aws

Guide de l’utilisateur

Studio de recherche et d'ingénierie

Studio de recherche et d'ingénierie: Guide de l’utilisateur

Table of Contents

Présentation de

> **Important**
>
> Cette version du guide de l'utilisateur couvre la version 2025.03 de Research and Engineering Studio sur. AWS Pour la version actuelle, consultez le guide de l' AWS utilisateur du studio de recherche et d'ingénierie.

Research and Engineering Studio (RES) est un produit open source AWS pris en charge qui permet aux administrateurs informatiques de fournir un portail Web aux scientifiques et aux ingénieurs pour exécuter des charges de travail informatiques techniques. AWS RES fournit aux utilisateurs une interface unique leur permettant de lancer des bureaux virtuels sécurisés pour mener des recherches scientifiques, concevoir des produits, effectuer des simulations techniques ou effectuer des analyses de données. Les utilisateurs peuvent se connecter au portail RES en utilisant leurs identifiants d'entreprise existants et travailler sur des projets individuels ou collaboratifs.

Les administrateurs peuvent créer des espaces de collaboration virtuels appelés projets pour un ensemble spécifique d'utilisateurs afin d'accéder à des ressources partagées et de collaborer. Les administrateurs peuvent créer leurs propres piles de logiciels d'application (à l'aide d'Amazon Machine Images ou AMIs), autoriser les utilisateurs de RES à lancer des bureaux virtuels Windows ou Linux, et autoriser l'accès aux données du projet via des systèmes de fichiers partagés. Les administrateurs peuvent attribuer des piles de logiciels et des systèmes de fichiers et restreindre l'accès aux seuls utilisateurs du projet. Les administrateurs peuvent utiliser la télémétrie intégrée pour surveiller l'utilisation de l'environnement et résoudre les problèmes des utilisateurs. Ils peuvent également établir des budgets pour des projets individuels afin d'éviter une surconsommation de ressources. Le produit étant open source, les clients peuvent également personnaliser l'expérience utilisateur du portail RES en fonction de leurs propres besoins.

RES est disponible sans frais supplémentaires et vous ne payez que pour les AWS ressources nécessaires à l'exécution de vos applications.

Ce guide fournit une présentation de Research and Engineering Studio on AWS, de son architecture de référence et de ses composants, des considérations relatives à la planification du déploiement et des étapes de configuration pour le déploiement de RES sur le cloud Amazon Web Services (AWS).

Fonctionnalités et avantages

Research and Engineering Studio on AWS fournit les fonctionnalités suivantes :

Interface utilisateur basée sur le Web

RES fournit un portail Web que les administrateurs, les chercheurs et les ingénieurs peuvent utiliser pour accéder à leurs espaces de travail de recherche et d'ingénierie et les gérer. Les scientifiques et les ingénieurs n'ont pas besoin d'une expertise Compte AWS ou d'une expertise dans le cloud pour utiliser RES.

Configuration basée sur le projet

Utilisez des projets pour définir des autorisations d'accès, allouer des ressources et gérer les budgets pour un ensemble de tâches ou d'activités. Attribuez des piles logicielles spécifiques (systèmes d'exploitation et applications approuvées) et des ressources de stockage à un projet pour garantir la cohérence et la conformité. Surveillez et gérez les dépenses par projet.

Outils de collaboration

Les scientifiques et les ingénieurs peuvent inviter d'autres membres de leur projet à collaborer avec eux, en définissant les niveaux d'autorisation qu'ils souhaitent que ces collègues aient. Ces personnes peuvent se connecter à RES pour se connecter à ces ordinateurs de bureau.

Intégration à l'infrastructure de gestion des identités existante

Intégrez votre infrastructure de gestion des identités et de services d'annuaire existante pour permettre la connexion au portail RES avec l'identité d'entreprise existante d'un utilisateur et attribuer des autorisations aux projets en utilisant les appartenances d'utilisateurs et de groupes existantes.

Stockage permanent et accès aux données partagées

Pour permettre aux utilisateurs d'accéder aux données partagées par le biais de sessions de bureau virtuel, connectez-vous à vos systèmes de fichiers existants dans RES. Les services de stockage pris en charge incluent Amazon Elastic File System pour les ordinateurs de bureau Linux et Amazon FSx for NetApp ONTAP pour les ordinateurs de bureau Windows et Linux.

Surveillance et établissement de rapports

Utilisez le tableau de bord d'analyse pour surveiller l'utilisation des ressources par type d'instance, de pile logicielle et de type de système d'exploitation. Le tableau de bord fournit également une ventilation de l'utilisation des ressources par projet à des fins de reporting.

Gestion du budget et des coûts

Créez un lien AWS Budgets vers vos projets RES pour suivre les coûts de chaque projet. Si vous dépassez votre budget, vous pouvez limiter le lancement de sessions VDI.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à Research and Engineering Studio sur AWS :

Navigateur de fichiers

Un navigateur de fichiers fait partie de l'interface utilisateur RES où les utilisateurs actuellement connectés peuvent consulter leur système de fichiers.

Système de fichiers

Le système de fichiers agit comme un conteneur pour les données du projet (souvent appelées ensembles de données). Il fournit une solution de stockage dans les limites d'un projet et améliore la collaboration et le contrôle d'accès aux données.

Administrateur global

Délégué administratif ayant accès aux ressources RES partagées dans un environnement RES. La portée et les autorisations s'étendent sur plusieurs projets. Ils peuvent créer ou modifier des projets et désigner des propriétaires de projets. Ils peuvent déléguer ou attribuer des autorisations aux propriétaires et aux membres du projet. Parfois, la même personne agit en tant qu'administrateur RES en fonction de la taille de l'organisation.

Project

Un projet est une partition logique au sein de l'application qui sert de limite distincte pour les données et les ressources de calcul ; cela garantit la gouvernance du flux de données et empêche le partage des données et des hôtes VDI entre les projets.

Autorisations basées sur le projet

Les autorisations basées sur les projets décrivent une partition logique des données et des hôtes VDI dans un système où plusieurs projets peuvent exister. L'accès d'un utilisateur aux données et aux hôtes VDI au sein d'un projet est déterminé par le ou les rôles qui lui sont associés. Un utilisateur doit disposer d'un accès (ou d'une adhésion au projet) pour chaque projet auquel il a

besoin d'accéder. Dans le cas contraire, un utilisateur ne pourra pas accéder aux données du projet et VDIs s'il n'a pas obtenu d'adhésion.

Membre du projet

Utilisateur final des ressources RES (VDI, stockage, etc.). La portée et les autorisations sont limitées aux projets auxquels elles sont attribuées. Ils ne peuvent ni déléguer ni attribuer d'autorisations.

Propriétaire du projet

Délégué administratif ayant accès à un projet spécifique et en étant propriétaire. La portée et les autorisations sont limitées au (x) projet (s) dont ils sont propriétaires. Ils peuvent attribuer des autorisations aux membres du projet dans les projets dont ils sont propriétaires.

Pile logicielle

Les piles logicielles sont des Amazon Machine Images (AMI) avec des métadonnées spécifiques aux RES basées sur le système d'exploitation qu'un utilisateur a sélectionné pour approvisionner son hôte VDI.

Hôtes VDI

Les hôtes d'instances de bureau virtuel (VDI) permettent aux membres du projet d'accéder aux données et aux environnements informatiques spécifiques au projet, garantissant ainsi des espaces de travail sécurisés et isolés.

Pour une référence générale des AWS termes, voir le AWS glossaire dans la référence AWS générale.

Présentation de l'architecture

Cette section fournit un schéma d'architecture des composants déployés avec ce produit.

Diagramme d'architecture

Le déploiement de ce produit avec les paramètres par défaut déploie les composants suivants dans votre Compte AWS.

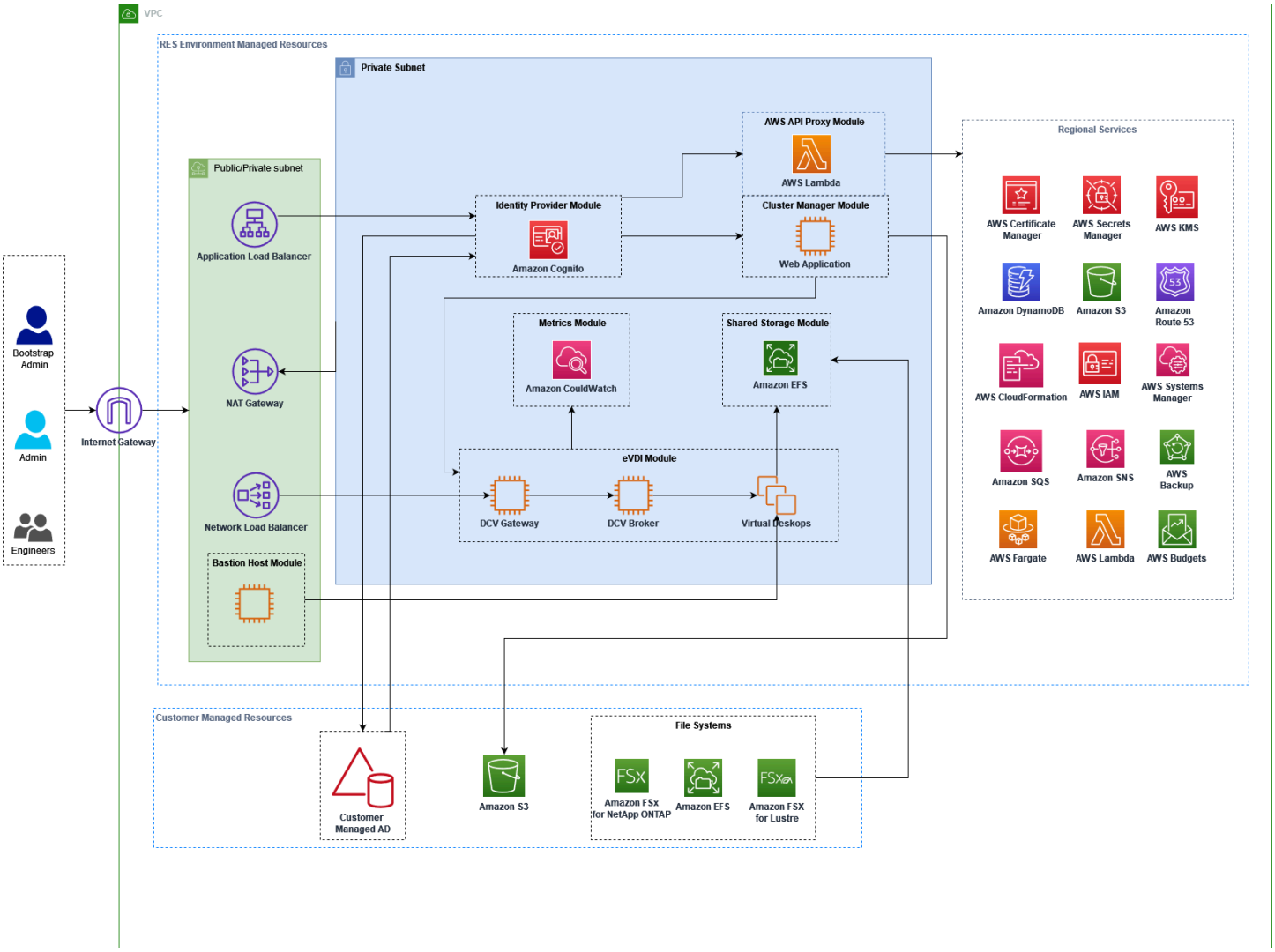


Figure 1 : Studio de recherche et d'ingénierie sur AWS l'architecture

> **Note**
>
> AWS CloudFormation les ressources sont créées à partir de AWS Cloud Development Kit (AWS CDK) constructions.

Le flux de processus de haut niveau pour les composants du produit déployés avec le AWS CloudFormation modèle est le suivant :

1. RES installe des composants pour le portail Web ainsi que :
   a. Composant de bureau virtuel d'ingénierie (eVDI) pour les charges de travail interactives
   b. Composant Metrics

      Amazon CloudWatch reçoit les métriques des composants eVDI.
   c. Composant Bastion Host

      Les administrateurs peuvent utiliser SSH pour se connecter au composant hôte Bastion afin de gérer l'infrastructure sous-jacente.
2. RES installe les composants dans des sous-réseaux privés situés derrière une passerelle NAT. Les administrateurs accèdent aux sous-réseaux privés via l'Application Load Balancer (ALB) ou le composant Bastion Host.
3. Amazon DynamoDB stocke la configuration de l'environnement.
4. AWS Certificate Manager (ACM) génère et stocke un certificat public pour l'Application Load Balancer (ALB).

   > **Note**
   >
   > Nous vous recommandons AWS Certificate Manager de l'utiliser pour générer un certificat fiable pour votre domaine.
5. Amazon Elastic File System (EFS) héberge le système de `/home` fichiers par défaut monté sur tous les hôtes d'infrastructure et sessions eVDI Linux applicables.
6. RES utilise Amazon Cognito pour créer un utilisateur bootstrap initial appelé « clusteradmin » et envoie des informations d'identification temporaires à l'adresse e-mail fournie lors de l'installation. Le « clusteradmin » doit changer le mot de passe la première fois qu'il se connecte.

7. Amazon Cognito s'intègre à l'Active Directory et aux identités des utilisateurs de votre organisation pour la gestion des autorisations.
8. Les zones de sécurité permettent aux administrateurs de restreindre l'accès à des composants spécifiques du produit en fonction des autorisations.

AWS services inclus dans ce produit

AWS service	Type	Description
Amazon Elastic Compute Cloud	Principal	Fournit les services informatiques sous-jacents pour créer des bureaux virtuels avec le système d'exploitation et la pile logicielle choisis.
Elastic Load Balancing	Principal	Les hôtes Bastion, cluster-manager et VDI sont créés dans des groupes Auto Scaling situés derrière l'équilibreur de charge. ELB équilibre le trafic du portail Web entre les hôtes RES.
Amazon Virtual Private Cloud	Principal	Tous les principaux composants du produit sont créés au sein de votre VPC.
Amazon Cognito	Principal	Gère les identités et l'authentification des utilisateurs. Les utilisateurs d'Active Directory sont mappés aux utilisateurs et aux groupes Amazon Cognito afin d'authentifier les niveaux d'accès.
Amazon Elastic File System	Principal	Fournit le système de `/home` fichiers pour le navigateur

AWS service	Type	Description
		de fichiers et les hôtes VDI, ainsi que pour les systèmes de fichiers externes partagés.
Amazon DynamoDB	Principal	Stocke les données de configuration telles que les utilisateurs, les groupes, les projets, les systèmes de fichiers et les paramètres des composants.
AWS Systems Manager	Principal	Stocke les documents permettant d'exécuter des commandes pour la gestion des sessions VDI.
AWS Lambda	Principal	Prend en charge les fonctionn alités du produit telles que la mise à jour des paramètres dans la table DynamoDB, le démarrage des flux de travail de synchronisation Active Directory et la mise à jour de la liste des préfixes.
Amazon CloudWatch	Soutenant	Fournit des statistiques et des journaux d'activité pour tous les EC2 hôtes Amazon et les fonctions Lambda.
Amazon Simple Storage Service	Soutenant	Stocke les fichiers binaires des applications pour le démarrage et la configuration de l'hôte.

AWS service	Type	Description
AWS Key Management Service	Soutenant	Utilisé pour le chiffrement au repos avec les files d'attente Amazon SQS, les tables DynamoDB et les rubriques Amazon SNS.
AWS Secrets Manager	Soutenant	Stocke les informations d'identification du compte de service dans Active Directory et les certificats auto-signés pour VDIs.
AWS CloudFormation	Soutenant	Fournit un mécanisme de déploiement pour le produit.
Gestion des identités et des accès AWS	Soutenant	Limite le niveau d'accès pour les hôtes.
Amazon Route 53	Soutenant	Crée une zone hébergée privée pour résoudre l'équilib reur de charge interne et le nom de domaine hôte du bastion.
Amazon Simple Queue Service	Soutenant	Crée des files d'attente de tâches pour prendre en charge les exécutions asynchrones.
Amazon Simple Notification Service	Soutenant	Prend en charge le modèle publication-abonné entre les composants VDI tels que le contrôleur et les hôtes.
AWS Fargate	Soutenant	Installe, met à jour et supprime des environnements à l'aide de tâches Fargate.

AWS service	Type	Description
Passerelle FSx de fichiers Amazon	Facultatif	Fournit un système de fichiers partagé externe.
Amazon FSx pour NetApp ONTAP	Facultatif	Fournit un système de fichiers partagé externe.
AWS Certificate Manager	Facultatif	Génère un certificat fiable pour votre domaine personnalisé.
AWS Backup	Facultatif	Offre des fonctionnalités de sauvegarde pour les EC2 hôtes Amazon, les systèmes de fichiers et DynamoDB.

Création d'un environnement de démonstration

Suivez les étapes décrites dans cette section pour essayer Research and Engineering Studio sur AWS. Cette démonstration déploie un environnement hors production avec un ensemble minimal de paramètres à l'aide du modèle de pile d'environnement de AWS démonstration du studio de recherche et d'ingénierie. Il utilise un serveur Keycloak pour le SSO.

Notez qu'après avoir déployé la pile, vous devez suivre les instructions Étapes après le déploiement ci-dessous pour configurer les utilisateurs dans l'environnement avant de vous connecter.

Créez une pile de démonstration en un clic

Cette CloudFormation pile crée tous les composants requis par le studio de recherche et d'ingénierie.

Temps de déploiement : ~90 minutes

Conditions préalables

Rubriques

- Créez un Compte AWS avec un utilisateur administratif
- Création d'une paire de clés SSH Amazon EC2
- Augmenter les quotas de service

Créez un Compte AWS avec un utilisateur administratif

Vous devez avoir Compte AWS un utilisateur administratif :

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un

utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Création d'une paire de clés SSH Amazon EC2

Si vous ne possédez pas de paire de clés SSH Amazon EC2, vous devez en créer une. Pour plus d'informations, consultez la section Création d'une paire de clés à l'aide d'Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Augmenter les quotas de service

Nous recommandons d'augmenter les quotas de service pour :

- Amazon VPC
  - Augmenter le quota d'adresses IP Elastic par passerelle NAT de cinq à huit
  - Augmenter le nombre de passerelles NAT par zone de disponibilité de cinq à dix
- Amazon EC2
  - Augmenter l'EC2-VPC Elastic IPs de cinq à dix

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à une région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés. Pour de plus amples informations, veuillez consulter the section called "Quotas pour AWS les services inclus dans ce produit".

Création de ressources et de paramètres d'entrée

1. Connectez-vous à la CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Vérifiez que vous êtes connecté à votre compte administrateur.

2. Lancez le modèle dans la console.
3. Sous Paramètres, passez en revue les paramètres de ce modèle de produit et modifiez-les si nécessaire.

Paramètre	Par défaut	Description
EnvironmentName	*<res-demo>*	Nom unique attribué à votre environnement RES commençant par res-, ne dépassant pas 11 caractères et sans majuscules.
AdministratorEmail		Adresse e-mail de l'utilisa teur qui termine la configura tion du produit. Cet utilisateur joue également le rôle d'un utilisateur hors pair en cas d'échec de l'intégration de l'authentification unique dans Active Directory.
KeyPair		La paire de clés utilisée pour se connecter aux hôtes de l'infrastructure.
Cliente IPCidr	<0.0.0.0/0>	Filtre d'adresse IP qui limite la connexion au système. Vous pouvez le mettre à jour ClientIpCidr après le déploiement.
InboundPrefixList		(Facultatif) Fournissez une liste de préfixes gérés pour IPs autoriser l'accès direct à l'interface utilisateur Web et au protocole SSH sur l'hôte Bastion.

4. Sélectionnez Créer la pile.

Étapes après le déploiement

1. Vous pouvez désormais vous connecter à l'environnement de démonstration à l'aide de l'utilisateur clusteradmin et du mot de passe temporaire envoyé à l'adresse e-mail d'administrateur que vous avez saisie lors de la configuration. Vous êtes invité à créer un nouveau mot de passe lors de votre première connexion.
2. Si vous souhaitez utiliser la fonctionnalité « Se connecter avec l'authentification unique de l'organisation », vous devez d'abord réinitialiser les mots de passe de chaque utilisateur sous lequel vous souhaitez vous connecter. Vous pouvez réinitialiser les mots de passe des utilisateurs depuis le AWS Directory Service. La pile de démonstration crée quatre utilisateurs avec des noms d'utilisateur que vous pouvez utiliser : admin1, user1, admin2 et user2.

    a. Accédez à la console Directory Service.
    b. Sélectionnez l'ID de répertoire pour votre environnement. Vous pouvez obtenir l'identifiant du répertoire à partir de la sortie de la `<StackName>*DirectoryService*` pile.
    c. Dans le menu déroulant Action en haut à droite, sélectionnez Réinitialiser le mot de passe utilisateur.
    d. Pour tous les utilisateurs que vous souhaitez utiliser, entrez le nom d'utilisateur, saisissez le nouveau mot de passe souhaité, puis choisissez Réinitialiser le mot de passe.
3. Une fois que vous avez réinitialisé les mots de passe des utilisateurs, rendez-vous sur la page de connexion unique pour accéder à l'environnement.

Votre déploiement est maintenant prêt. Utilisez celle EnvironmentUrl que vous avez reçue dans votre e-mail pour accéder à l'interface utilisateur, ou vous pouvez également obtenir la même URL à partir de la sortie de la pile déployée. Vous pouvez désormais vous connecter à l'environnement du studio de recherche et d'ingénierie avec l'utilisateur et le mot de passe pour lesquels vous avez réinitialisé le mot de passe dans Active Directory.

