la configuración multirregional que se pueden encontrar al utilizarlos AWS IAM Identity Center y se proporcionan los pasos de solución de problemas para resolverlos.

## La región en la que quiero replicar mi instancia de IAM Identity Center no está disponible en la consola de IAM Identity Center

Primero debe crear una clave de réplica para la clave de KMS gestionada por el cliente en la región en la que desee replicar su instancia de IAM Identity Center. Una vez creada la clave de réplica, verá la región en la lista de regiones disponibles para las réplicas. Para obtener más información, consulte [the section called “Paso 1: Crear una clave de réplica”](#).

## AWS errores de inicio de sesión en aplicaciones gestionadas en otra región

Si ningún usuario del Centro de Identidad de IAM puede iniciar sesión en las aplicaciones AWS gestionadas de otra región después de añadir la región al Centro de Identidad de IAM, confirme que ha configurado la URL del Servicio de Atención al Consumidor de Afirmaciones (ACS) de la región adicional en el proveedor de identidad externo, tal y como se describe en [the section called “Paso 3: Actualizar la configuración del IdP externo”](#). Además, confirme que sus usuarios tengan conectividad con la región.

# Historial del documento

En la siguiente tabla se describen las adiciones importantes a la AWS IAM Identity Center documentación. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

- Última actualización importante de la documentación: 21 de octubre de 2025

| Cambio                                                                                    | Descripción                                                                                                                                                                     | Fecha                   |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Soporte multirregional</a>                                                    | Se agregó soporte multirregional, que incluye la replicación en regiones adicionales y el Cuenta de AWS acceso y uso de aplicaciones AWS administradas en regiones adicionales. | 2 de febrero de 2026    |
| <a href="#">Política AWS gestionada actualizada</a>                                       | Se actualizó la política AWSIdentityCenterExternalManagementPolicy AWS administrada para cambiar el ARN del inquilino de aprovisionamiento.                                     | 5 de diciembre de 2025  |
| <a href="#">Nuevo tema de política AWS gestionada</a>                                     | Se han añadido detalles para la política AWSIdentityCenterExternalManagementPolicy AWS gestionada.                                                                              | 21 de noviembre de 2025 |
| <a href="#">Instrucciones de auditoría y conciliación de aprovisionamiento automático</a> | Se agregó una guía para auditar y conciliar los usuarios, grupos y membresías de grupos aprovisionados automáticamente por SCIM                                                 | 17 de octubre de 2025   |

mediante Identity Store y comandos. APIs AWS CLI

### [Cuotas de solicitud de servicio de OIDC](#)

Se agregaron cuotas de solicitud de servicios de la OIDC, incluidos los límites de tarifas para el registro de OAuth clientes, la creación de tokens y otras operaciones de la OIDC.

13 de octubre de 2025

### [Actualizaciones de la política AWS gestionada](#)

El Centro de Identidad de IAM ha actualizado las políticas AWSSSOMasterAccountAdministrator gestionadas e AWSSSODirectoryReadOnly incluye AWS KMS los permisos necesarios para las instancias del Centro de Identidad de IAM que utilizan claves gestionadas por el cliente para el cifrado. AWSSSOMemberAccountAdministrator AWSSSODirectoryAdministrator

17 de septiembre de 2025

### [Claves administradas por el cliente para el cifrado en reposo](#)

Se ha añadido la compatibilidad con las claves de KMS administradas por el cliente para cifrar los datos de identidad de los empleados en reposo.

17 de septiembre de 2025

|                                                                                                   |                                                                                                                                                                                                          |                          |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#"><u>Ejemplo de política basada en recursos para permitir la creación de tokens</u></a> | Se agregó un ejemplo de política basada en recursos que permite la creación de tokens para aplicaciones de clientes autorizadas.                                                                         | 16 de septiembre de 2025 |
| <a href="#"><u>Compatibilidad de las sesiones de usuario en segundo plano</u></a>                 | Se agregó contenido para las sesiones de usuario en segundo plano.                                                                                                                                       | 11 de agosto de 2025     |
| <a href="#"><u>Sesiones de consola con identidad mejorada</u></a>                                 | Terminología actualizada para las sesiones de consola mejoradas con identidad (anteriormente denominadas sesiones con reconocimiento de identidad).                                                      | 12 de mayo de 2025       |
| <a href="#"><u>Introducción a la reorganización</u></a>                                           | Se reorganizó el contenido de introducción para mejorar la claridad y la experiencia del usuario.                                                                                                        | 6 de mayo de 2025        |
| <a href="#"><u>Obsolescencia de la sincronización de AD con IAM Identity Center</u></a>           | Ya no puede aprovisionar a los usuarios de Active Directory con la sincronización de AD de IAM Identity Center. En su lugar, puede utilizar la sincronización de AD configurable de IAM Identity Center. | 17 de abril de 2025      |
| <a href="#"><u>Contenido actualizado para la sesión autenticada</u></a>                           | Se actualiza la duración de las sesiones de IAM Identity Center cuando se elimina la sesión del usuario.                                                                                                 | 2 de abril de 2025       |