Planifiez votre déploiement

Cette section contient des informations sur les coûts, la sécurité, les régions prises en charge et les quotas qui peuvent vous aider à planifier le déploiement de Research and Engineering Studio on AWS.

Cost

Research and Engineering Studio on AWS est disponible sans frais supplémentaires, et vous ne payez que pour les AWS ressources nécessaires à l'exécution de vos applications. Pour de plus amples informations, veuillez consulter AWS services inclus dans ce produit.

> **Note**
>
> Vous êtes responsable du coût des AWS services utilisés lors de l'utilisation de ce produit. Nous vous recommandons de créer un budget AWS Cost Explorerpour aider à gérer les coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque AWS service utilisé dans ce produit.

Sécurité

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée de décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Research and Engineering Studio on AWS, voir AWS Services concernés par programme de conformitéAWS .

- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Pour comprendre comment appliquer le modèle de responsabilité partagée aux AWS services utilisés par Research and Engineering Studio, voirConsidérations relatives à la sécurité des services inclus dans ce produit. Pour plus d'informations sur AWS la sécurité, consultez AWS Cloud la section Sécurité.

Rôles IAM

Gestion des identités et des accès AWS Les rôles (IAM) permettent aux clients d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs du. AWS Cloud Ce produit crée des rôles IAM qui accordent aux AWS Lambda fonctions du produit et aux instances Amazon EC2 l'accès pour créer des ressources régionales.

RES prend en charge les politiques basées sur l'identité au sein d'IAM. Lors du déploiement, RES crée des politiques pour définir les autorisations et les accès de l'administrateur. L'administrateur qui implémente le produit crée et gère les utilisateurs finaux et les chefs de projet au sein de l'Active Directory du client existant intégré à RES. Pour plus d'informations, consultez la section Création de politiques IAM dans le guide de l'utilisateur AWS d'Identity and Access Management.

L'administrateur de votre organisation peut gérer l'accès des utilisateurs à l'aide d'un Active Directory. Lorsque les utilisateurs finaux accèdent à l'interface utilisateur RES, RES s'authentifie auprès d'Amazon Cognito.

Groupes de sécurité

Les groupes de sécurité créés dans ce produit sont conçus pour contrôler et isoler le trafic réseau entre les fonctions Lambda, les instances EC2, les instances CSR des systèmes de fichiers et les points de terminaison VPN distants. Nous vous recommandons de passer en revue les groupes de sécurité et de restreindre davantage l'accès, le cas échéant, une fois le produit déployé.

Chiffrement des données

Par défaut, Research and Engineering Studio on AWS (RES) chiffre les données clients au repos et en transit à l'aide d'une clé détenue par RES. Lorsque vous déployez RES, vous pouvez spécifier un AWS KMS key. RES utilise vos informations d'identification pour accorder un accès clé. Si vous

fournissez un produit détenu et géré par un client AWS KMS key, les données du client au repos seront cryptées à l'aide de cette clé.

RES chiffre les données des clients en transit à l'aide du protocole SSL/TLS. Nous avons besoin du protocole TLS 1.2, mais nous recommandons le protocole TLS 1.3.

Considérations relatives à la sécurité des services inclus dans ce produit

Pour des informations plus détaillées concernant les considérations de sécurité relatives aux services utilisés par Research and Engineering Studio, suivez les liens de ce tableau :

AWS informations sur la sécurité du service	Type de service	Comment le service est utilisé dans RES
Amazon Elastic Compute Cloud	Principal	Fournit les services informatiques sous-jacents pour créer des bureaux virtuels avec le système d'exploitation et la pile logicielle choisis.
Elastic Load Balancing	Principal	Les hôtes Bastion, cluster-manager et VDI sont créés dans des groupes Auto Scaling situés derrière l'équilibreur de charge. ELB équilibre le trafic du portail Web entre les hôtes RES.
Amazon Virtual Private Cloud	Principal	Tous les principaux composants du produit sont créés au sein de votre VPC.
Amazon Cognito	Principal	Gère les identités et l'authentification des utilisateurs. Les utilisateurs d'Active Directory sont mappés aux utilisateurs et aux groupes Amazon

AWS informations sur la sécurité du service	Type de service	Comment le service est utilisé dans RES
		Cognito afin d'authentifier les niveaux d'accès.
Amazon Elastic File System	Principal	Fournit le système de `/home` fichiers pour le navigateur de fichiers et les hôtes VDI, ainsi que pour les systèmes de fichiers externes partagés.
Amazon DynamoDB	Principal	Stocke les données de configuration telles que les utilisateurs, les groupes, les projets, les systèmes de fichiers et les paramètres des composants.
AWS Systems Manager	Principal	Stocke les documents permettant d'exécuter des commandes pour la gestion des sessions VDI.
AWS Lambda	Principal	Prend en charge les fonctionn alités du produit telles que la mise à jour des paramètres dans la table DynamoDB, le démarrage des flux de travail de synchronisation Active Directory et la mise à jour de la liste des préfixes.
Amazon CloudWatch	Soutenir	Fournit des métriques et des journaux d'activité pour tous les hôtes Amazon EC2 et les fonctions Lambda.

AWS informations sur la sécurité du service	Type de service	Comment le service est utilisé dans RES
Amazon Simple Storage Service	Soutenir	Stocke les fichiers binaires des applications pour le démarrage et la configuration de l'hôte.
AWS Key Management Service	Soutenir	Utilisé pour le chiffrement au repos avec les files d'attente Amazon SQS, les tables DynamoDB et les rubriques Amazon SNS.
AWS Secrets Manager	Soutenir	Stocke les informations d'identification du compte de service dans Active Directory et les certificats auto-signés pour VDIs.
AWS CloudFormation	Soutenir	Fournit un mécanisme de déploiement pour le produit.
Gestion des identités et des accès AWS	Soutenir	Limite le niveau d'accès pour les hôtes.
Amazon Route 53	Soutenir	Crée une zone hébergée privée pour résoudre l'équilib reur de charge interne et le nom de domaine hôte du bastion.
Amazon Simple Queue Service	Soutenir	Crée des files d'attente de tâches pour prendre en charge les exécutions asynchrones.

AWS informations sur la sécurité du service	Type de service	Comment le service est utilisé dans RES
Amazon Simple Notification Service	Soutenir	Prend en charge le modèle publication-abonné entre les composants VDI tels que le contrôleur et les hôtes.
AWS Fargate	Soutenir	Installe, met à jour et supprime des environnements à l'aide de tâches Fargate.
Passerelle FSx de fichiers Amazon	Facultatif	Fournit un système de fichiers partagé externe.
Amazon FSx pour NetApp ONTAP	Facultatif	Fournit un système de fichiers partagé externe.
AWS Certificate Manager	Facultatif	Génère un certificat fiable pour votre domaine personnalisé.
AWS Backup	Facultatif	Offre des fonctionnalités de sauvegarde pour les hôtes Amazon EC2, les systèmes de fichiers et DynamoDB.

Quotas

Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre Compte AWS.

Quotas pour AWS les services inclus dans ce produit

Assurez-vous de disposer d'un quota suffisant pour chacun des services mis en œuvre dans ce produit. Pour plus d'informations, consultez Quotas de service AWS.

Pour ce produit, nous recommandons d'augmenter les quotas pour les services suivants :

- Amazon Virtual Private Cloud

- Amazon EC2

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

AWS CloudFormation quotas

Vous avez Compte AWS AWS CloudFormation des quotas dont vous devez tenir compte lorsque vous lancez le stack de ce produit. En comprenant ces quotas, vous pouvez éviter les erreurs de limitation qui vous empêcheraient de déployer correctement ce produit. Pour plus d'informations, consultez la section sur les AWS CloudFormation quotas dans le guide de l'AWS CloudFormation utilisateur.

Planification de la résilience

Le produit déploie une infrastructure par défaut avec le nombre et la taille minimum d'instances Amazon EC2 pour faire fonctionner le système. Pour améliorer la résilience dans les environnements de production à grande échelle, nous recommandons d'augmenter les paramètres de capacité minimale par défaut au sein des groupes Auto Scaling (ASG) de l'infrastructure. L'augmentation de la valeur d'une instance à deux instances permet de tirer parti de plusieurs zones de disponibilité (AZ) et de réduire le délai de restauration des fonctionnalités du système en cas de perte de données inattendue.

Les paramètres ASG peuvent être personnalisés dans la console Amazon EC2 à l'adresse. https://console.aws.amazon.com/ec2/ Le produit en crée quatre ASGs par défaut, chaque nom se terminant par`-asg`. Vous pouvez modifier les valeurs minimales et souhaitées en fonction de votre environnement de production. Sélectionnez le groupe que vous souhaitez modifier, puis choisissez Actions et sélectionnez Modifier. Pour plus d'informations ASGs, consultez la section Dimensionner la taille de votre groupe Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Soutenu Régions AWS

Ce produit utilise des services qui ne sont pas tous disponibles actuellement Régions AWS. Vous devez lancer ce produit dans un Région AWS endroit où tous les services sont disponibles. Pour connaître la disponibilité la plus récente des AWS services par région, consultez la Région AWS liste complète des services.

Le studio de recherche et d'ingénierie sur AWS est soutenu dans les domaines suivants Régions AWS :

Nom de la région	Région	Versions précédentes	Dernière version (2025.03)
USA Est (Virginie du Nord)	us-east-1	oui	oui
USA Est (Ohio)	us-east-2	oui	oui
USA Ouest (Californie du Nord)	us-west-1	oui	oui
USA Ouest (Oregon)	us-west-2	oui	oui
Asie-Pacifique (Tokyo)	ap-northeast-1	oui	oui
Asie-Pacifique (Séoul)	ap-northeast-2	oui	oui
Asie-Pacifique (Mumbai)	ap-south-1	oui	oui
Asie-Pacifique (Singapour)	ap-southeast-1	oui	oui
Asie-Pacifique (Sydney)	ap-southeast-2	oui	oui
Canada (Centre)	ca-central-1	oui	oui
Europe (Francfort)	eu-central-1	oui	oui
Europe (Milan)	eu-south-1	oui	oui
Europe (Irlande)	eu-west-1	oui	oui
Europe (Londres)	eu-west-2	oui	oui
Europe (Paris)	eu-west-3	oui	oui

Nom de la région	Région	Versions précédentes	Dernière version (2025.03)
Europe (Stockholm)	eu-north-1	non	oui
Israël (Tel Aviv)	il-central-1	oui	oui
AWS GovCloud (US-Ouest)	us-gov-west-1	oui	oui

Déployez le produit

> **Note**
>
> Ce produit utilise des AWS CloudFormation modèles et des piles pour automatiser son déploiement. Les CloudFormation modèles décrivent les AWS ressources incluses dans ce produit et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans les modèles.

Avant de lancer le produit, examinez le coût, l'architecture, la sécurité du réseau et les autres considérations abordées précédemment dans ce guide.

Rubriques

Conditions préalables

Rubriques

Créez un Compte AWS avec un utilisateur administratif

Vous devez disposer d' Compte AWS un compte utilisateur administratif :

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Création d'une paire de clés SSH Amazon EC2

Si vous ne possédez pas de paire de clés SSH Amazon EC2, vous devez en créer une. Pour plus d'informations, consultez la section Création d'une paire de clés à l'aide d'Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Augmenter les quotas de service

Nous recommandons d'augmenter les quotas de service pour :

- Amazon VPC
  - Augmentez le quota d'adresses IP Elastic par passerelle NAT de cinq à huit.
  - Augmentez le nombre de passerelles NAT par zone de disponibilité de cinq à dix.
- Amazon EC2
  - Augmenter l'EC2-VPC Elastic IPs de cinq à dix

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à une région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés. Pour de plus amples informations, veuillez consulter Quotas pour AWS les services inclus dans ce produit.

Créez un domaine personnalisé (facultatif)

Nous vous recommandons d'utiliser un domaine personnalisé pour le produit afin de disposer d'une URL conviviale. Vous pouvez fournir un domaine personnalisé et éventuellement fournir un certificat pour celui-ci.

Il existe un processus dans la pile des ressources externes pour créer un certificat pour un domaine personnalisé que vous fournissez. Vous pouvez ignorer les étapes ci-dessous si vous possédez un domaine et souhaitez utiliser les fonctionnalités de génération de certificats de la pile de ressources externes.

Vous pouvez également suivre ces étapes pour enregistrer un domaine à l'aide d'Amazon Route 53 et importer un certificat pour le domaine à l'aide d'Amazon Route 53 AWS Certificate Manager.

1. Suivez les instructions pour enregistrer un domaine auprès de Route53. Vous devriez recevoir un e-mail de confirmation.
2. Récupérez la zone hébergée pour votre domaine. Ceci est créé automatiquement par Route53.
    a. Ouvrez la console Route53.
    b. Choisissez Zones hébergées dans le menu de navigation de gauche.
    c. Ouvrez la zone hébergée créée pour votre nom de domaine et copiez l'ID de zone hébergée.
3. Ouvrez AWS Certificate Manager et suivez ces étapes pour demander un certificat de domaine. Assurez-vous que vous vous trouvez dans la région où vous prévoyez de déployer la solution.
4. Choisissez Lister les certificats dans le menu de navigation, puis recherchez votre demande de certificat. La demande devrait être en attente.
5. Choisissez votre numéro de certificat pour ouvrir la demande.
6. Dans la section Domaines, choisissez Créer des enregistrements dans Route53. Le traitement de la demande prendra environ dix minutes.
7. Une fois le certificat émis, copiez l'ARN depuis la section État du certificat.

Créer un domaine (GovCloud uniquement)

Si vous effectuez un déploiement dans la région AWS GovCloud (ouest des États-Unis) et que vous utilisez un domaine personnalisé pour Research and Engineering Studio, vous devrez suivre ces étapes préalables.

1. Déployez la CloudFormation pile de certificats dans le AWS compte de partition commerciale où le domaine public hébergé a été créé.
2. Dans les CloudFormation sorties du certificat, recherchez et notez le `CertificateARN` et`PrivateKeySecretARN`.
3. Dans le compte de GovCloud partition, créez un secret avec la valeur de la `CertificateARN` sortie. Notez le nouvel ARN secret et ajoutez deux balises au secret pour `vdc-gateway` pouvoir accéder à la valeur du secret :
   a. rouge : ModuleName = virtual-desktop-controller
   b. res : EnvironmentName = [nom de l'environnement] (Cela pourrait être res-demo.)
4. Dans le compte de GovCloud partition, créez un secret avec la valeur de la `PrivateKeySecretArn` sortie. Notez le nouvel ARN secret et ajoutez deux balises au secret pour `vdc-gateway` pouvoir accéder à la valeur du secret :
   a. rouge : ModuleName = virtual-desktop-controller
   b. res : EnvironmentName = [nom de l'environnement] (Cela pourrait être res-demo.)

Fournir des ressources externes

Research and Engineering Studio s' AWS attend à ce que les ressources externes suivantes existent lors de son déploiement.

- Mise en réseau (VPC, sous-réseaux publics et sous-réseaux privés)

  C'est ici que vous exécuterez les instances EC2 utilisées pour héberger l'environnement RES, Active Directory (AD) et le stockage partagé.
- Stockage (Amazon EFS)

  Les volumes de stockage contiennent les fichiers et les données nécessaires à l'infrastructure de bureau virtuel (VDI).
- Service d'annuaire (AWS Directory Service for Microsoft Active Directory)

  Le service d'annuaire authentifie les utilisateurs dans l'environnement RES.
- Secret contenant le nom d'utilisateur et le mot de passe du compte de service Active Directory formatés sous forme de paire clé-valeur (nom d'utilisateur, mot de passe)

Research and Engineering Studio accède aux secrets que vous fournissez, y compris le mot de passe du compte de service, en utilisant AWS Secrets Manager.

> **Warning**
>
> Vous devez fournir une adresse e-mail valide pour tous les utilisateurs Active Directory (AD) que vous souhaitez synchroniser.

> **Tip**
>
> Si vous déployez un environnement de démonstration et que ces ressources externes ne sont pas disponibles, vous pouvez utiliser des recettes de calcul AWS haute performance pour générer les ressources externes. Consultez la section suivante pour déployer des ressources dans votre compte. Création de ressources externes
> Pour les déploiements de démonstration dans la région AWS GovCloud (ouest des États-Unis), vous devrez suivre les étapes requises dans. Créer un domaine (GovCloud uniquement)

Configurer LDAPS dans votre environnement (facultatif)

Si vous envisagez d'utiliser la communication LDAPS dans votre environnement, vous devez suivre ces étapes pour créer et joindre des certificats au contrôleur de domaine AWS Managed Microsoft AD (AD) afin d'assurer la communication entre AD et RES.

1. Suivez les étapes indiquées dans Comment activer le protocole LDAPS côté serveur pour votre. AWS Managed Microsoft AD Vous pouvez ignorer cette étape si vous avez déjà activé LDAPS.
2. Après avoir confirmé que LDAPS est configuré sur l'AD, exportez le certificat AD :
    a. Accédez à votre serveur Active Directory.
    b. Ouvrez PowerShell en tant qu'administrateur.
    c. Exécutez `certmgr.msc` pour ouvrir la liste des certificats.
    d. Ouvrez la liste des certificats en ouvrant d'abord les Autorités de certification racine fiables, puis les certificats.

e. Sélectionnez et maintenez (ou cliquez avec le bouton droit) le certificat portant le même nom que votre serveur AD et choisissez Toutes les tâches, puis Exporter.

f. Sélectionnez X.509 codé en Base-64 (.CER) et choisissez Next.

g. Sélectionnez un répertoire, puis cliquez sur Suivant.

3. Créez un secret dans AWS Secrets Manager :

   Lorsque vous créez votre secret dans Secrets Manager, choisissez Autre type de secrets sous Type de secret et collez votre certificat codé PEM dans le champ Texte en clair.

4. Notez l'ARN créé et saisissez-le en tant que `DomainTLSCertificateSecretARN` paramètre dansÉtape 1 : Lancez le produit.

Configuration d'un compte de service pour Microsoft Active Directory

Si vous choisissez Microsoft Active Directory (AD) comme source d'identité pour RES, vous disposez d'un compte de service dans votre AD qui permet un accès par programmation. Vous devez transmettre un secret contenant les informations d'identification du compte de service dans le cadre de votre installation RES. Le compte de service est responsable des fonctions suivantes :

- Synchroniser les utilisateurs depuis l'AD : RES doit synchroniser les utilisateurs depuis l'AD pour leur permettre de se connecter au portail Web. Le processus de synchronisation utilise le compte de service pour interroger l'AD à l'aide de LDAP afin de déterminer quels utilisateurs et groupes sont disponibles.
- Joindre le domaine AD : il s'agit d'une opération facultative pour les bureaux virtuels Linux et les hôtes d'infrastructure où l'instance rejoint le domaine AD. Dans RES, cela est contrôlé par le `DisableADJoin` paramètre. Ce paramètre est défini sur False par défaut, ce qui signifie que les bureaux virtuels Linux tenteront de rejoindre le domaine AD dans la configuration par défaut.
- Se connecter à AD : les bureaux virtuels et les hôtes d'infrastructure Linux se connecteront au domaine AD s'ils ne le rejoignent pas (`DisableADJoin`= True). Pour que cette fonctionnalité fonctionne, le compte de service doit également disposer d'un accès en lecture pour les utilisateurs et les groupes du `Users0U` and`Groups0U`.

Le compte de service nécessite les autorisations suivantes :

- Pour synchroniser les utilisateurs et se connecter à AD → Accès en lecture pour les utilisateurs et les groupes dans le `Users0U` et`Groups0U`.

- Pour rejoindre le domaine AD → créer `Computer` des objets dans le`Computers0U`.

Le script situé à l' https://github.com/aws-samples/aws-hpc-recipes/blob/main/recipes/res/res_demo_env/assets/service_account.ps1 fournit un exemple de la manière d'accorder les autorisations appropriées à un compte de service. Vous pouvez le modifier en fonction de votre propre AD.

Configuration d'un VPC privé (facultatif)

Le déploiement d'un studio de recherche et d'ingénierie dans un VPC isolé offre une sécurité renforcée pour répondre aux exigences de conformité et de gouvernance de votre entreprise. Cependant, le déploiement standard de RES repose sur l'accès à Internet pour installer les dépendances. Pour installer RES dans un VPC privé, vous devez satisfaire aux conditions préalables suivantes :

Rubriques

- Préparer les images Amazon Machine (AMIs)
- Configuration des points de terminaison VPC
- Connectez-vous aux services sans points de terminaison VPC
- Définir les paramètres de déploiement d'un VPC privé

Préparer les images Amazon Machine (AMIs)

1. Téléchargez les dépendances. Pour être déployée dans un VPC isolé, l'infrastructure RES nécessite la disponibilité de dépendances sans accès public à Internet.
2. Créez un rôle IAM avec un accès en lecture seule à Amazon S3 et une identité fiable en tant qu'Amazon EC2.

    a. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

    b. Dans Rôles, sélectionnez Créer un rôle.

    c. Sur la page Sélectionner une entité de confiance :

    - Sous Type d'entité de confiance, sélectionnez Service AWS.
    - Pour Cas d'utilisation sous Service ou cas d'utilisation, choisissez EC2, puis Next.

    d. Dans Ajouter des autorisations, sélectionnez les politiques d'autorisation suivantes, puis cliquez sur Suivant :

- Amazon S3 ReadOnlyAccess
- Amazon SSMManaged InstanceCore
- EC2InstanceProfileForImageBuilder

e. Ajoutez un nom et une description du rôle, puis choisissez Créer un rôle.

3. Créez le composant du générateur d'images EC2 :

a. Ouvrez la console https://console.aws.amazon.com//imagebuilder EC2 Image Builder à l'adresse.

b. Sous Ressources enregistrées, sélectionnez Composants, puis Créer un composant.

c. Sur la page Créer un composant, entrez les informations suivantes :

- Pour Type de composant, choisissez Construire.
- Pour les détails du composant, choisissez :

Paramètre	Entrée utilisateur
Système d'exploitation d'images (OS)	Linux
Versions de systèmes d'exploitation compatibles	Amazon Linux 2, RHEL8 RHEL9, ou Windows 10 et 11
Nom du composant	Entrez un nom tel que : *<research-and-engineering-studio-infrastructure>*
Version du composant	Nous vous recommandons de commencer par la version 1.0.0.
Description	Entrée utilisateur facultative.

d. Sur la page Créer un composant, choisissez Définir le contenu du document.

i. Avant de saisir le contenu du document de définition, vous aurez besoin d'un URI pour le fichier tar.gz. Chargez le fichier tar.gz fourni par RES dans un compartiment Amazon S3 et copiez l'URI du fichier depuis les propriétés du compartiment.

ii. Saisissez :

> **Note**
>
> `AddEnvironmentVariables`est facultatif, et vous pouvez le supprimer si vous n'avez pas besoin de variables d'environnement personnalisées dans vos hôtes d'infrastructure.
>
> Si vous configurez `http_proxy` des variables d'`https_proxy`environnement, les `no_proxy` paramètres sont nécessaires pour empêcher l'instance d'utiliser un proxy pour interroger localhost, les adresses IP des métadonnées de l'instance et les services prenant en charge les points de terminaison VPC.

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may
 not use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
```

```
          action: S3Download
          onFailure: Abort
          maxAttempts: 3
          inputs:
             - source: '<s3 tar.gz file uri>'
               destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
               expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - 'cd /root/bootstrap/res_dependencies'
                 - 'tar -xf res_dependencies.tar.gz'
                 - 'cd all_dependencies'
                 - '/bin/bash install.sh'
       - name: AddEnvironmentVariables
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - |
                   echo -e "
                   http_proxy=http://<ip>:<port>
                   https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
```

```
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com,ecs.
{{ AWSRegion }}.amazonaws.com,.execute-api.{{ AWSRegion }}.amazonaws.com
>                   " > /etc/environment
```

e. Choisissez Créer un composant.

4. Créez une recette d'image Image Builder.

   a. Sur la page Créer une recette, entrez les informations suivantes :

Section	Paramètre	Entrée utilisateur
Détails de la recette	Nom	Entrez un nom approprié , tel que res-recipe-linux-x 86.
	Version	Entrez une version, commençant généralement par 1.0.0.
	Description	Ajoutez une description facultative.
Image de base	Sélectionnez une image	Sélectionnez les images gérées.
	SE	Amazon Linux ou Red Hat Enterprise Linux (RHEL)
	Origine de l'image	Démarrage rapide (géré par Amazon)
	Nom de l'image	Amazon Linux 2 x86, Red Hat Enterprise Linux 8

Section	Paramètre	Entrée utilisateur
		x86 ou Red Hat Enterprise Linux 9 x86
	Options de gestion automatique des versions	Utilisez la dernière version du système d'exploitation disponible.
Configuration de l'instance	–	Conservez tout dans les paramètres par défaut et assurez-vous que l'option Supprimer l'agent SSM après l'exécution du pipeline n'est pas sélection née.
Répertoire de travail	Chemin du répertoire de travail	/root/bootstrap/res_dépendances
Composants	Construire des composants	Recherchez et sélectionnez les éléments suivants : • Géré par Amazon : -2-linux aws-cli-version • Géré par Amazon : amazon-cloudwatch-agent-linux • Détenu par vous : composant Amazon EC2 créé précédemment. Entrez votre Compte AWS identifiant et votre actuel Région AWS dans les champs.

Section	Paramètre	Entrée utilisateur
	Composants de test	Recherchez et sélectionnez : • Géré par Amazon : simple-boot-test-linux

b. Choisissez Créer une recette.

5. Créez la configuration de l'infrastructure Image Builder.

a. Sous Ressources enregistrées, sélectionnez Configurations d'infrastructure.

b. Choisissez Créer une configuration d'infrastructure.

c. Sur la page Créer une configuration d'infrastructure, entrez ce qui suit :

Section	Paramètre	Entrée utilisateur
Général	Nom	Entrez un nom approprié, tel que res-infra-linux-x 86.
	Description	Ajoutez une description facultative.
	Rôle IAM	Sélectionnez le rôle IAM créé précédemment.
AWS infrastructure	Type d'instance	Choisissez t3.medium.
	VPC, sous-réseau et groupes de sécurité	Sélectionnez une option qui autorise l'accès à Internet et au compartiment Amazon S3. Si vous devez créer un groupe de sécurité, vous pouvez en créer un depuis la console Amazon EC2 avec les entrées suivantes :

Section	Paramètre	Entrée utilisateur

		• VPC : sélectionnez le même VPC que celui utilisé pour la configura tion de l'infrastructure. Ce VPC doit avoir accès à Internet.
		• Règle entrante :
		  • Type : SSH
		  • Source : Personnalisé
		  • Bloc CIDR : 0.0.0.0/0

d. Choisissez Créer une configuration d'infrastructure.

6. Créez un nouveau pipeline EC2 Image Builder :

   a. Accédez à Pipelines d'images, puis choisissez Créer un pipeline d'images.

   b. Sur la page Spécifier les détails du pipeline, entrez ce qui suit et choisissez Next :

      - Nom du pipeline et description facultative
      - Pour le calendrier de création, définissez un calendrier ou choisissez Manuel si vous souhaitez démarrer le processus de cuisson des AMI manuellement.

   c. Sur la page Choisir une recette, choisissez Utiliser une recette existante et entrez le nom de la recette créée précédemment. Choisissez Suivant.

   d. Sur la page Définir le traitement d'image, sélectionnez les flux de travail par défaut, puis cliquez sur Suivant.

   e. Sur la page Définir la configuration de l'infrastructure, choisissez Utiliser la configuration d'infrastructure existante et entrez le nom de la configuration d'infrastructure créée précédemment. Choisissez Suivant.

   f. Sur la page Définir les paramètres de distribution, tenez compte des points suivants pour vos sélections :

      - L'image de sortie doit résider dans la même région que l'environnement RES déployé, afin que RES puisse lancer correctement les instances hôtes de l'infrastructure à partir

de celui-ci. À l'aide des valeurs par défaut du service, l'image de sortie sera créée dans la région où le service EC2 Image Builder est utilisé.

- Si vous souhaitez déployer RES dans plusieurs régions, vous pouvez choisir Créer de nouveaux paramètres de distribution et y ajouter d'autres régions.

g. Passez en revue vos sélections et choisissez Créer un pipeline.

7. Exécutez le pipeline EC2 Image Builder :

   a. Dans Pipelines d'images, recherchez et sélectionnez le pipeline que vous avez créé.

   b. Choisissez Actions, puis sélectionnez Exécuter le pipeline.

   Le pipeline peut prendre entre 45 minutes et une heure pour créer une image AMI.

8. Notez l'ID d'AMI de l'AMI générée et utilisez-le comme entrée pour le paramètre InfrastructureHost AMI dansthe section called “Étape 1 : Lancez le produit”.

Configuration des points de terminaison VPC

Pour déployer RES et lancer des bureaux virtuels, vous devez Services AWS accéder à votre sous-réseau privé. Vous devez configurer les points de terminaison VPC pour fournir l'accès requis, et vous devrez répéter ces étapes pour chaque point de terminaison.

1. Si aucun point de terminaison n'a été configuré auparavant, suivez les instructions fournies dans Accès et Service AWS utilisation d'un point de terminaison VPC d'interface.
2. Sélectionnez un sous-réseau privé dans chacune des deux zones de disponibilité.

Service AWS	Nom du service
Application Auto Scaling	com.amazonaws. *region*.mise à l'échelle automatique de l'application
AWS CloudFormation	com.amazonaws. *region*.cloud formation
Amazon CloudWatch	com.amazonaws. *region*.surveillance
Amazon CloudWatch Logs	com.amazonaws. *region*.journaux

Service AWS	Nom du service
Amazon DynamoDB	com.amazonaws. *region*.dynamodb (nécessite un point de terminaison de passerelle)
Amazon EC2	com.amazonaws. *region*.ec2
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr .dkr
Amazon Elastic File System	com.amazonaws. *region*système de fichiers .elastic
Elastic Load Balancing	com.amazonaws. *region*. équilibrage de charge élastique
Amazon EventBridge	com.amazonaws. *region*.événements
Amazon FSx	com.amazonaws. *region*.fsx
AWS Key Management Service	com.amazonaws. *region*.km
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
AWS Lambda	com.amazonaws. *region*.lambda
Amazon S3	com.amazonaws. *region*.s3 (Nécessite un point de terminaison de passerelle créé par défaut dans RES.) Des points de terminaison d'interface Amazon S3 supplémentaires sont nécessaires pour le montage croisé de buckets dans un environnement isolé. Consultez la section Accès aux points de terminaison de l'interface Amazon Simple Storage Service.
AWS Secrets Manager	com.amazonaws. *region*.secretsmanager
Amazon Elastic Container Service	com.amazonaws. *region*.ecs

Service AWS	Nom du service
Amazon SES	com.amazonaws. *region*.email-smtp (Non pris en charge dans les zones de disponibilité suivantes : use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 et cac1-az4.)
AWS Security Token Service	com.amazonaws. *region*.sts
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
AWS Systems Manager	com.amazonaws. *region*Messages .ec2
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*Messages .sms

Connectez-vous aux services sans points de terminaison VPC

Pour intégrer des services qui ne prennent pas en charge les points de terminaison VPC, vous pouvez configurer un serveur proxy dans un sous-réseau public de votre VPC. Suivez ces étapes pour créer un serveur proxy avec l'accès minimum nécessaire pour un déploiement de Research and Engineering Studio en utilisant AWS Identity Center comme fournisseur d'identité.

1. Lancez une instance Linux dans le sous-réseau public du VPC que vous utiliserez pour votre déploiement RES.
   - Famille Linux — Amazon Linux 2 ou Amazon Linux 3
   - Architecture — x86
   - Type d'instance : t2.micro ou supérieur
   - Groupe de sécurité — TCP sur le port 3128 à partir de 0.0.0.0/0
2. Connectez-vous à l'instance pour configurer un serveur proxy.
   a. Ouvrez la connexion HTTP.
   b. Autorisez la connexion aux domaines suivants à partir de tous les sous-réseaux concernés :

- .amazonaws.com (pour les services génériques) AWS
- .amazoncognito.com (pour Amazon Cognito)
- .awsapps.com (pour Identity Center)
- .signin.aws (pour Identity Center)
- . amazonaws-us-gov.com (pour Gov Cloud)

c. Refusez toutes les autres connexions.

d. Activez et démarrez le serveur proxy.

e. Notez le PORT sur lequel le serveur proxy écoute.

3. Configurez votre table de routage pour autoriser l'accès au serveur proxy.

   a. Accédez à votre console VPC et identifiez les tables de routage pour les sous-réseaux que vous utiliserez pour les hôtes d'infrastructure et les hôtes VDI.

   b. Modifiez la table de routage pour permettre à toutes les connexions entrantes d'accéder à l'instance de serveur proxy créée lors des étapes précédentes.

   c. Procédez ainsi pour les tables de routage de tous les sous-réseaux (sans accès Internet) que vous allez utiliser pour VDIs Infrastructure/.

4. Modifiez le groupe de sécurité de l'instance EC2 du serveur proxy et assurez-vous qu'il autorise les connexions TCP entrantes sur le PORT sur lequel le serveur proxy écoute.

Définir les paramètres de déploiement d'un VPC privé

Dansthe section called “Étape 1 : Lancez le produit”, vous êtes censé saisir certains paramètres dans le CloudFormation modèle. Assurez-vous de définir les paramètres suivants comme indiqué pour réussir le déploiement dans le VPC privé que vous venez de configurer.

Paramètre	Input
InfrastructureHostAMI	Utilisez l'ID d'AMI d'infrastructure créé dansthe section called “Préparer les images Amazon Machine (AMIs)”.
IsLoadBalancerInternetFacing	Réglé sur false.

Paramètre	Input
LoadBalancerSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
InfrastructureHostSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
VdiSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
ClientIP	Vous pouvez choisir votre adresse CIDR VPC pour autoriser l'accès à toutes les adresses IP VPC.
HttpProxy	Exemple : `http://10.1.2.3:123`
HttpsProxy	Exemple : `http://10.1.2.3:123`

Paramètre	Input
NoProxy	Exemple :