|                                                                                      |                                                                                                                                  |                          |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">Actualizaciones de la política gestionada AWS</a>                        | Permisos actualizados para la política <code>AWSSS0ServiceRolePolicy</code> AWS gestionada.                                      | 11 de febrero de 2025    |
| <a href="#">Se mejoró el flujo de trabajo de habilitación de IAM Identity Center</a> | Se actualizó el flujo de trabajo para habilitar las instancias de organización y cuenta de IAM Identity Center.                  | 11 de febrero de 2025    |
| <a href="#">Actualizaciones para la activación de IAM Identity Center</a>            | Se actualizaron el contenido y los procedimientos para habilitar las instancias de organización y cuenta de IAM Identity Center. | 10 de octubre de 2024    |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Permisos actualizados para la política <code>AWSIAMIdentityCenterAllowListForIdentityContext</code> AWS gestionada.              | 2 de octubre de 2024     |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Permisos actualizados para la política <code>AWSSS0MasterAccountAdministrator</code> AWS gestionada.                             | 26 de septiembre de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Permisos actualizados para la política <code>AWSIAMIdentityCenterAllowListForIdentityContext</code> AWS gestionada.              | 4 de septiembre de 2024  |
| <a href="#">Actualizaciones de la sección “¿Qué es el IAM Identity Center?” tema</a> | Se actualizó el contenido que describe las ventajas y las capacidades del IAM Identity Center.                                   | 19 de agosto de 2024     |

|                                                               |                                                                                                        |                     |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 12 de julio de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 27 de junio de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 17 de mayo de 2024  |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 30 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSSSOMasterAccountAdministrator AWS gestionada.                | 26 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSSSOMemberAccountAdministrator AWS gestionada.                | 26 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Permisos actualizados para la política AWSSS0ReadOnly AWS gestionada.                                  | 26 de abril de 2024 |

[Actualizaciones de la política  
AWS gestionada](#)

Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

26 de abril de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

24 de abril de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

19 de abril de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

11 de abril de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Permisos actualizados para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

26 de noviembre de 2023

[Nuevo tema de política AWS  
gestionada](#)

Se han añadido detalles para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

15 de noviembre de 2023

[Guía de introducción mejorada sobre el uso de IAM Identity Center](#)

Contenido nuevo agregado para empezar a utilizar IAM Identity Center y crear un usuario administrativo

23 de septiembre de 2022

[Usuarios y grupos actualizados en la referencia de la API de Identity Center](#)

Esta actualización incluye referencias a la nueva creación, actualización y eliminación APIs en la Guía de referencia de la API de Identity Center.

31 de agosto de 2022

[AWS El inicio de sesión único \(AWS SSO\) pasó a llamarse IAM Identity Center AWS](#)

AWS presenta. AWS IAM Identity Center IAM Identity Center amplía las capacidades de AWS Identity and Access Management (IAM) para ayudarle a gestionar de forma centralizada las cuentas y el acceso a las aplicaciones para los usuarios de su plantilla . Las características de IAM Identity Center incluyen la asignación de aplicaciones, los permisos para varias cuentas y un portal de acceso AWS .

26 de julio de 2022

[Compatibilidad con límites de permisos y política administrada por el cliente en los conjuntos de permisos](#)

Se agregó contenido para usar políticas AWS administradas y administradas por el cliente AWS Identity and Access Management (IAM) con conjuntos de permisos.

14 de julio de 2022

|                                                                          |                                                                                                                                                                                  |                         |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Support para AWS regiones habilitadas manualmente</a>        | Contenido agregado para utilizar IAM Identity Center en regiones habilitadas de forma manual.                                                                                    | 15 de junio de 2022     |
| <a href="#">Actualizaciones para las políticas AWS gestionadas</a>       | Permisos actualizados para la política AWSSS0ServiceRolePolicy AWS gestionada.                                                                                                   | 11 de mayo de 2022      |
| <a href="#">Compatibilidad con la administración delegada</a>            | Contenido agregado para la característica de administración delegada.                                                                                                            | 11 de mayo de 2022      |
| <a href="#">Actualizaciones de las políticas AWS gestionadas</a>         | Se actualizaron los permisos para las AWSSS0MasterAccountAdministrator políticas AWSSS0MemberAccountAdministrator administradas y las políticas AWSSS0ReadOnlyAWS administradas. | 28 de abril de 2022     |
| <a href="#">Compatibilidad con la sincronización con AD configurable</a> | Contenido agregado para la característica de sincronización con AD configurable.                                                                                                 | 14 de abril de 2022     |
| <a href="#">Nuevo tema sobre políticas AWS administradas</a>             | Se han añadido detalles para la política AWSSS0MasterAccountAdministrator AWS gestionada.                                                                                        | 4 de agosto de 2021     |
| <a href="#">Actualizaciones para cuotas</a>                              | Ajustes en las tablas de cuotas.                                                                                                                                                 | 21 de diciembre de 2020 |