```
127.0.0.1,169.254.169.254,169.254.17
0.2,localhost,us-east-1.res,us-east-
1.vpce.amazonaws.com,us-east-1.elb.a
mazonaws.com,s3.us-east-1.amazonaws.
com,s3.dualstack.us-east-1.amazonaws
.com,ec2.us-east-1.amazonaws.com,ec2
.us-east-1.api.aws,ec2messages.us-ea
st-1.amazonaws.com,ssm.us-east-1.ama
zonaws.com,ssmmessages.us-east-1.ama
zonaws.com,kms.us-east-1.amazonaws.c
om,secretsmanager.us-east-1.amazonaw
s.com,sqs.us-east-1.amazonaws.com,el
asticloadbalancing.us-east-1.amazona
ws.com,sns.us-east-1.amazonaws.com,l
ogs.us-east-1.amazonaws.com,logs.us-
east-1.api.aws,elasticfilesystem.us-
east-1.amazonaws.com,fsx.us-east-1.a
mazonaws.com,dynamodb.us-east-1.amaz
onaws.com,api.ecr.us-east-1.amazonaw
s.com,.dkr.ecr.us-east-1.amazonaws.c
om,kinesis.us-east-1.amazonaws.com,.
data-kinesis.us-east-1.amazonaws.com
,.control-kinesis.us-east-1.amazonaw
s.com,events.us-east-1.amazonaws.com
,cloudformation.us-east-1.amazonaws.
com,sts.us-east-1.amazonaws.com,appl
ication-autoscaling.us-east-1.amazon
aws.com,monitoring.us-east-1.amazona
ws.com,ecs.us-east-1.amazonaws.com,.
execute-api.us-east-1.amazonaws.com
```

Création de ressources externes

Cette CloudFormation pile crée des certificats de réseau, de stockage, d'Active Directory et de domaine (si un PortalDomainName est fourni). Vous devez disposer de ces ressources externes pour déployer le produit.

Vous pouvez télécharger le modèle de recettes avant le déploiement.

Temps de déploiement : environ 40 à 90 minutes

1. Connectez-vous à la CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Vérifiez que vous êtes connecté à votre compte administrateur.

2. Lancez le modèle dans la console.

   Si vous déployez dans la région AWS GovCloud (ouest des États-Unis), lancez le modèle dans le compte de GovCloud partition.

3. Entrez les paramètres du modèle :

Paramètre	Par défaut	Description
DomainName	`corp.res.com`	Domaine utilisé pour l'Active Directory. La valeur par défaut est fournie dans le `LDIF` fichier qui configure les utilisateurs de bootstrap . Si vous souhaitez utiliser les utilisateurs par défaut, laissez la valeur par défaut. Pour modifier la valeur, mettez-la à jour et fournissez un `LDIF` fichier distinct. Il n'est pas nécessaire que cela corresponde au domaine utilisé pour Active Directory.
SubDomain (GovCloud uniquement)		Ce paramètre est facultatif pour les régions commercia

Paramètre	Par défaut	Description
		les, mais obligatoire pour les GovCloud régions. Si vous fournissez un SubDomain, le paramètre sera préfixé DomainNam e par le paramètre fourni. Le nom de domaine Active Directory fourni deviendra un sous-domaine.
AdminPassword		Le mot de passe de l'adminis trateur Active Directory (nom d'utilisateur`Admin`). Cet utilisateur est créé dans le répertoire actif pour la phase d'amorçage initiale et n'est plus utilisé par la suite. Important : le format de ce champ peut être (1) un mot de passe en texte brut ou (2) l'ARN d'un AWS secret formaté par key/ value paire`{"passwor d":"somepassword"}` . Remarque : Le mot de passe de cet utilisateur doit répondre aux exigences de complexité du mot de passe d'Active Directory.

Paramètre	Par défaut	Description
ServiceAccountPassword		Mot de passe utilisé pour créer un compte de service (`ReadOnlyUser`). Ce compte est utilisé pour la synchronisation. Important : le format de ce champ peut être (1) un mot de passe en texte brut ou (2) l'ARN d'un AWS secret formaté par key/value paire`{"password":"somepassword"}` . Remarque : Le mot de passe de cet utilisateur doit répondre aux exigences de complexité du mot de passe d'Active Directory.
Paire de clés		Connecte les instances administratives à l'aide d'un client SSH. Remarque : Le gestionnaire de AWS Systems Manager session peut également être utilisé pour se connecter à des instances.

Paramètre	Par défaut	Description
LDIFS3Chemin	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	Le chemin Amazon S3 vers un fichier LDIF importé pendant la phase de démarrage de la configuration d'Active Directory. Pour plus d'informations, consultez Support LDIF. Le paramètre est prérempli avec un fichier qui crée un certain nombre d'utilisateurs dans Active Directory. Pour consulter le fichier, consultez le fichier res.ldif disponible dans. GitHub
ClientIpCidr		Adresse IP à partir de laquelle vous allez accéder au site. Par exemple, vous pouvez sélectionner votre adresse IP et l'utiliser `[IPADDRESS]/32` pour n'autoriser l'accès qu'à partir de votre hébergeur. Vous pouvez le mettre à jour après le déploiement.
ClientPrefixList		Entrez une liste de préfixes pour permettre l'accès aux nœuds de gestion Active Directory. Pour plus d'informations sur la création d'une liste de préfixes gérée, voir Utilisation de listes de préfixes gérées par le client.

Paramètre	Par défaut	Description
EnvironmentName	`res-[environment name]`	S'il `PortalDomainName` est fourni, ce paramètre est utilisé pour ajouter des balises aux secrets générés afin qu'ils puissent être utilisés dans l'environnement. Cela devra correspondre au `EnvironmentName` paramètre utilisé lors de la création de la pile RES. Si vous déployez plusieurs environnements dans votre compte, celui-ci doit être unique.
PortalDomainName		Pour les GovCloud déploiements, ne saisissez pas ce paramètre. Les certificats et les secrets ont été créés manuellement lors des prérequis. Le nom de domaine du compte dans Amazon Route 53. Si cela est fourni, un certificat public et un fichier clé seront générés et téléchargés sur AWS Secrets Manager. Si vous avez votre propre domaine et vos propres certificats, ce paramètre `EnvironmentName` peut être laissé vide.

4. Reconnaissez toutes les cases à cocher dans Capabilities, puis choisissez Create stack.

Étape 1 : Lancez le produit

Suivez les step-by-step instructions de cette section pour configurer et déployer le produit dans votre compte.

Temps de déploiement : environ 60 minutes

Vous pouvez télécharger le CloudFormation modèle de ce produit avant de le déployer.

Si vous déployez dans AWS GovCloud (ouest des États-Unis), utilisez ce modèle.

res-stack - Utilisez ce modèle pour lancer le produit et tous les composants associés. La configuration par défaut déploie la pile principale RES et les ressources d'authentification, de frontend et de backend.

> **Note**
>
> AWS CloudFormation les ressources sont créées à partir de constructions AWS Cloud Development Kit (AWS CDK) (AWS CDK).

Le AWS CloudFormation modèle déploie Research and Engineering Studio AWS dans le AWS Cloud. Vous devez remplir les prérequis avant de lancer la pile.

1. Connectez-vous à la CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.
2. Lancez le modèle.

   Pour effectuer un déploiement dans AWS GovCloud (ouest des États-Unis), lancez ce modèle.
3. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer la solution sous une autre forme Région AWS, utilisez le sélecteur de région dans la barre de navigation de la console.

   > **Note**
   >
   > Ce produit utilise le service Amazon Cognito, qui n'est actuellement pas disponible du tout. Régions AWS Vous devez lancer ce produit Région AWS là où Amazon Cognito est disponible. Pour connaître la disponibilité la plus récente par région, consultez la Région AWS liste complète des services.

4. Sous Paramètres, passez en revue les paramètres de ce modèle de produit et modifiez-les si nécessaire. Si vous avez déployé les ressources externes automatisées, vous pouvez trouver ces paramètres dans l'onglet Sorties de la pile de ressources externes.

Paramètre	Par défaut	Description
EnvironmentName	*<res-demo>*	Nom unique attribué à votre environnement RES commençant par res-, ne dépassant pas 11 caractères et sans majuscules.
AdministratorEmail		Adresse e-mail de l'utilisa teur qui termine la configura tion du produit. Cet utilisateur joue également le rôle d'un utilisateur hors pair en cas d'échec de l'intégration de l'authentification unique dans Active Directory.
InfrastructureHostAMI	ami- *[numbers or letters only]*	(Facultatif) Vous pouvez fournir un identifiant d'AMI personnalisé à utiliser pour tous les hôtes de l'infrastructure. Les versions actuellement prises en charge OSes sont Amazon Linux 2 RHEL8 RHEL9,, Windows Server 2019 et 2022 (x86), ainsi que Windows 10 et 11. Pour de plus amples informations, veuillez consulter Préparer les images Amazon Machine (AMIs).

Paramètre	Par défaut	Description
SSHKeyPaire		La paire de clés utilisée pour se connecter aux hôtes de l'infrastructure.
ClientIP	*x.x.x*.0/24 ou .0/32 *x.x.x*	Filtre d'adresse IP qui limite la connexion au système. Vous pouvez le mettre à jour ClientIpCidr après le déploiement.
ClientPrefixList		(Facultatif) Fournissez une liste de préfixes gérés pour IPs autoriser l'accès direct à l'interface utilisateur Web et au protocole SSH sur l'hôte Bastion.
IAMPermissionLimite		(Facultatif) Vous pouvez fournir un ARN de politique géré qui sera attaché en tant que limite d'autoris ation à tous les rôles créés dans RES. Pour de plus amples informations, veuillez consulter Définition de limites d'autorisation personnal isées.
VpcId		ID du VPC où les instances seront lancées.

Paramètre	Par défaut	Description
IsLoadBalancerInternetFacing		Sélectionnez true pour déployer un équilibreur de charge connecté à Internet (nécessite des sous-réseaux publics pour l'équilibreur de charge). Pour les déploiements nécessitant un accès Internet restreint, sélectionnez false.
LoadBalancerSubnets		Sélectionnez au moins deux sous-réseaux dans différentes zones de disponibilité où les équilibreurs de charge seront lancés. Pour les déploiements nécessitant un accès Internet restreint, sélectionnez des sous-réseaux privés. Pour les déploiements nécessitant un accès à Internet, sélectionnez des sous-réseaux publics. Si plus de deux ont été créés par la pile réseau externe, sélectionnez tous ceux qui ont été créés.

Paramètre	Par défaut	Description
InfrastructureHostSubnets		Sélectionnez au moins deux sous-réseaux privés dans différentes zones de disponibilité où les hôtes de l'infrastructure seront lancés. Si plus de deux ont été créés par la pile réseau externe, sélectionnez tous ceux qui ont été créés.
VdiSubnets		Sélectionnez au moins deux sous-réseaux privés dans différentes zones de disponibilité où les instances VDI seront lancées. Si plus de deux ont été créés par la pile réseau externe, sélection nez tous ceux qui ont été créés.
ActiveDirectoryName	`corp.res.com`	Domaine de l'Active Directory. Il n'est pas nécessaire qu'il correspon de au nom de domaine du portail.
ADShortNom	`corp`	Nom abrégé de l'Active Directory. Ce nom est également appelé le nom NetBIOS.
Base LDAP	**`DC=corp,DC=res,DC=com`**	Un chemin LDAP vers la base au sein de la hiérarchie LDAP.

Paramètre	Par défaut	Description
LDAPConnectionURI		Un chemin ldap ://unique accessible par le serveur hôte d'Active Directory . Si vous avez déployé les ressources externes automatisées avec le domaine AD par défaut, vous pouvez utiliser ldap : // corp.res.com.
ServiceAccountCredentialsSecretArn		Fournissez un ARN secret contenant le nom d'utilisateur et le mot de passe de l' ServiceAccount utilisateur Active Directory, sous la forme d'une paire nom d' key/value utilisateur:mot de passe.
Utilisateur Sou		Unité organisationnelle au sein d'AD pour les utilisateurs qui se synchroniseront.
Groupe SOU		Unité organisationnelle au sein d'AD pour les groupes qui seront synchronisés.
SudoersGroupName	RESAdministrators	Nom du groupe contenant tous les utilisateurs disposant d'un accès sudoer sur les instances lors de l'installation et d'un accès administrateur sur RES.

Paramètre	Par défaut	Description
Ordinateur SOU		Unité organisationnelle au sein d'AD que les instances rejoindront.
Domaine : TLSCertificate SecretArn		(Facultatif) Fournissez un ARN secret de certificat TLS de domaine pour permettre la communication TLS avec AD.
EnableLdapIDMapping		Détermine si les numéros UID et GID sont générés par SSSD ou si les numéros fournis par l'AD sont utilisés. Définissez sur True pour utiliser l'UID et le GID générés par SSSD, ou sur False pour utiliser l'UID et le GID fournis par l'AD. Dans la plupart des cas, ce paramètre doit être défini sur True.
Désactiver ADJoin	False	Pour empêcher les hôtes Linux de rejoindre le domaine du répertoire, passez à True. Dans le cas contraire, conservez le paramètre par défaut False.
ServiceAccountUserDN		Indiquez le nom distincti f (DN) de l'utilisateur du compte de service dans le répertoire.

Paramètre	Par défaut	Description
SharedHomeFilesystemID		ID EFS à utiliser pour le système de fichiers de base partagé pour les hôtes Linux VDI.
CustomDomainNamefo rWebApp		(Facultatif) Sous-domaine utilisé par le portail Web pour fournir des liens vers la partie Web du système.
CustomDomainNameforVDI		(Facultatif) Sous-domaine utilisé par le portail Web pour fournir des liens vers la partie VDI du système.
ACMCertificateARNf orWebApp		(Facultatif) Lorsque vous utilisez la configuration par défaut, le produit héberge l'application Web sous le domaine amazonaws.com. Vous pouvez héberger les produits et services sous votre domaine. Si vous avez déployé les ressource s externes automatisées, celles-ci ont été générées pour vous et les informations se trouvent dans les sorties de la pile res-bi. Si vous devez générer un certificat pour votre application Web, consultezGuide de configura tion.

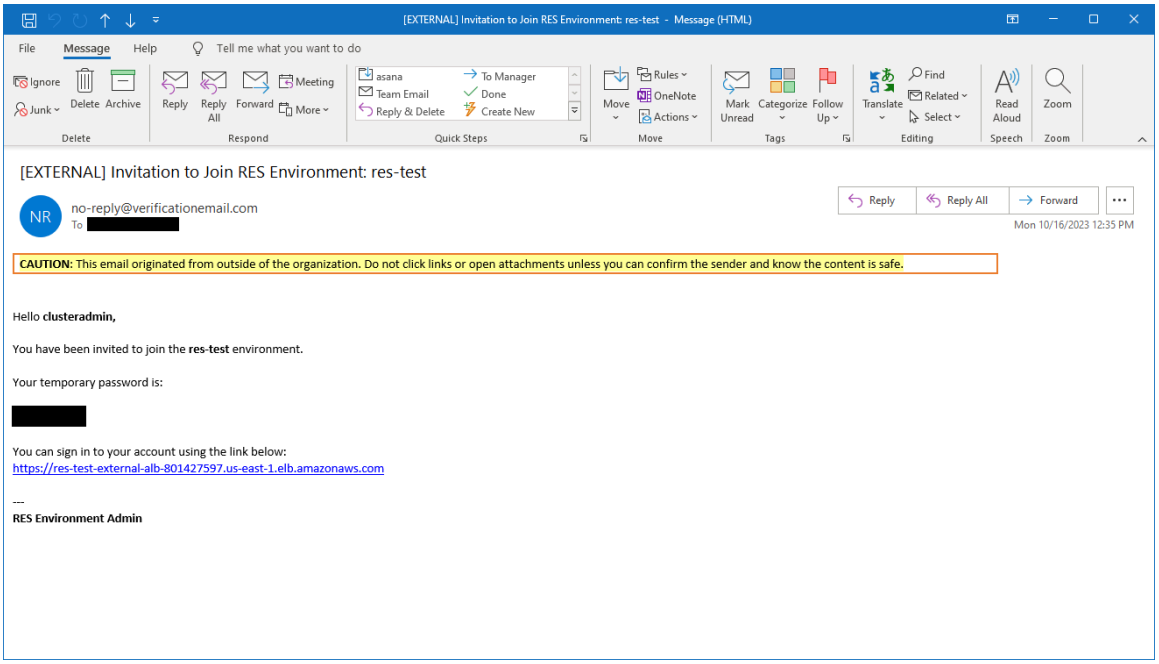
Paramètre	Par défaut	Description
CertificateSecretARNforVDI		(Facultatif) Ce secret ARN stocke le certificat public du certificat public de votre portail Web. Si vous définissez un nom de domaine de portail pour vos ressources externes automatisées, vous pouvez trouver cette valeur sous l'onglet Outputs de la pile res-bi.
PrivateKeySecretARNforVDI		(Facultatif) Ce secret ARN stocke la clé privée du certificat de votre portail Web. Si vous définissez un nom de domaine de portail pour vos ressources externes automatisées, vous pouvez trouver cette valeur sous l'onglet Outputs de la pile res-bi.

5. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 60 minutes.

Étape 2 : Connectez-vous pour la première fois

Une fois la pile de produits déployée sur votre compte, vous recevrez un e-mail contenant vos informations d'identification. Utilisez l'URL pour vous connecter à votre compte et configurer l'espace de travail pour les autres utilisateurs.



Une fois que vous vous êtes connecté pour la première fois, vous pouvez configurer les paramètres du portail Web pour vous connecter au fournisseur SSO. Pour obtenir des informations de configuration après le déploiement, consultez leGuide de configuration. Notez qu'il `clusteradmin` s'agit d'un compte révolutionnaire : vous pouvez l'utiliser pour créer des projets et attribuer des membres d'utilisateurs ou de groupes à ces projets ; il ne peut pas attribuer de piles logicielles ni déployer un bureau pour lui-même.

Mettre à jour le produit

Research and Engineering Studio (RES) dispose de deux méthodes pour mettre à jour le produit, selon qu'il s'agit d'une mise à jour majeure ou mineure.

RES utilise un schéma de version basé sur la date. Une version majeure utilise l'année et le mois, et une version mineure ajoute un numéro de séquence si nécessaire. Par exemple, la version 2024.01 a été publiée en janvier 2024 en tant que version majeure ; la version 2024.01.01 était une mise à jour mineure de cette version.

Rubriques

Mises à jour majeures des versions

Research and Engineering Studio utilise des instantanés pour faciliter la migration d'un environnement RES antérieur vers le dernier sans perdre vos paramètres d'environnement. Vous pouvez également utiliser ce processus pour tester et vérifier les mises à jour de votre environnement avant d'intégrer des utilisateurs.

Pour mettre à jour votre environnement avec la dernière version de RES :

1. Créez un instantané de votre environnement actuel. Consultez the section called “Créer un instantané”.
2. Redéployez RES avec la nouvelle version. Consultez the section called “Étape 1 : Lancez le produit”.
3. Appliquez l'instantané à votre environnement mis à jour. Consultez the section called “Appliquer un instantané”.
4. Vérifiez que toutes les données ont bien migré vers le nouvel environnement.

Mises à jour mineures des versions

Pour les mises à jour mineures de RES, aucune nouvelle installation n'est requise. Vous pouvez mettre à jour la pile RES existante en mettant à jour son CloudFormation modèle. Vérifiez la version

de votre environnement RES actuel CloudFormation avant de déployer la mise à jour. Vous trouverez le numéro de version au début du modèle.

Par exemple : `"Description": "RES_2024.1"`

Pour effectuer une mise à jour de version mineure :

1. Téléchargez le dernier CloudFormation modèle enthe section called “Étape 1 : Lancez le produit”.
2. Ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
3. Dans Stacks, recherchez et sélectionnez la pile principale. Il doit apparaître sous la forme*<stack-name>*.
4. Choisissez Mettre à jour.
5. Choisissez Remplacer le modèle actuel.
6. Pour Source du modèle, choisissez Charger un fichier de modèle.
7. Choisissez Choisir un fichier et chargez le modèle que vous avez téléchargé.
8. Dans Spécifier les détails de la pile, choisissez Next. Il n'est pas nécessaire de mettre à jour les paramètres.
9. Dans Configurer les options de pile, choisissez Next.
10. Lors de la révision<stack-name>, choisissez Soumettre.

Désinstallez le produit

Vous pouvez désinstaller le studio de recherche et d'ingénierie AWS du produit depuis AWS Management Console ou en utilisant le AWS Command Line Interface. Vous devez supprimer manuellement les compartiments Amazon Simple Storage Service (Amazon S3) créés par ce produit. Ce produit ne supprime pas automatiquement < EnvironmentName >- shared-storage-security-group si vous avez enregistré des données à conserver.

En utilisant le AWS Management Console

1. Connectez-vous à la console AWS CloudFormation.
2. Sur la page Stacks, sélectionnez la pile d'installation de ce produit.
3. Sélectionnez Delete (Supprimer).

En utilisant AWS Command Line Interface

Déterminez si le AWS Command Line Interface (AWS CLI) est disponible dans votre environnement. Pour les instructions d'installation, reportez-vous à la section Qu'est-ce que AWS Command Line Interface le guide de AWS CLI l'utilisateur contient ? Après avoir confirmé que le produit AWS CLI est disponible et configuré sur le compte administrateur de la région où le produit a été déployé, exécutez la commande suivante.

```
$ aws cloudformation delete-stack --stack-name <RES-stack-name>
```

Suppression du shared-storage-security-group

> **Warning**
>
> Le produit conserve ce système de fichiers par défaut pour éviter toute perte de données involontaire. Si vous choisissez de supprimer le groupe de sécurité et les systèmes de fichiers associés, toutes les données conservées dans ces systèmes seront définitivement supprimées. Nous vous recommandons de sauvegarder les données ou de les réaffecter à un nouveau groupe de sécurité.

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/efs/.
2. Supprimez tous les systèmes de fichiers associés à`<RES-stack-name>-shared-storage-security-group`. Vous pouvez également réaffecter ces systèmes de fichiers à un autre groupe de sécurité pour conserver les données.
3. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
4. Supprimez la `<RES-stack-name>-shared-storage-security-group`.

Supprimer les compartiments Amazon S3

Ce produit est configuré pour conserver le compartiment Amazon S3 créé par le produit (à déployer dans une région optionnelle) si vous décidez de supprimer la AWS CloudFormation pile afin d'éviter toute perte de données accidentelle. Après avoir désinstallé le produit, vous pouvez supprimer manuellement ce compartiment S3 si vous n'avez pas besoin de conserver les données. Suivez ces étapes pour supprimer le compartiment Amazon S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Buckets dans le volet de navigation.
3. Localisez les compartiments `stack-name` S3.
4. Sélectionnez chaque compartiment Amazon S3, puis choisissez Empty. Vous devez vider chaque seau.
5. Sélectionnez le compartiment S3 et choisissez Supprimer.

Pour supprimer des compartiments S3 à l'aide de AWS CLI, exécutez la commande suivante :

```
$ aws s3 rb s3://<bucket-name> --force
```

> **Note**
>
> La `--force` commande vide le compartiment de son contenu.

Guide de configuration

Ce guide de configuration fournit des instructions post-déploiement destinées à un public technique sur la manière de personnaliser et d'intégrer davantage le studio de recherche et d'ingénierie AWS du produit.

Rubriques

Gestion des identités

Research and Engineering Studio peut utiliser n'importe quel fournisseur d'identité conforme à la norme SAML 2.0. Pour utiliser Amazon Cognito en tant qu'annuaire d'utilisateurs natif permettant aux utilisateurs de se connecter au portail Web et à Linux à l'aide des identités utilisateur VDIs Cognito, consultez. Configuration des utilisateurs d'Amazon Cognito Si vous avez déployé RES à l'aide de ressources externes ou si vous prévoyez d'utiliser le centre d'identité IAM, consultezConfiguration de l'authentification unique (SSO) avec IAM Identity Center. Si vous avez votre propre fournisseur d'identité conforme à la norme SAML 2.0, consultezConfiguration de votre fournisseur d'identité pour l'authentification unique (SSO).

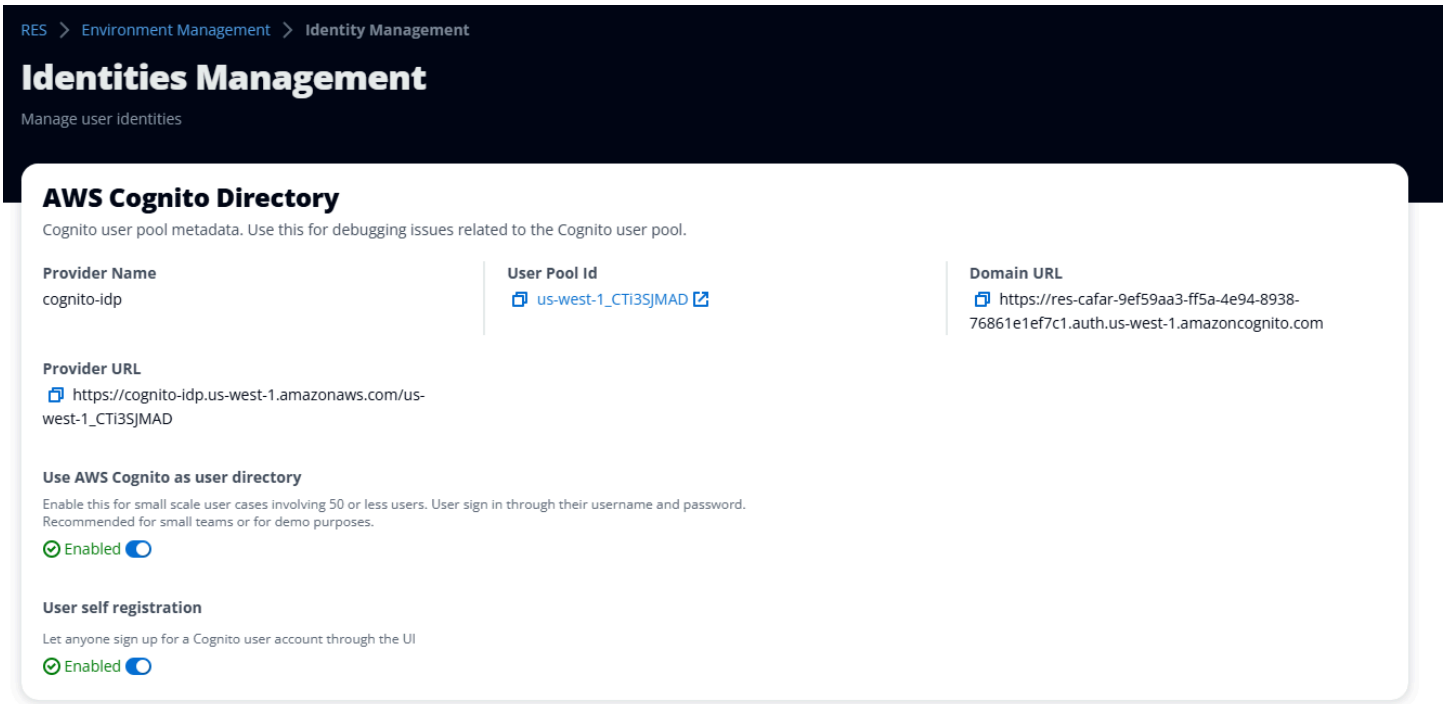
Rubriques

Configuration des utilisateurs d'Amazon Cognito

Le studio de recherche et d'ingénierie (RES) vous permet de configurer Amazon Cognito en tant qu'annuaire d'utilisateurs natif. Cela permet aux utilisateurs de se connecter au portail Web et sur Linux avec les identités d'utilisateur Amazon VDIs Cognito. Les administrateurs peuvent importer plusieurs utilisateurs dans le groupe d'utilisateurs à l'aide d'un fichier csv depuis AWS la console. Pour en savoir plus sur l'importation groupée d'utilisateurs, consultez la section Importation d'utilisateurs dans des groupes d'utilisateurs à partir d'un fichier CSV dans le manuel Amazon Cognito Developer Guide. RES prend en charge l'utilisation conjointe d'un annuaire d'utilisateurs natif basé sur Amazon Cognito et d'un SSO.

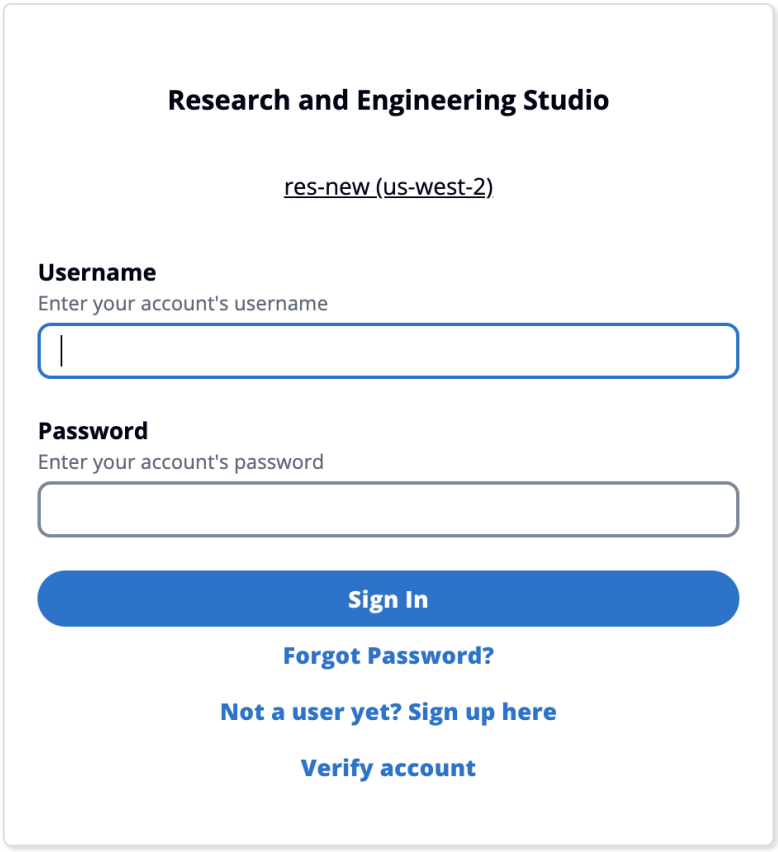
Configuration administrative

En tant qu'administrateur RES, pour configurer l'environnement RES afin d'utiliser Amazon Cognito comme annuaire d'utilisateurs, cliquez sur le bouton Utiliser Amazon Cognito comme annuaire d'utilisateurs sur la page de gestion des identités accessible depuis la page de gestion de l'environnement. Pour permettre aux utilisateurs de s'auto-enregistrer, activez le bouton d'auto-enregistrement des utilisateurs sur cette même page.



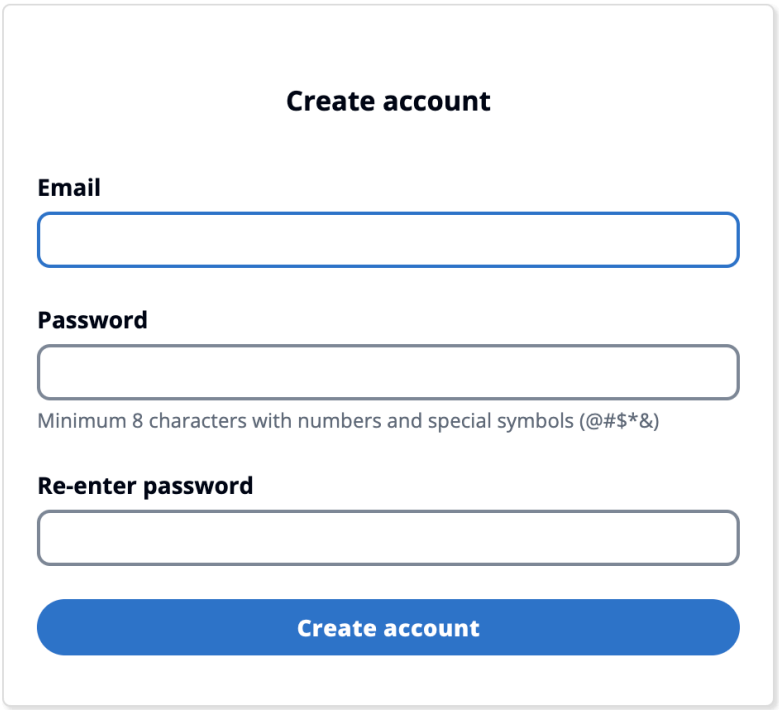
Flux de connexion up/sign de l'utilisateur

Si l'enregistrement automatique des utilisateurs est activé, vous pouvez communiquer à vos utilisateurs l'URL de votre application Web. Les utilisateurs y trouveront une option indiquant Vous n'êtes pas encore un utilisateur ? Inscrivez-vous ici.

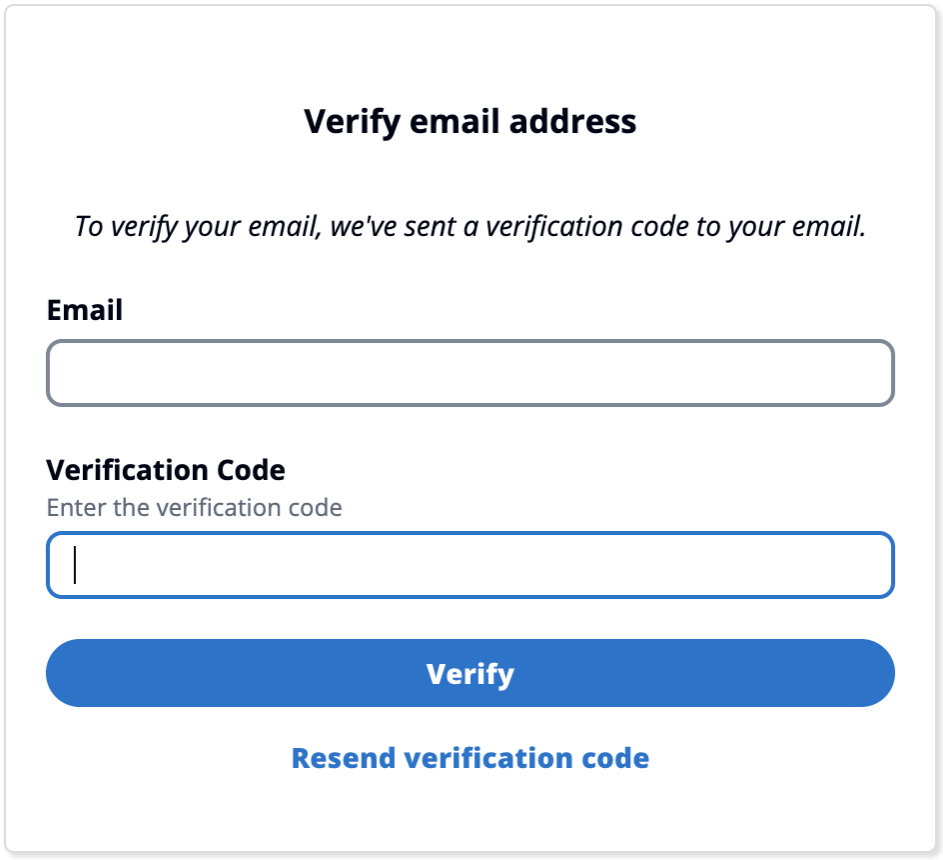


Flux d'inscription

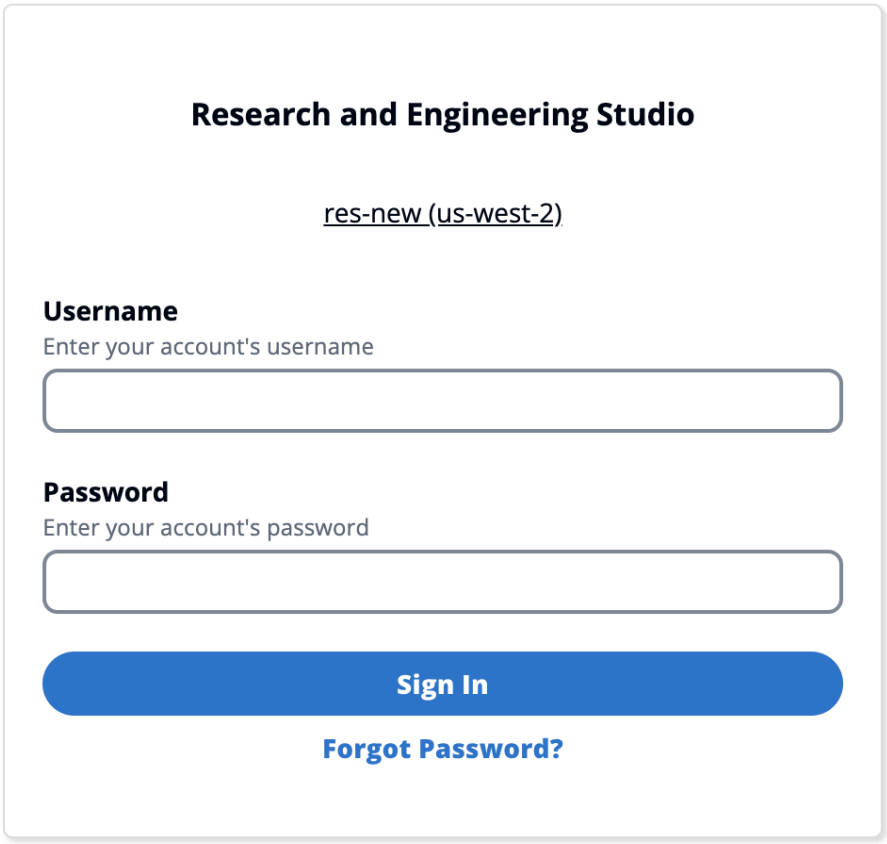
Utilisateurs qui ont choisi Pas encore utilisateur ? Inscrivez-vous ici. Il leur sera demandé de saisir leur e-mail et leur mot de passe pour créer un compte.



Dans le cadre du processus d'inscription, les utilisateurs seront invités à saisir le code de vérification reçu dans leur e-mail pour terminer le processus d'inscription.

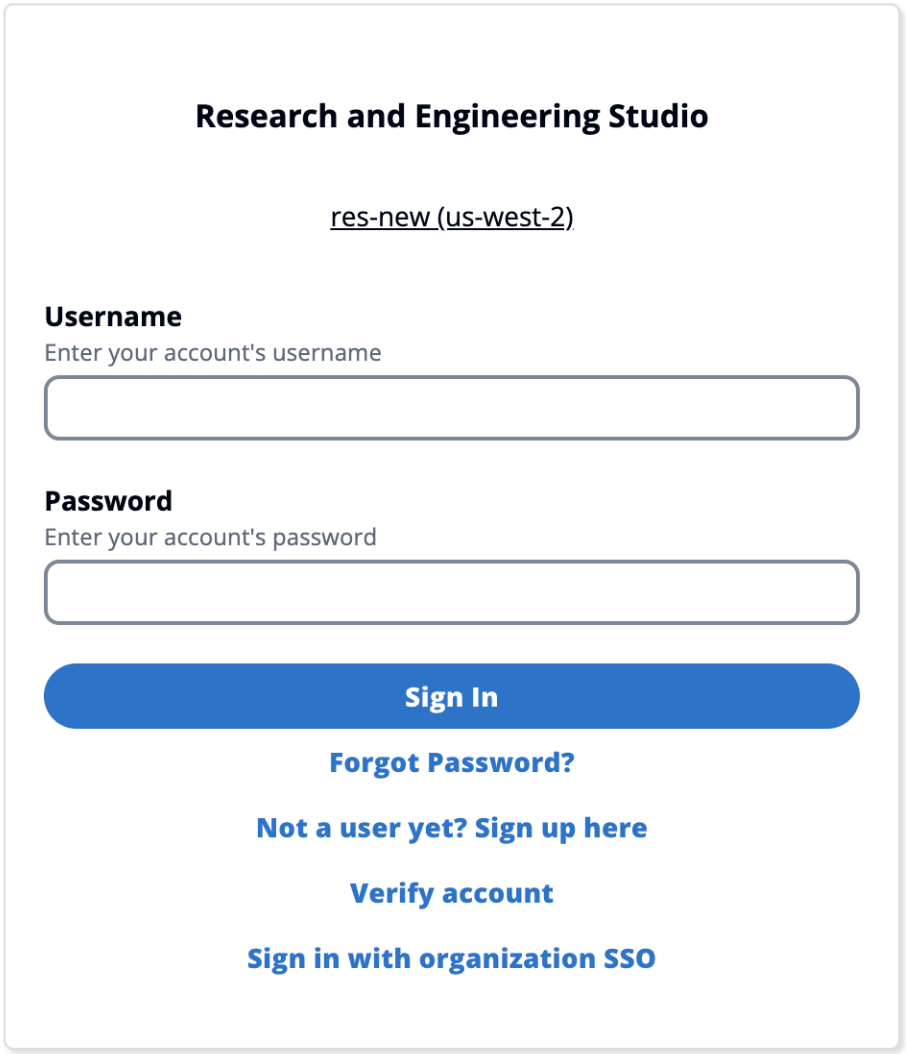


Si l'auto-inscription est désactivée, les utilisateurs ne verront pas le lien d'inscription. Les administrateurs doivent configurer les utilisateurs dans Amazon Cognito en dehors de RES. (Voir Création de comptes utilisateur en tant qu'administrateur dans le manuel Amazon Cognito Developer Guide.)



Options de la page de connexion

Si l'authentification unique et Amazon Cognito sont toutes deux activées, une option permettant de se connecter avec l'authentification unique de l'organisation apparaît. Lorsque les utilisateurs cliquent sur cette option, ils sont redirigés vers leur page de connexion SSO. Par défaut, les utilisateurs s'authentifient auprès d'Amazon Cognito s'il est activé.



Constaintes

- Le nom de votre groupe Amazon Cognito peut comporter un maximum de six lettres ; seules les lettres minuscules sont acceptées.
- L'inscription à Amazon Cognito n'autorisera pas deux adresses e-mail portant le même nom d'utilisateur mais une adresse de domaine différente.
- Si Active Directory et Amazon Cognito sont activés et que le système détecte un nom d'utilisateur dupliqué, seuls les utilisateurs d'Active Directory seront autorisés à s'authentifier. Les administrateurs doivent prendre des mesures pour ne pas configurer de noms d'utilisateur dupliqués entre Amazon Cognito et leur Active Directory.

- Les utilisateurs de Cognito ne seront pas autorisés à lancer une application basée sur Windows VDIs car RES ne prend pas en charge l'authentification basée sur Amazon Cognito pour les instances Windows.

Synchronisation

RES synchronise sa base de données avec les informations relatives aux utilisateurs et aux groupes provenant d'Amazon Cognito toutes les heures. Tous les utilisateurs appartenant au groupe « admins » se verront attribuer le privilège sudo dans leur. VDIs

Vous pouvez également lancer la synchronisation manuellement depuis la console Lambda.

Lancez le processus de synchronisation manuellement :

1. Ouvrez la console Lambda.
2. Recherchez le Lambda de synchronisation Cognito. Ce Lambda suit cette convention de dénomination :. `{RES_ENVIRONMENT_NAME}_cognito-sync-lambda`
3. Sélectionnez Test.
4. Dans la section Test event, cliquez sur le bouton Test en haut à droite. Le format du corps de l'événement n'a pas d'importance.

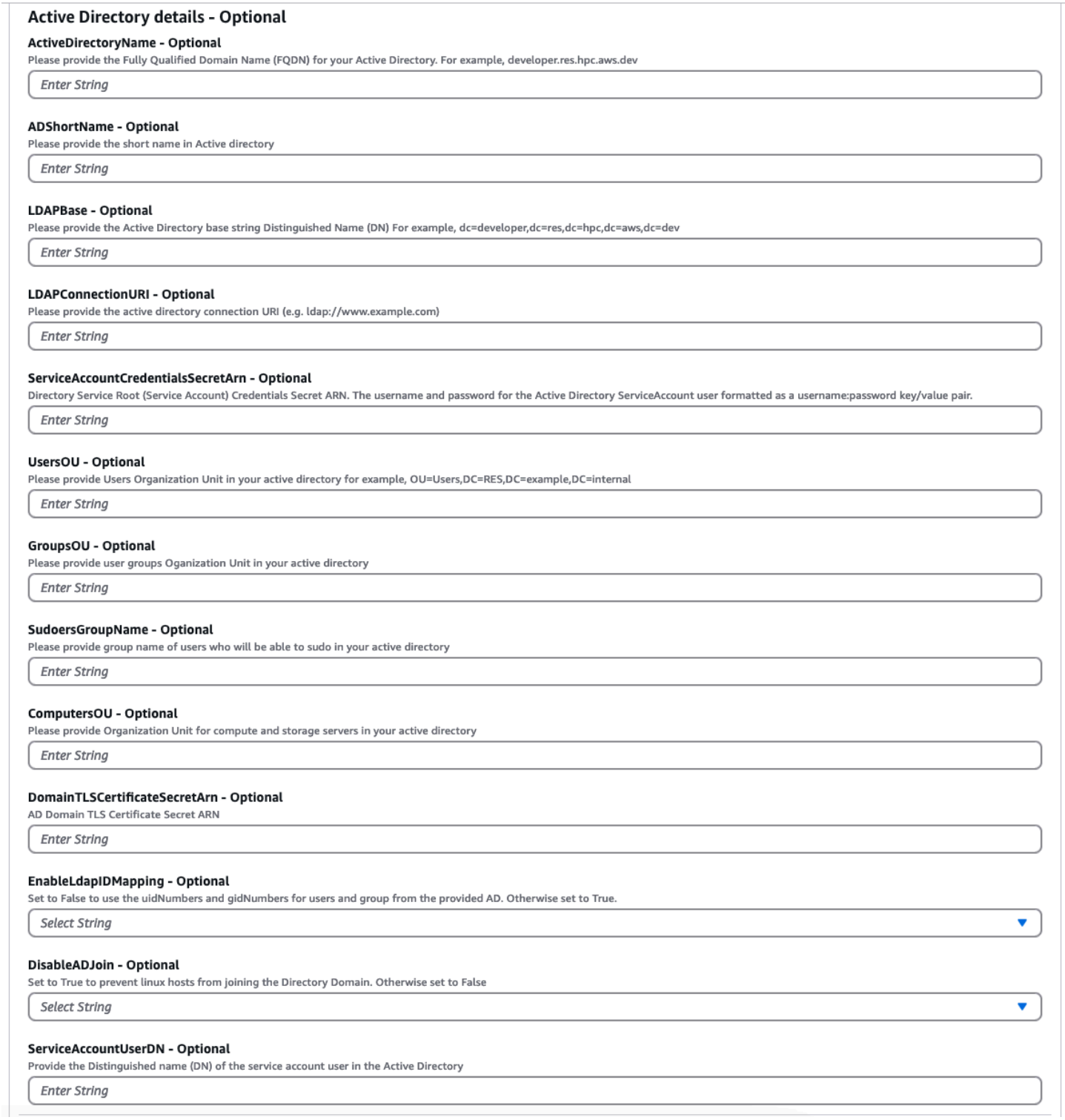
Considérations relatives à la sécurité pour Cognito

Avant la version 2024.12, la journalisation de l'activité des utilisateurs, qui fait partie de la fonctionnalité du plan Amazon Cognito Plus, était activée par défaut. Nous l'avons supprimée de notre déploiement de base afin de réduire les coûts pour les clients qui souhaitent essayer RES. Vous pouvez réactiver cette fonctionnalité si nécessaire pour l'aligner sur les paramètres de sécurité cloud de votre organisation.

Synchronisation Active Directory

Configuration d'exécution

Tous les paramètres CFN liés à Active Directory (AD) sont facultatifs lors de l'installation.

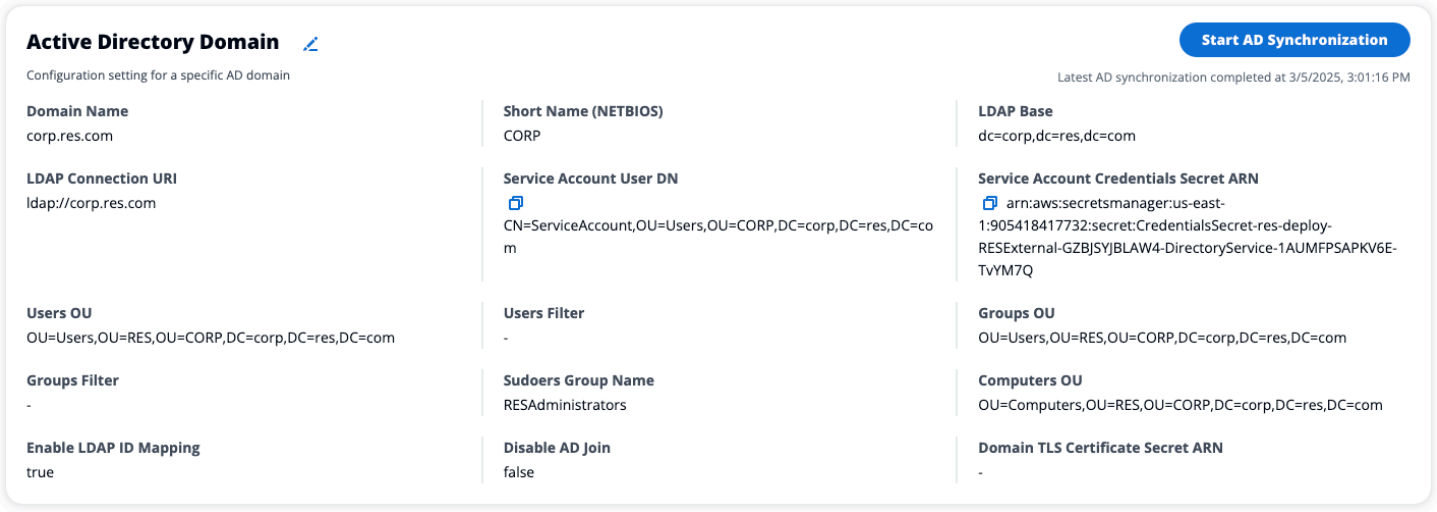


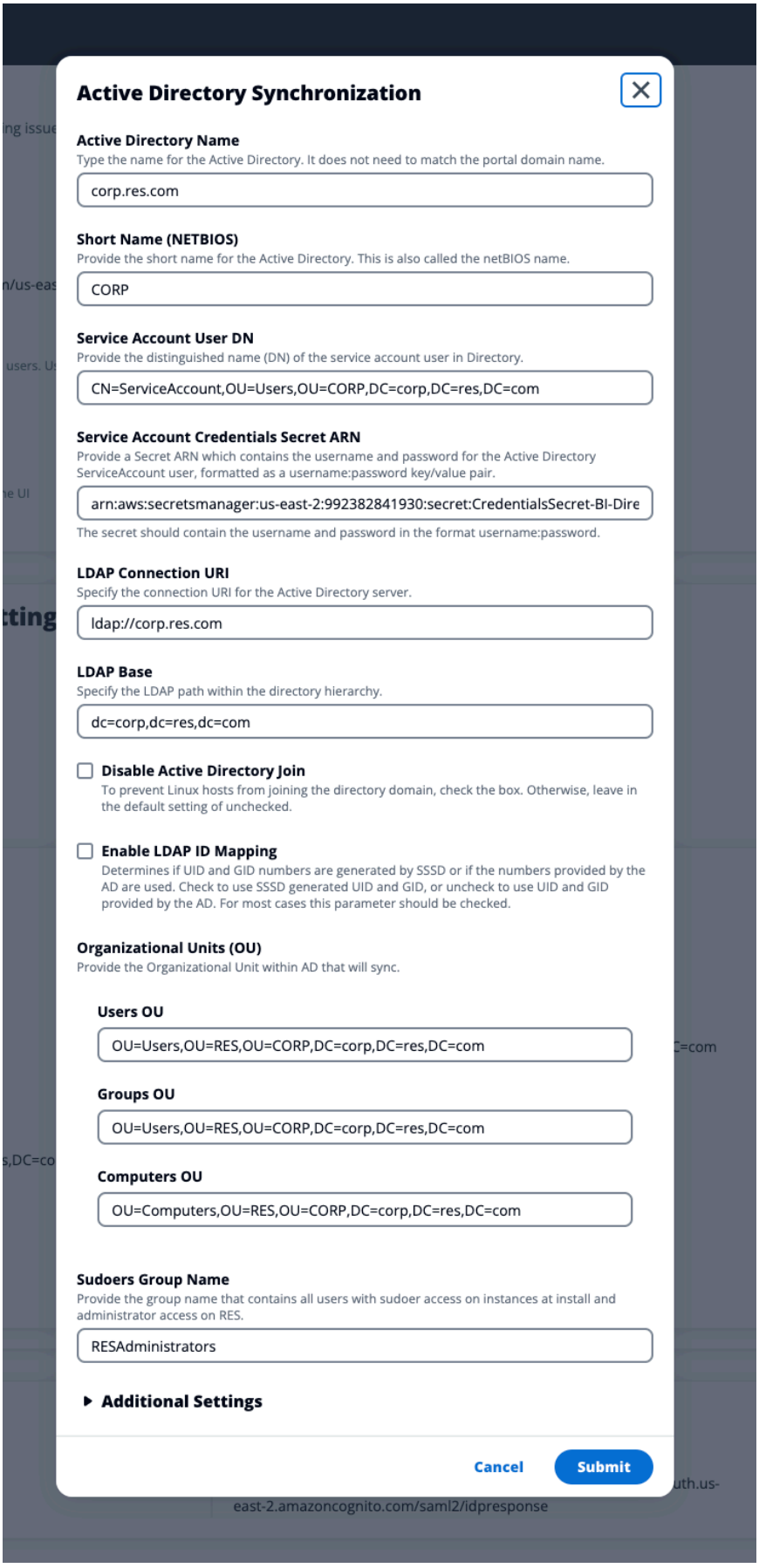
Pour tout ARN secret fourni lors de l'exécution (par exemple, `ServiceAccountCredentialsSecretArn` ou`DomainTLSCertificateSecretArn`), assurez-vous d'ajouter les balises suivantes au secret pour que RES obtienne l'autorisation de lire la valeur du secret :

- clé : `res:EnvironmentName`, valeur : *`<your RES environment name>`*
- clé : `res:ModuleName`, valeur : `directoryservice`

Toutes les mises à jour de configuration AD sur le portail Web seront automatiquement récupérées lors de la prochaine synchronisation AD planifiée (toutes les heures). Les utilisateurs peuvent avoir besoin de reconfigurer le SSO après avoir modifié la configuration AD (par exemple, s'ils passent à un autre AD).

Après l'installation initiale, les administrateurs peuvent consulter ou modifier la configuration AD sur le portail Web RES sous la page Gestion des identités :




Active Directory Synchronization
Active Directory Name
Type the name for the Active Directory. It does not need to match the portal domain name.
corp.res.com
Short Name (NETBIOS)
Provide the short name for the Active Directory. This is also called the netBIOS name.
CORP
Service Account User DN
Provide the distinguished name (DN) of the service account user in Directory.
CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com
Service Account Credentials Secret ARN
Provide a Secret ARN which contains the username and password for the Active Directory ServiceAccount user, formatted as a username:password key/value pair.
arn:aws:secretsmanager:us-east-2:992382841930:secret:CredentialsSecret-BI-Dire
The secret should contain the username and password in the format username:password.
LDAP Connection URI
Specify the connection URI for the Active Directory server.
ldap://corp.res.com
LDAP Base
Specify the LDAP path within the directory hierarchy.
dc=corp,dc=res,dc=com
Disable Active Directory Join
To prevent Linux hosts from joining the directory domain, check the box. Otherwise, leave in the default setting of unchecked.
Enable LDAP ID Mapping
Determines if UID and GID numbers are generated by SSSD or if the numbers provided by the AD are used. Check to use SSSD generated UID and GID, or uncheck to use UID and GID provided by the AD. For most cases this parameter should be checked.
Organizational Units (OU)
Provide the Organizational Unit within AD that will sync.
Users OU
OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Groups OU
OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Computers OU
OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Sudoers Group Name
Provide the group name that contains all users with sudoer access on instances at install and administrator access on RES.
RESAdministrators
Additional Settings
Cancel
Submit
east-2.amazoncognito.com/saml2/idpresponse

Réglages supplémentaires

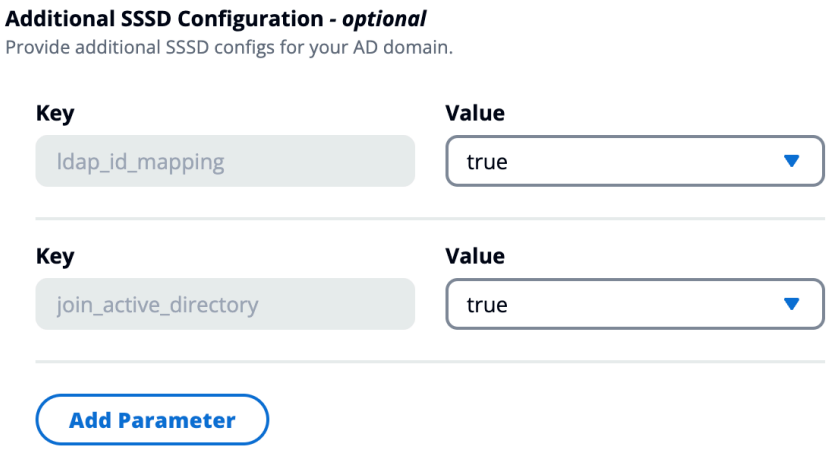
Filtres

Les administrateurs peuvent filtrer les utilisateurs ou les groupes à synchroniser à l'aide des options Filtre des utilisateurs et Filtre des groupes. Les filtres doivent respecter la syntaxe du filtre LDAP. Voici un exemple de filtre :