|                                                                                    |                                                                                                                            |                         |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Nuevos ejemplos de políticas</a>                                       | Nuevos ejemplos agregados de políticas administradas por el cliente y actualizaciones a la sección de permisos requeridos. | 21 de diciembre de 2020 |
| <a href="#">Compatibilidad con el control de acceso basado en atributos (ABAC)</a> | Contenido agregado para la característica ABAC.                                                                            | 24 de noviembre de 2020 |
| <a href="#">Compatibilidad con inscripción forzosa de MFA</a>                      | Actualizaciones para exigir a los usuarios que inscriban un dispositivo MFA al iniciar sesión.                             | 23 de noviembre de 2020 |
| <a href="#">Support para WebAuthn</a>                                              | Contenido agregado para la nueva característica WebAuthn.                                                                  | 20 de noviembre de 2020 |
| <a href="#">Compatibilidad con Ping Identity</a>                                   | Contenido agregado para integrarlo con productos de Ping Identity en calidad de proveedor de identidad externo compatible. | 26 de octubre de 2020   |
| <a href="#">Support para OneLogin</a>                                              | Contenido agregado para integrarlo con OneLogin en calidad de proveedor de identidad externo compatible.                   | 31 de julio de 2020     |
| <a href="#">Compatibilidad con Okta</a>                                            | Contenido agregado para integrarlo con Okta en calidad de proveedor de identidad externo compatible.                       | 28 de mayo de 2020      |

|                                                                                                                 |                                                                                                                                            |                         |
|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#"><u>Compatibilidad con proveedores de identidad externos</u></a>                                     | Referencias modificadas del directorio a la fuente de identidad y contenido agregado para admitir a los proveedores de identidad externos. | 26 de noviembre de 2019 |
| <a href="#"><u>Nueva configuración de MFA</u></a>                                                               | Tema de la verificación en 2 pasos eliminado y nuevo tema de MFA agregado en su lugar.                                                     | 24 de octubre de 2019   |
| <a href="#"><u>Nueva configuración para agregar la verificación en 2 pasos</u></a>                              | Contenido agregado sobre cómo habilitar la verificación en dos pasos para los usuarios.                                                    | 16 de enero de 2019     |
| <a href="#"><u>Support para la duración de la sesión en AWS las cuentas</u></a>                                 | Se agregó contenido sobre cómo configurar la duración de la sesión de una AWS cuenta.                                                      | 30 de octubre de 2018   |
| <a href="#"><u>Nueva opción para usar el directorio de Identity Center</u></a>                                  | Contenido agregado para elegir un directorio de Identity Center o conectarse a un directorio existente en Active Directory.                | 17 de octubre de 2018   |
| <a href="#"><u>Compatibilidad con el estado de retransmisión y la duración de la sesión en aplicaciones</u></a> | Se ha agregado contenido sobre el estado de retransmisión y la duración de la sesión para las aplicaciones.                                | 10 de octubre de 2018   |

[Compatibilidad adicional con las nuevas aplicaciones](#)

Se agregó 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, y UserEcho al catálogo de aplicaciones.

3 de agosto de 2018

[Compatibilidad con el acceso de cuentas múltiples a cuentas de administración](#)

Contenido agregado sobre cómo delegar a los usuarios el acceso de múltiples cuentas a una cuenta de administración.

9 de julio de 2018

[Compatibilidad con las nuevas aplicaciones](#)

Se agregó DocuSign, Keeper Security, y SugarCRM al catálogo de aplicaciones.

16 de marzo de 2018

[Obtener credenciales temporales para acceder a la CLI](#)

Se agregó información sobre cómo obtener credenciales temporales para ejecutar AWS CLI comandos.

22 de febrero de 2018

[Nueva guía](#)

Esta es la primera versión de la Guía del usuario de IAM Identity Center.

7 de diciembre de 2017



# AWS Glosario

Para obtener la AWS terminología más reciente, consulte el [AWS glosario](#) de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.