```
(sAMAccountname=<user>)
```

Paramètres SSSD personnalisés

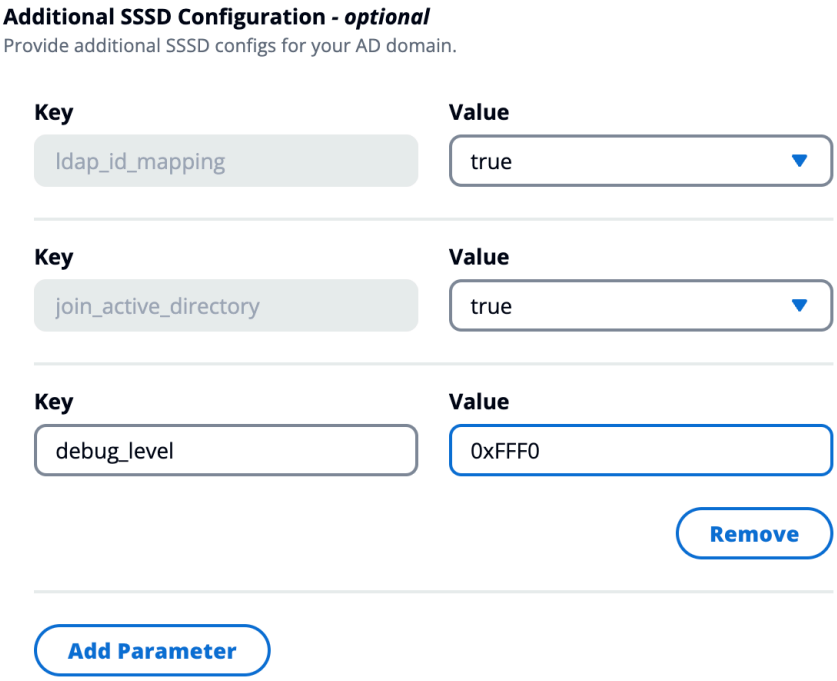
Les administrateurs peuvent fournir un dictionnaire de paires clé-valeur contenant des paramètres et des valeurs SSSD à écrire dans la `[domain_type/DOMAIN_NAME]` section du fichier de configuration SSSD sur les instances de cluster. RES applique automatiquement les mises à jour SSSD : il redémarre le service SSSD sur les instances de cluster et déclenche le processus de synchronisation AD. Pour une description complète du fichier de configuration SSSD, consultez les pages de manuel Linux pour`SSSD`.



Les paramètres et valeurs SSSD doivent être compatibles avec la configuration RES SSSD décrite ici :

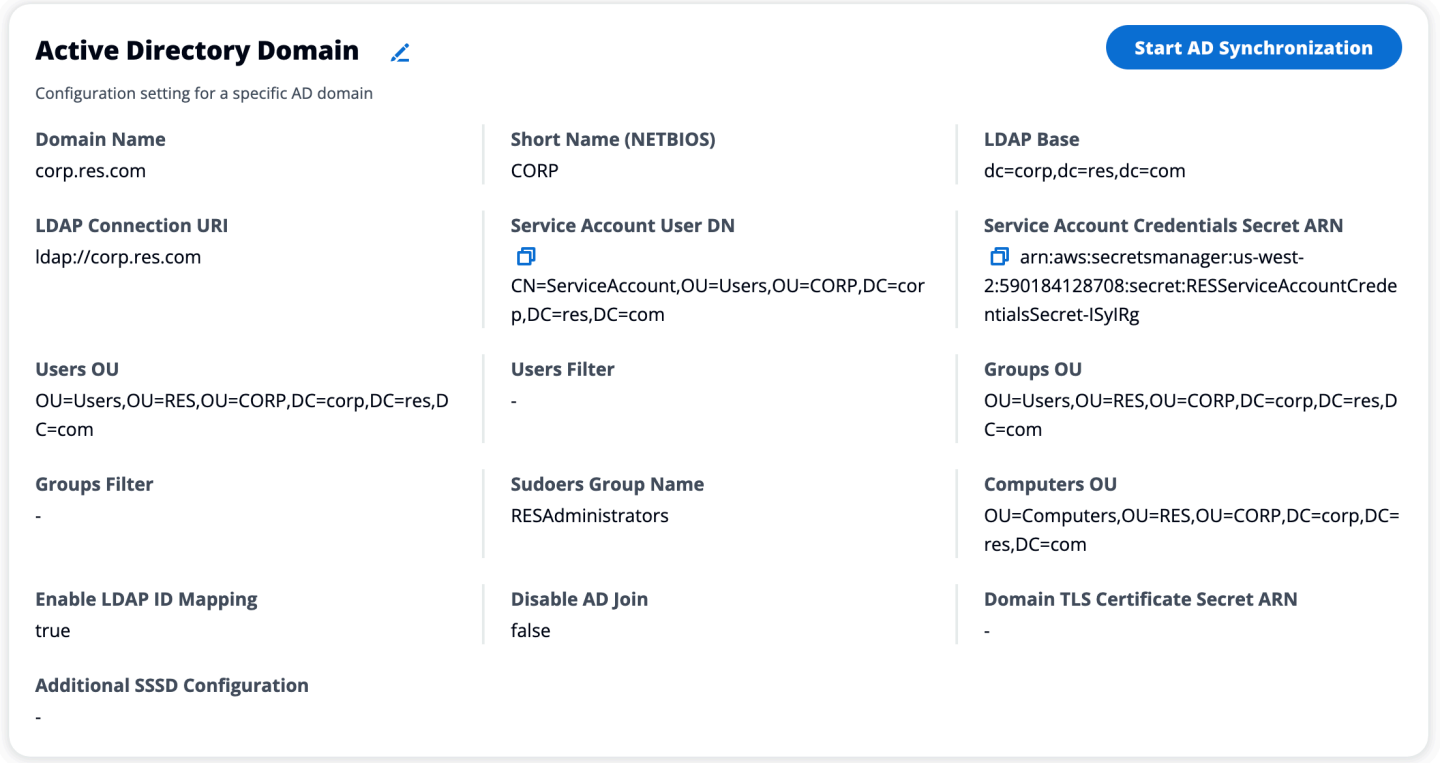
- `id_provider`est défini en interne par RES et ne doit pas être modifié.
- Les configurations liées à AD`ldap_uri`, y compris`ldap_search_base`, `ldap_default_bind_dn` et `ldap_default_authtok` sont définies en fonction des autres configurations AD fournies et ne doivent pas être modifiées.

L'exemple suivant active le niveau de débogage pour les journaux SSSD :

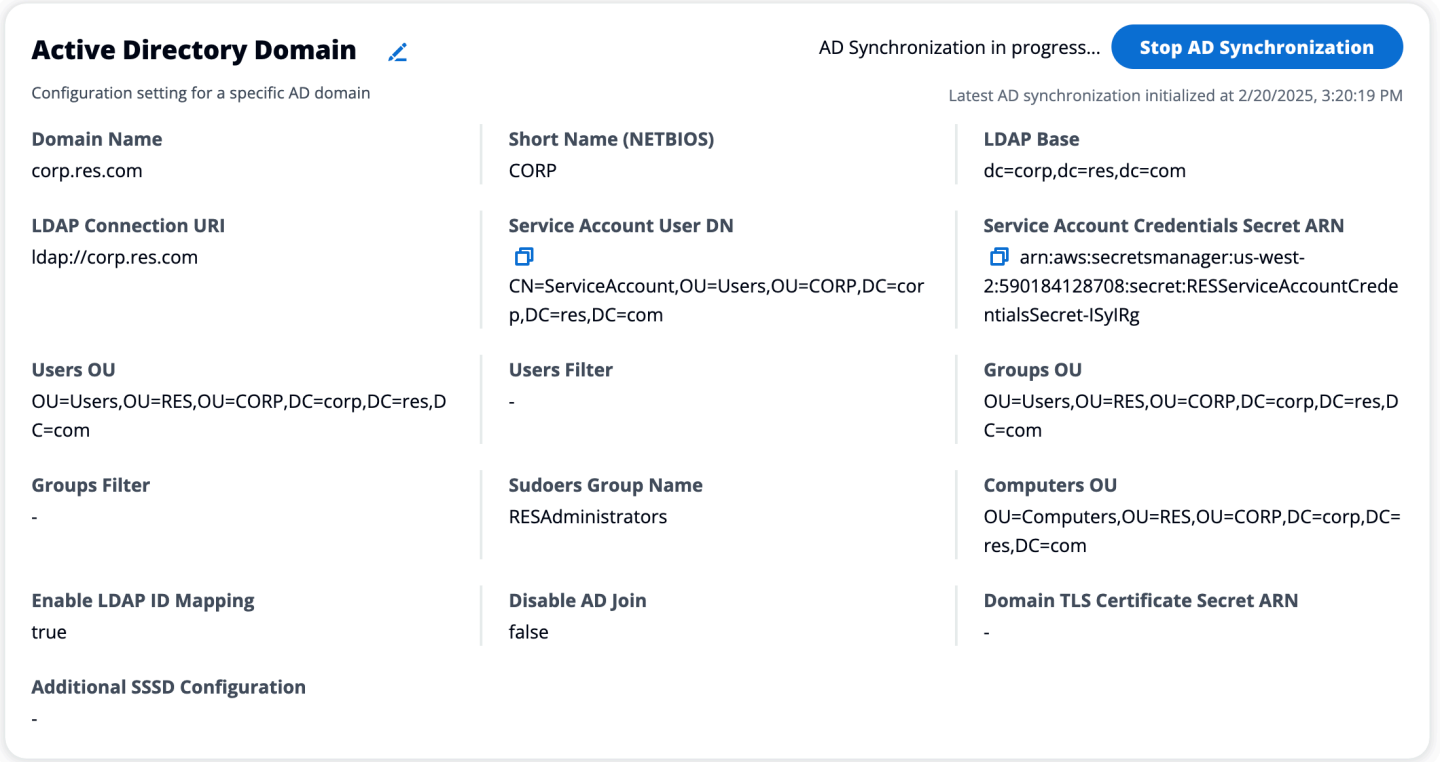


Comment démarrer ou arrêter manuellement la synchronisation (versions 2025.03 et ultérieures)

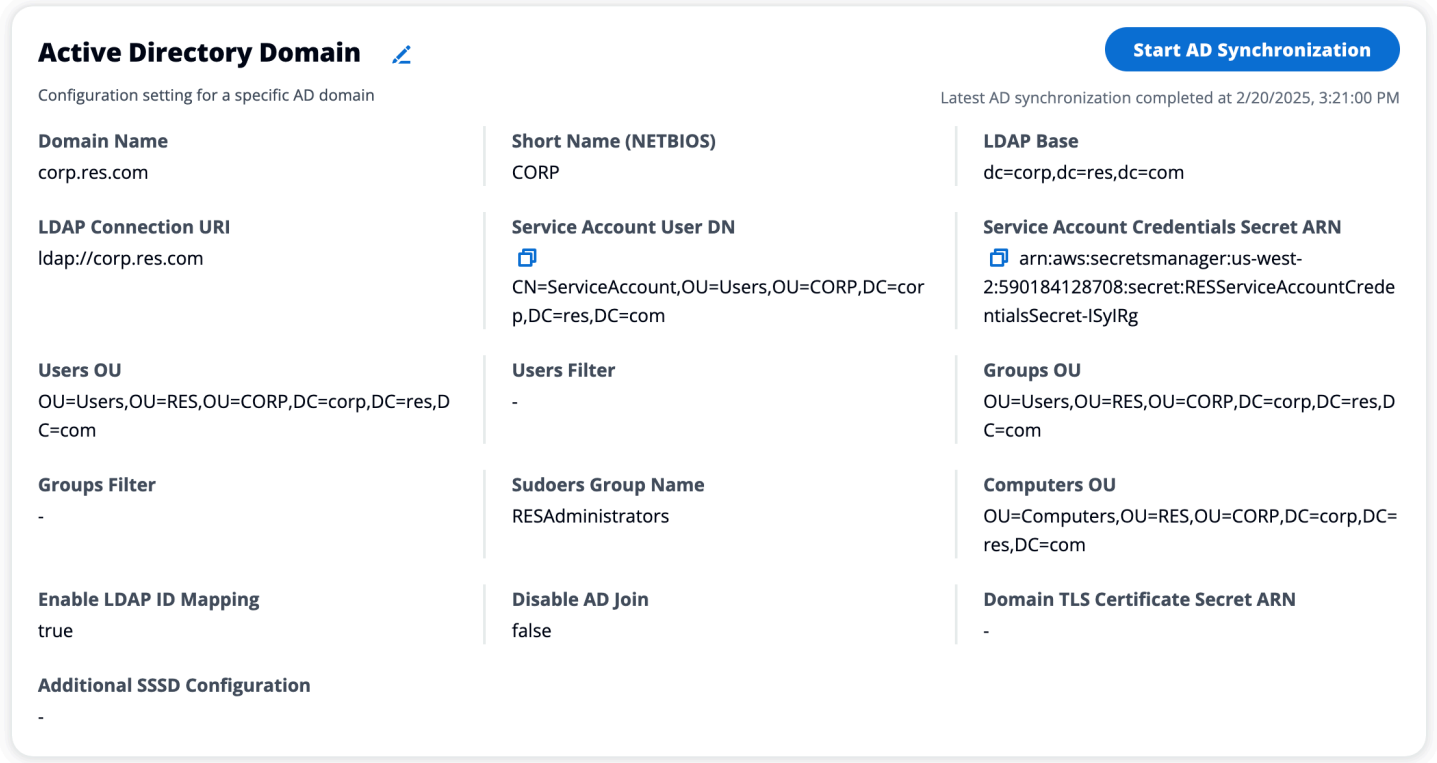
Accédez à la page Gestion des identités, puis cliquez sur le bouton Démarrer la synchronisation AD dans le conteneur de domaine Active Directory pour déclencher une synchronisation AD à la demande.



Pour arrêter une synchronisation AD en cours, sélectionnez le bouton Arrêter la synchronisation AD dans le conteneur de domaine Active Directory.



Vous pouvez également vérifier l'état de synchronisation AD et l'heure de synchronisation la plus récente dans le conteneur de domaine Active Directory.



Comment exécuter manuellement la synchronisation (versions 2024.12 et 2024.12.01)

Le processus de synchronisation Active Directory a été transféré de l'hôte infrarouge de Cluster Manager à une tâche unique d'Amazon Elastic Container Service (ECS) en arrière-plan. Le processus est planifié pour s'exécuter toutes les heures et vous pouvez trouver une tâche ECS en cours d'exécution dans la console Amazon ECS sous le `<res-environment-name>-ad-sync-cluster` cluster pendant qu'elle est en cours d'exécution.

Pour le lancer manuellement :

1. Accédez à la console Lambda et recherchez le lambda appelé. `<res-environment>-scheduled-ad-sync`
2. Ouvrez la fonction Lambda et accédez à Test
3. Dans le fichier Event JSON, entrez ce qui suit :

```
{
    "detail-type": "Scheduled Event"
}
```

4. Sélectionnez Tester).
5. Observez les journaux de la tâche AD Sync en cours d'exécution sous CloudWatch→ Groupes de journaux →`<environment-name>/ad-sync`. Vous verrez les journaux de chacune des tâches ECS en cours d'exécution. Sélectionnez le plus récent pour afficher les journaux.

> **Note**
>
> - Si vous modifiez les paramètres AD ou ajoutez des filtres AD, RES ajoutera les nouveaux utilisateurs en fonction des nouveaux paramètres spécifiés et supprimera les utilisateurs précédemment synchronisés et qui ne sont plus inclus dans l'espace de recherche LDAP.
> - RES ne peut pas supprimer un user/group élément activement affecté à un projet. Vous devez supprimer des utilisateurs des projets pour que RES les supprime de l'environnement.

Configuration SSO

Une fois la configuration AD fournie, les utilisateurs doivent configurer l'authentification unique (SSO) pour pouvoir se connecter au portail Web RES en tant qu'utilisateur AD. La configuration SSO a été déplacée de la page des paramètres généraux vers la nouvelle page de gestion des identités. Pour plus d'informations sur la configuration de l'authentification unique, consultezGestion des identités.

Configuration de l'authentification unique (SSO) avec IAM Identity Center

Si aucun centre d'identité n'est déjà connecté à l'Active Directory géré, commencez parÉtape 1 : configurer un centre d'identité. Si vous avez déjà un centre d'identité connecté à l'Active Directory géré, commencez parÉtape 2 : Se connecter à un centre d'identité.

> **Note**
>
> Si vous effectuez un déploiement dans la région AWS GovCloud (ouest des États-Unis), configurez le SSO dans le compte de AWS GovCloud (US) partition sur lequel vous avez déployé Research and Engineering Studio.

Étape 1 : configurer un centre d'identité

Activation du centre d'identité IAM

1. Connectez-vous à la console Gestion des identités et des accès AWS.
2. Ouvrez le Identity Center.
3. Sélectionnez Activer.
4. Choisissez Activer avec AWS Organizations.
5. Sélectionnez Continuer.

> **Note**
>
> Assurez-vous que vous vous trouvez dans la même région que celle dans laquelle vous gérez Active Directory.

Connexion d'IAM Identity Center à un Active Directory géré

Après avoir activé IAM Identity Center, suivez les étapes de configuration recommandées ci-dessous :

1. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
2. Sous Source d'identité, choisissez Actions, puis Modifier la source d'identité.
3. Sous Répertoires existants, sélectionnez votre répertoire.
4. Choisissez Suivant.
5. Passez en revue vos modifications et entrez **`ACCEPT`** dans le champ de confirmation.
6. Choisissez Modifier la source d'identité.

Synchronisation des utilisateurs et des groupes avec le centre d'identité

Une fois les modifications Connexion d'IAM Identity Center à un Active Directory géré effectuées, une bannière de confirmation verte apparaît.

1. Dans le bandeau de confirmation, sélectionnez Démarrer la configuration guidée.
2. Dans Configurer les mappages d'attributs, choisissez Next.

3. Dans la section Utilisateur, entrez les utilisateurs que vous souhaitez synchroniser.
4. Choisissez Ajouter.
5. Choisissez Suivant.
6. Passez en revue vos modifications, puis choisissez Enregistrer la configuration.
7. Le processus de synchronisation peut prendre quelques minutes. Si vous recevez un message d'avertissement indiquant que les utilisateurs ne se synchronisent pas, choisissez Reprendre la synchronisation.

Activation des utilisateurs

1. Dans le menu, sélectionnez Utilisateurs.
2. Sélectionnez le ou les utilisateurs auxquels vous souhaitez autoriser l'accès.
3. Choisissez Activer l'accès utilisateur.

Étape 2 : Se connecter à un centre d'identité

Configuration de l'application dans IAM Identity Center

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez Add application (Ajouter une application).
4. Dans les préférences de configuration, choisissez J'ai une application que je souhaite configurer.
5. Sous Type d'application, choisissez SAML 2.0.
6. Choisissez Suivant.
7. Entrez le nom d'affichage et la description que vous souhaitez utiliser.
8. Sous métadonnées IAM Identity Center, copiez le lien vers le fichier de métadonnées SAML IAM Identity Center. Vous en aurez besoin lors de la configuration d'IAM Identity Center avec le portail RES.
9. Sous Propriétés de l'application, entrez l'URL de démarrage de votre application. Par exemple, `<your-portal-domain>/sso`.
10. Sous URL ACS de l'application, entrez l'URL de redirection depuis le portail RES. Pour le trouver :

a. Sous Gestion de l'environnement, sélectionnez Paramètres généraux.
b. Sélectionnez l'onglet Fournisseur d'identité.
c. Sous Single Sign-On, vous trouverez l'URL de redirection SAML.

11. Sous Audience SAML de l'application, entrez l'URN Amazon Cognito.

    Pour créer l'urne :

    a. Depuis le portail RES, ouvrez les paramètres généraux.
    b. Sous l'onglet Fournisseur d'identité, recherchez l'ID du groupe d'utilisateurs.
    c. Ajoutez l'ID du groupe d'utilisateurs à cette chaîne :

    ```
    urn:amazon:cognito:sp:<user_pool_id>
    ```

12. Après avoir saisi l'URN Amazon Cognito, choisissez Soumettre.

Configuration des mappages d'attributs pour l'application

1. Dans le Identity Center, ouvrez les informations relatives à l'application que vous avez créée.
2. Choisissez Actions, puis Modifier les mappages d'attributs.
3. Dans le champ Objet, entrez**`${user:email}`**.
4. Sous Format, choisissez EmailAddress.
5. Choisissez Ajouter un nouveau mappage d'attributs.
6. Sous Attribut utilisateur dans l'application, entrez « e-mail ».
7. Sous Correspond à cette valeur de chaîne ou à cet attribut utilisateur dans IAM Identity Center, entrez**`${user:email}`**.
8. Dans Format, saisissez « non spécifié ».
9. Sélectionnez Enregistrer les modifications.

Ajouter des utilisateurs à l'application dans IAM Identity Center

1. Dans le Identity Center, ouvrez Utilisateurs assignés pour l'application que vous avez créée et choisissez Attribuer des utilisateurs.
2. Sélectionnez les utilisateurs auxquels vous souhaitez attribuer l'accès à l'application.
3. Choisissez Assign users (Affecter des utilisateurs).

Configuration de l'IAM Identity Center dans l'environnement RES

1. Dans l'environnement du studio de recherche et d'ingénierie, sous Gestion de l'environnement, ouvrez les paramètres généraux.
2. Ouvrez l'onglet Fournisseur d'identité.
3. Sous Authentification unique, choisissez Modifier (à côté de Statut).
4. Complétez le formulaire avec les informations suivantes :
   a. Choisissez SAML.
   b. Sous Nom du fournisseur, entrez un nom convivial.
   c. Choisissez Entrer l'URL du point de terminaison du document de métadonnées.
   d. Entrez l'URL que vous avez copiée lors de la copieConfiguration de l'application dans IAM Identity Center.
   e. Sous Attribut e-mail du fournisseur, entrez « e-mail ».
   f. Sélectionnez Soumettre.
5. Actualisez la page et vérifiez que le statut s'affiche comme activé.

Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)

Research and Engineering Studio s'intègre à n'importe quel fournisseur d'identité SAML 2.0 pour authentifier l'accès des utilisateurs au portail RES. Ces étapes indiquent comment intégrer le fournisseur d'identité SAML 2.0 que vous avez choisi. Si vous avez l'intention d'utiliser IAM Identity Center, consultezConfiguration de l'authentification unique (SSO) avec IAM Identity Center.

> **Note**
>
> L'adresse e-mail de l'utilisateur doit correspondre dans l'assertion SAML de l'IDP et dans Active Directory. Vous devrez connecter votre fournisseur d'identité à votre Active Directory et synchroniser régulièrement les utilisateurs.

Rubriques

- Configurez votre fournisseur d'identité
- Configurez RES pour utiliser votre fournisseur d'identité

- Configuration de votre fournisseur d'identité dans un environnement hors production
- Débogage des problèmes liés à l'IdP SAML

Configurez votre fournisseur d'identité

Cette section décrit les étapes à suivre pour configurer votre fournisseur d'identité avec les informations du groupe d'utilisateurs RES Amazon Cognito.

1. RES suppose que vous disposez d'un AD (AWS Managed AD ou AD auto-provisionné) avec les identités d'utilisateur autorisées à accéder au portail et aux projets RES. Connectez votre AD à votre fournisseur de services d'identité et synchronisez les identités des utilisateurs. Consultez la documentation de votre fournisseur d'identité pour savoir comment connecter votre AD et synchroniser les identités des utilisateurs. Par exemple, consultez la section Utilisation d'Active Directory comme source d'identité dans le Guide de AWS IAM Identity Center l'utilisateur.
2. Configurez une application SAML 2.0 pour RES dans votre fournisseur d'identité (IdP). Cette configuration nécessite les paramètres suivants :
   - URL de redirection SAML : URL utilisée par votre IdP pour envoyer la réponse SAML 2.0 au fournisseur de services.

     > **Note**
     >
     > En fonction de l'IdP, l'URL de redirection SAML peut porter un nom différent :
     >
     > - URL de l'application
     > - URL du service Assertion Consumer (ACS)
     > - URL de liaison ACS POST

     Pour obtenir l'URL

     1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
     2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
     3. Choisissez l'URL de redirection SAML.

- URI d'audience SAML : ID unique de l'entité d'audience SAML du côté du fournisseur de services.

  > **Note**
  >
  > En fonction de l'IdP, l'URI d'audience SAML peut porter un nom différent :
  >
  > - ClientID
  > - Audience SAML de l'application
  > - ID de l'entité SP

  Fournissez l'entrée dans le format suivant.

  ```
  urn:amazon:cognito:sp:user-pool-id
  ```

  Pour trouver l'URI de votre audience SAML

  1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
  2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
  3. Choisissez User Pool Id.

3. L'assertion SAML publiée sur RES doit être fields/claims définie comme suit sur l'adresse e-mail de l'utilisateur :
   - Sujet ou NameID SAML
   - Courrier électronique SAML
4. Votre IdP ajoute des éléments fields/claims à l'assertion SAML, en fonction de la configuration. RES nécessite ces champs. La plupart des fournisseurs remplissent automatiquement ces champs par défaut. Reportez-vous aux entrées et valeurs de champ suivantes si vous devez les configurer.

   - AudienceRestriction— Réglé sur`urn:amazon:cognito:sp:user-pool-id`. *user-pool-id*Remplacez-le par l'ID de votre groupe d'utilisateurs Amazon Cognito.

     ```
     <saml:AudienceRestriction>
         <saml:Audience> urn:amazon:cognito:sp:user-pool-id
     </saml:AudienceRestriction>
     ```

- Réponse — Réglé `InResponseTo` sur`https://user-pool-domain/saml2/idpresponse`. *`user-pool-domain`*Remplacez-le par le nom de domaine de votre groupe d'utilisateurs Amazon Cognito.

```
<saml2p:Response
  Destination="http://user-pool-domain/saml2/idpresponse"
  ID="id123"
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  IssueInstant="Date-time stamp"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

- SubjectConfirmationData— Réglé sur `Recipient` le point de `saml2/idpresponse` terminaison de votre groupe d'utilisateurs et `InResponseTo` sur l'ID de demande SAML d'origine.

```
<saml2:SubjectConfirmationData
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  NotOnOrAfter="Date-time stamp"
  Recipient="https://user-pool-domain/saml2/idpresponse"/>
```

- AuthnStatement— Configurez comme suit :

```
<saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
  SessionIndex="32413b2e54db89c764fb96ya2k"
 SessionNotOnOrAfter="2016-10-30T13:13:28">
    <saml2:SubjectLocality />
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
```

5. Si votre application SAML possède un champ URL de déconnexion, définissez-le sur :. *`<domain-url>`*`/saml2/logout`

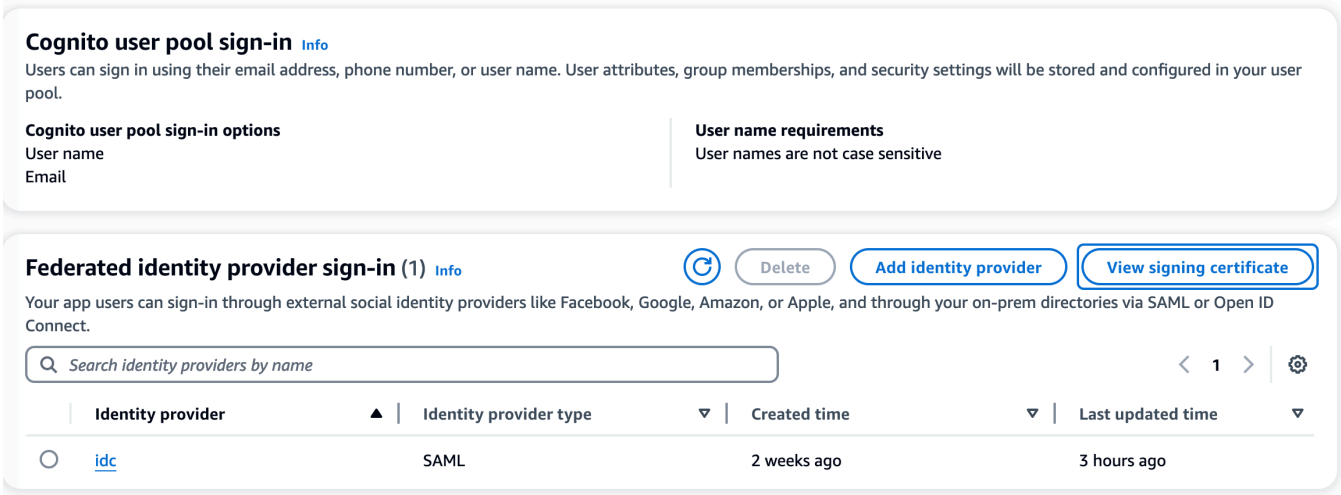
Pour obtenir l'URL du domaine

1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
3. Choisissez l'URL du domaine.

6. Si votre IdP accepte un certificat de signature afin d'établir un lien de confiance avec Amazon Cognito, téléchargez le certificat de signature Amazon Cognito et chargez-le dans votre IdP.

Pour obtenir le certificat de signature

1. Ouvrez la console Amazon Cognito dans la section Getting Started with AWS Management Console
2. Sélectionnez votre groupe d'utilisateurs. Votre groupe d'utilisateurs doit être`res-<environment name>-user-pool`.
3. Sélectionnez l'onglet Expérience de connexion.
4. Dans la section Connexion au fournisseur d'identité fédéré, choisissez Afficher le certificat de signature.



Vous pouvez utiliser ce certificat pour configurer Active Directory IDP, en ajouter un `relying party trust` et activer le support SAML sur cette partie utilisatrice.

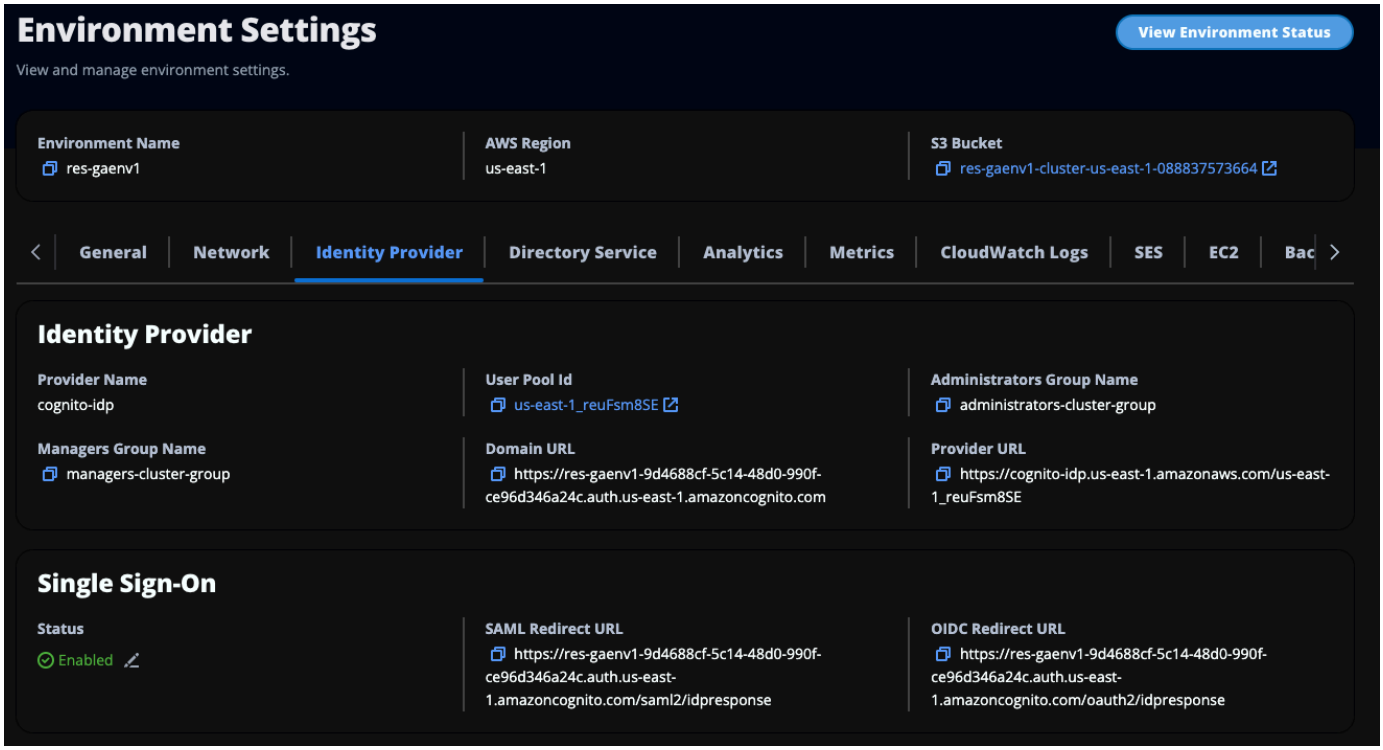
> **Note**
>
> Cela ne s'applique pas à Keycloak et IDC.

5. Une fois la configuration de l'application terminée, téléchargez le XML ou l'URL des métadonnées de l'application SAML 2.0. Vous l'utiliserez dans la section suivante.

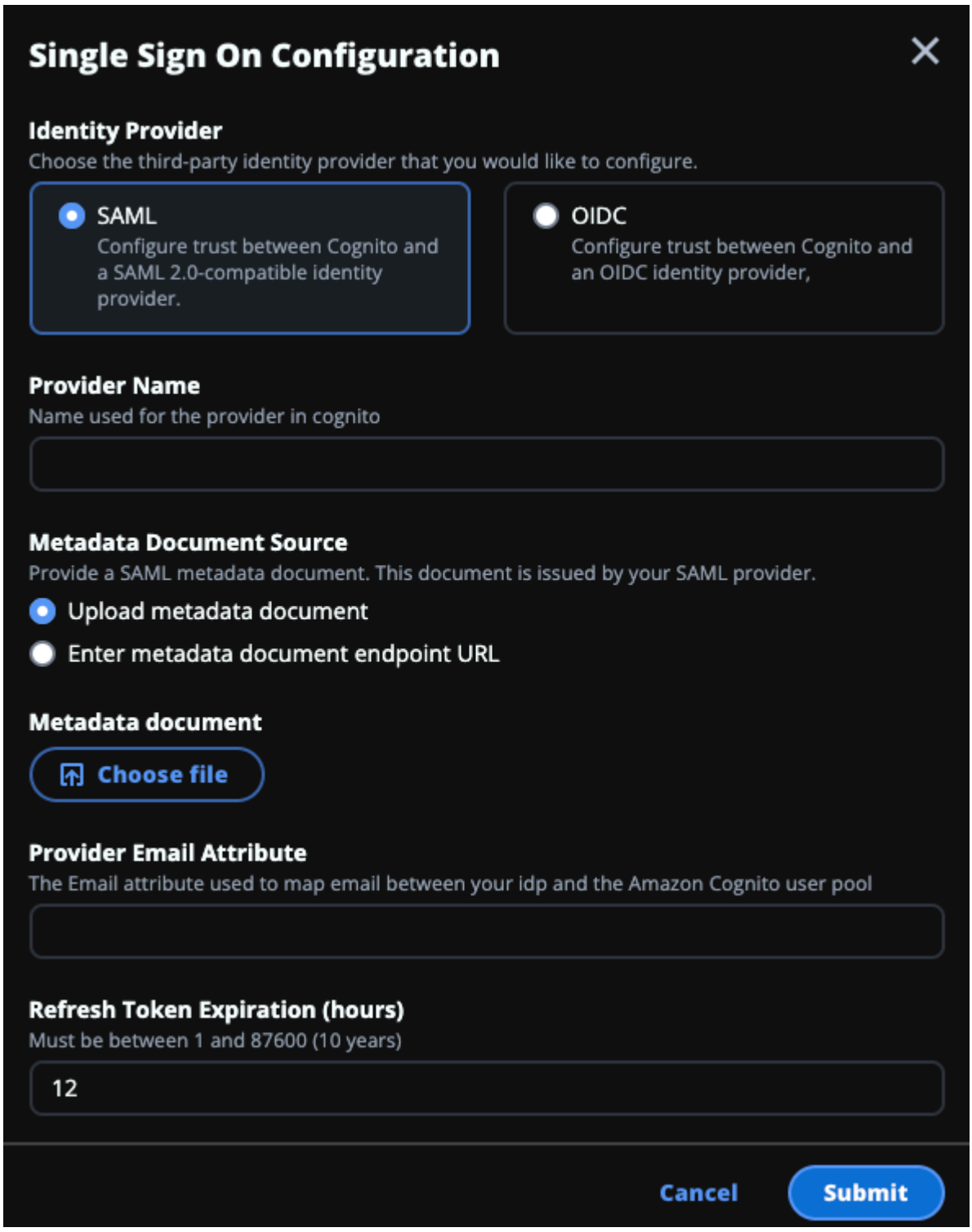
Configurez RES pour utiliser votre fournisseur d'identité

Pour terminer la configuration de l'authentification unique pour RES

1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.



3. Sous Single Sign-On, cliquez sur l'icône de modification à côté de l'indicateur d'état pour ouvrir la page de configuration de Single Sign-On.



a. Pour le fournisseur d'identité, choisissez SAML.

b. Dans Nom du fournisseur, entrez un nom unique pour votre fournisseur d'identité.

> **Note**
>
> Les noms suivants ne sont pas autorisés :
>
> - Cognito
> - IdentityCenter

c. Sous Source du document de métadonnées, choisissez l'option appropriée et téléchargez le document XML de métadonnées ou fournissez l'URL du fournisseur d'identité.

d. Pour Attribut e-mail du fournisseur, entrez la valeur du texte`email`.

e. Sélectionnez Soumettre.

4. Rechargez la page des paramètres d'environnement. L'authentification unique est activée si la configuration est correcte.

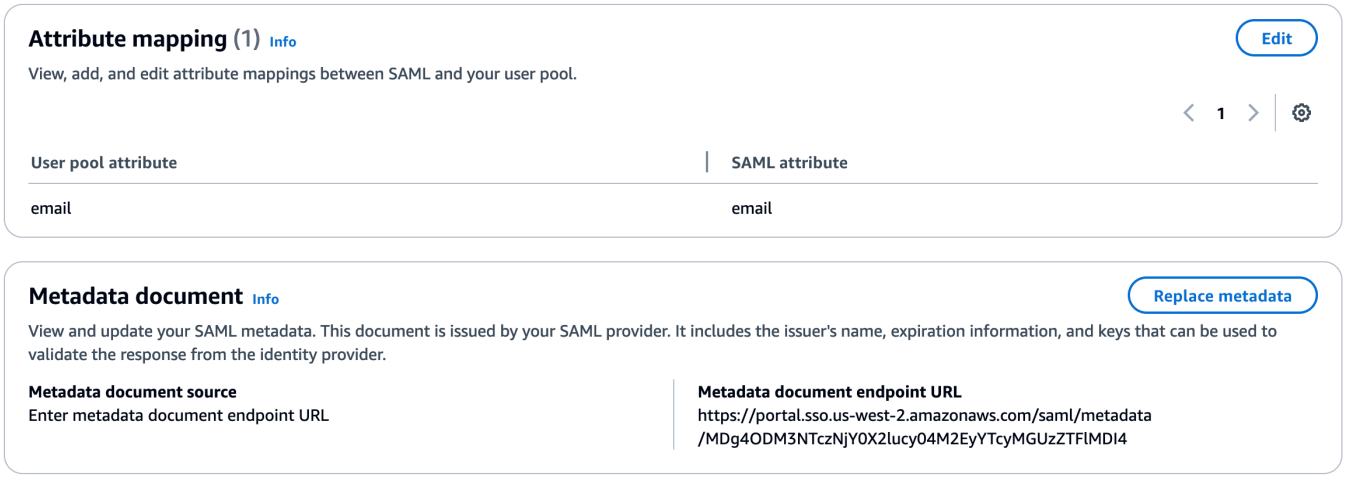
Configuration de votre fournisseur d'identité dans un environnement hors production

Si vous avez utilisé les ressources externes fournies pour créer un environnement RES hors production et que vous avez configuré IAM Identity Center comme fournisseur d'identité, vous souhaiterez peut-être configurer un autre fournisseur d'identité tel qu'Okta. Le formulaire d'activation de RES SSO demande trois paramètres de configuration :

1. Nom du fournisseur : ne peut pas être modifié
2. Document de métadonnées ou URL — Peut être modifié
3. Attribut e-mail du fournisseur — Peut être modifié

Pour modifier le document de métadonnées et l'attribut e-mail du fournisseur, procédez comme suit :

1. Accédez à la console Amazon Cognito.
2. Dans le menu de navigation, sélectionnez Groupes d'utilisateurs.
3. Sélectionnez votre groupe d'utilisateurs pour afficher l'aperçu du groupe d'utilisateurs.
4. Dans l'onglet Expérience de connexion, accédez à Connexion au fournisseur d'identité fédéré et ouvrez votre fournisseur d'identité configuré.
5. En règle générale, il vous suffit de modifier les métadonnées et de laisser le mappage des attributs inchangé. Pour mettre à jour le mappage des attributs, choisissez Modifier. Pour mettre à jour le document de métadonnées, choisissez Remplacer les métadonnées.



6. Si vous avez modifié le mappage des attributs, vous devez mettre à jour la `<environment name>.cluster-settings` table dans DynamoDB.

   a. Ouvrez la console DynamoDB et choisissez Tables dans le menu de navigation.

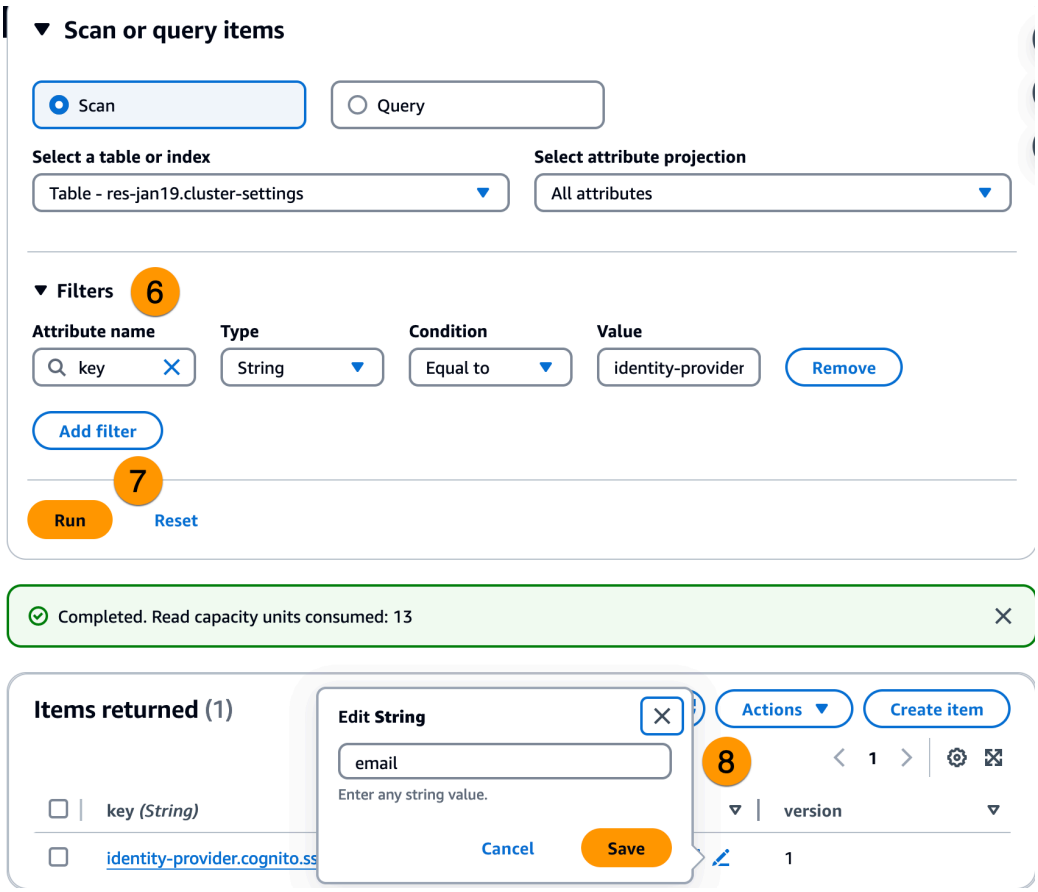
   b. Recherchez et sélectionnez le `<environment name>.cluster-settings` tableau, puis dans le menu Actions, sélectionnez Explorer les éléments.

   c. Sous Numériser ou interroger des éléments, accédez à Filtres et entrez les paramètres suivants :

      - Nom de l'attribut — `key`
      - Valeur — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Cliquez sur Exécuter.

7. Sous Articles renvoyés, recherchez la `identity-provider.cognito.sso_idp_provider_email_attribute` chaîne et choisissez Modifier pour modifier la chaîne en fonction de vos modifications dans Amazon Cognito.



Débogage des problèmes liés à l'IdP SAML

Traceur SAML — Vous pouvez utiliser cette extension pour le navigateur Chrome afin de suivre les requêtes SAML et de vérifier les valeurs d'assertion SAML. Pour plus d'informations, consultez SAML-Tracer sur le Chrome Web Store.

Outils de développement SAML : OneLogin fournit des outils que vous pouvez utiliser pour décoder la valeur codée SAML et vérifier les champs obligatoires dans l'assertion SAML. Pour plus d'informations, voir Base 64 Decode + Inflate sur le OneLogin site Web.

Amazon CloudWatch Logs — Vous pouvez vérifier la présence d'erreurs ou d'avertissements dans vos CloudWatch journaux RES dans Logs. Vos journaux se trouvent dans un groupe de journaux au format de nom`res-environment-name`/`cluster-manager`.

Documentation Amazon Cognito — Pour plus d'informations sur l'intégration de SAML à Amazon Cognito, consultez la section Ajouter des fournisseurs d'identité SAML à un groupe d'utilisateurs dans le manuel Amazon Cognito Developer Guide.

Définition de mots de passe pour les utilisateurs

1. Dans la Directory Service console, sélectionnez le répertoire de la pile créée.
2. Dans le menu Actions, sélectionnez Réinitialiser le mot de passe utilisateur.
3. Sélectionnez l'utilisateur et entrez un nouveau mot de passe.
4. Choisissez Réinitialiser le mot de passe.

Création de sous-domaines

Si vous utilisez un domaine personnalisé, vous devez configurer des sous-domaines pour prendre en charge les parties Web et VDI de votre portail.

> **Note**
>
> Si vous effectuez un déploiement dans la région AWS GovCloud (ouest des États-Unis), configurez l'application Web et les sous-domaines VDI dans le compte de partition commerciale hébergeant la zone hébergée publique du domaine.

1. Ouvrez la console Route 53.
2. Recherchez le domaine que vous avez créé et choisissez Créer un enregistrement.
3. Entrez « web » comme nom de l'enregistrement.
4. Sélectionnez CNAME comme type d'enregistrement.
5. Dans Value, saisissez le lien que vous avez reçu dans l'e-mail initial.
6. Choisissez Créer des enregistrements.
7. Pour créer un enregistrement pour le VDC, récupérez l'adresse NLB.
    a. Ouvrez la AWS CloudFormation console.
    b. Sélectionnez `<environment-name>-vdc`.
    c. Choisissez Ressources et ouvrez`<environmentname>-vdc-external-nlb`.
    d. Copiez le nom DNS depuis le NLB.
8. Ouvrez la console Route 53.
9. Trouvez votre domaine et choisissez Créer un enregistrement.
10. Sous Nom de l'enregistrement, entrez`vdc`.

11. Sous Record type (Type d'enregistrement), sélectionnez CNAME.
12. Pour le NLB, entrez le DNS.
13. Choisissez Créer un registre.

Création d'un certificat ACM

Par défaut, RES héberge le portail Web sous un équilibreur de charge d'application utilisant le domaine amazonaws.com. Pour utiliser votre propre domaine, vous devez configurer un SSL/TLS certificat public que vous avez fourni ou demandé à AWS Certificate Manager (ACM). Si vous utilisez ACM, vous recevrez un nom de AWS ressource que vous devrez fournir en paramètre pour chiffrer le SSL/TLS canal entre le client et l'hôte des services Web.

> **Tip**
>
> Si vous déployez le package de démonstration des ressources externes, vous devrez saisir le domaine de votre choix `PortalDomainName` lors du déploiement de la pile de ressources externesCréation de ressources externes.

Pour créer un certificat pour des domaines personnalisés :

1. Depuis la console, ouvrez AWS Certificate Managerpour demander un certificat public. Si vous déployez dans AWS GovCloud l'ouest des États-Unis, créez le certificat dans votre compte de GovCloud partition.
2. Choisissez Demander un certificat public, puis cliquez sur Suivant.
3. Sous Noms de domaine, demandez un certificat pour les deux `*.PortalDomainName` et`PortalDomainName`.
4. Sous Méthode de validation, choisissez Validation DNS.
5. Cliquez sur Demander.
6. Dans la liste des certificats, ouvrez les certificats demandés. Chaque certificat aura le statut En attente de validation.

   > **Note**
   >
   > Si vous ne voyez pas vos certificats, actualisez la liste.

7. Effectuez l'une des actions suivantes :
   - Déploiement commercial :

     Dans les détails du certificat pour chaque certificat demandé, choisissez Create records in Route 53. Le statut du certificat doit passer à Émis.
   - GovCloud déploiement :

     Si vous déployez dans AWS GovCloud (ouest des États-Unis), copiez la clé et la valeur CNAME. À partir du compte de partition commerciale, utilisez les valeurs pour créer un nouvel enregistrement dans la zone hébergée publique. Le statut du certificat doit passer à Émis.
8. Copiez le nouvel ARN du certificat à saisir en tant que paramètre pour`ACMCertificateARNforWebApp`.

Amazon CloudWatch Logs

Research and Engineering Studio crée les groupes de journaux suivants CloudWatch lors de l'installation. Consultez le tableau suivant pour les rétentions par défaut :

CloudWatch Groupes de journaux	Retention
`/aws/lambda/ <installation-stack-name>-cluster-endpoints`	N'expire jamais
`/aws/lambda/ <installation-stack-name>-cluster-manager-scheduled-ad-sync`	N'expire jamais
`/aws/lambda/ <installation-stack-name>-cluster-settings`	N'expire jamais
`/aws/lambda/ <installation-stack-name>-oauth-credentials`	N'expire jamais
`/aws/lambda/ <installation-stack-name>-self-signed-certificate`	N'expire jamais

CloudWatch Groupes de journaux	Retention
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	N'expire jamais
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	N'expire jamais
/aws/lambda/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope	N'expire jamais
/*<installation-stack-name>* /cluster-manager	3 mois
/*<installation-stack-name>* /vdc/controller	3 mois
/*<installation-stack-name>* /vdc/dcv-broker	3 mois
/*<installation-stack-name>* /vdc/dcv-connection-gateway	3 mois

Si vous souhaitez modifier la rétention par défaut d'un groupe de journaux, vous pouvez accéder à la CloudWatch console et suivre les instructions de la section Modifier la conservation des données des CloudWatch journaux dans les journaux.

Définition de limites d'autorisation personnalisées

À partir du 2024.04, vous pouvez éventuellement modifier les rôles créés par RES en attachant des limites d'autorisation personnalisées. Une limite d'autorisation personnalisée peut être définie dans le cadre de l' CloudFormation installation RES en fournissant l'ARN de la limite d'autorisation dans le cadre du paramètre IAMPermission Boundary. Aucune limite d'autorisation n'est définie pour les rôles RES si ce paramètre est laissé vide. Vous trouverez ci-dessous la liste des actions dont les rôles RES ont besoin pour fonctionner. Assurez-vous que toute limite d'autorisation que vous prévoyez d'utiliser explicitement autorise les actions suivantes :

```
[
    {
        "Effect": "Allow",
        "Resource": "*",
        "Sid": "ResRequiredActions",
        "Action": [
            "access-analyzer:*",
            "account:GetAccountInformation",
            "account:ListRegions",
            "acm:*",
            "airflow:*",
            "amplify:*",
            "amplifybackend:*",
            "amplifyuibuilder:*",
            "aoss:*",
            "apigateway:*",
            "appflow:*",
            "application-autoscaling:*",
            "appmesh:*",
            "apprunner:*",
            "aps:*",
            "athena:*",
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
```

```
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
            "ecr:*",
            "ecs:*",
            "eks:*",
            "elastic-inference:*",
            "elasticache:*",
            "elasticbeanstalk:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "elasticmapreduce:*",
            "elastictranscoder:*",
            "es:*",
            "events:*",
            "firehose:*",
            "fis:*",
            "fms:*",
            "forecast:*",
            "fsx:*",
            "geo:*",
            "glacier:*",
            "glue:*",
            "grafana:*",
```

```
            "guardduty:*",
            "health:*",
            "iam:*",
            "identitystore:*",
            "imagebuilder:*",
            "inspector2:*",
            "inspector:*",
            "internetmonitor:*",
            "iot:*",
            "iotanalytics:*",
            "kafka:*",
            "kafkaconnect:*",
            "kinesis:*",
            "kinesisanalytics:*",
            "kms:*",
            "lambda:*",
            "lightsail:*",
            "logs:*",
            "memorydb:*",
            "mgh:*",
            "mobiletargeting:*",
            "mq:*",
            "neptune-db:*",
            "organizations:DescribeOrganization",
            "osis:*",
            "personalize:*",
            "pi:*",
            "pipes:*",
            "polly:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
            "resource-groups:*",
            "route53:*",
            "route53domains:*",
            "route53resolver:*",
            "rum:*",
            "s3:*",
```

```
            "sagemaker:*",
            "scheduler:*",
            "schemas:*",
            "sdb:*",
            "secretsmanager:*",
            "securityhub:*",
            "serverlessrepo:*",
            "servicecatalog:*",
            "servicequotas:*",
            "ses:*",
            "signer:*",
            "sns:*",
            "sqs:*",
            "ssm:*",
            "ssmmessages:*",
            "states:*",
            "storagegateway:*",
            "sts:*",
            "support:*",
            "tag:GetResources",
            "tag:GetTagKeys",
            "tag:GetTagValues",
            "textract:*",
            "timestream:*",
            "transcribe:*",
            "transfer:*",
            "translate:*",
            "vpc-lattice:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*",
            "wisdom:*",
            "xray:*"
        ]
    }
]
```

Configurez Res Ready AMIs

Grâce aux Amazon Machine Images (AMI) compatibles RES, vous pouvez préinstaller les dépendances RES pour les instances de bureau virtuel (VDI) sur vos AMI personnalisées.

L'utilisation d'AMI compatibles RES améliore les temps de démarrage des instances VDI à l'aide des images préconfigurées. À l'aide d'EC2 Image Builder, vous pouvez créer et enregistrer AMIs vos piles de logiciels en tant que nouvelles. Pour plus d'informations sur Image Builder, consultez le guide de l'utilisateur d'Image Builder.

Avant de commencer, vous devez déployer la dernière version de RES.

Rubriques

Préparer un rôle IAM pour accéder à l'environnement RES

Pour accéder au service d'environnement RES depuis EC2 Image Builder, vous devez créer ou modifier un rôle IAM appelé RES-. EC2 InstanceProfileForImageBuilder Pour plus d'informations sur la configuration d'un rôle IAM à utiliser dans Image Builder, consultez Gestion des identités et des accès AWS (IAM) dans le guide de l'utilisateur d'Image Builder.

Votre rôle nécessite :

- Des relations de confiance incluant le service Amazon EC2.
- Amazon SSMManaged InstanceCore et ses EC2 InstanceProfileForImageBuilder politiques.
- Une politique RES personnalisée avec un accès limité à DynamoDB et Amazon S3 à l'environnement RES déployé.

  (Cette politique peut être soit un document de politique géré par le client, soit un document de politique intégré au client.)

1. Commencez par créer une nouvelle politique qui sera attachée à votre rôle : IAM -> Politiques -> Créer une politique

2. Sélectionnez JSON dans l'éditeur de politiques.
3. Copiez et collez la politique affichée ici dans l'éditeur, en la *us-east-1* remplaçant par celle que vous souhaitez Région AWS, *111122223333* par votre identifiant de AWS compte et *{RES-EnvironmentName}* par votre RES le cas EnvironmentName échéant.

   Politique RES :

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:us-east-1:111122223333:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*",
                        "cluster-manager.host_modules.*",
                        "identity-provider.cognito.enable_native_user_login"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::{RES-EnvironmentName}-cluster-us-
east-1-111122223333/idea/vdc/res-ready-install-script-packages/*",
                "arn:aws:s3:::research-engineering-studio-us-east-1/
host_modules/*"
            ]
        }
    ]
```

```
}
```

4. Choisissez Next et fournissez un nom et une description facultative pour terminer la création de la politique.
5. Pour créer le rôle, commencez par accéder à IAM -> Rôles -> Créer un rôle.
6. Sous Type d'entité de confiance, sélectionnez « AWS service ».
7. Sélectionnez EC2 dans le menu déroulant Service ou cas d'utilisation.
8. Dans la section Cas d'utilisation, sélectionnez EC2, puis Next.
9. Recherchez puis sélectionnez le nom de la politique que vous avez créée précédemment.
10. Choisissez Next et fournissez un nom et une description facultative pour terminer la création du rôle.
11. Sélectionnez votre nouveau rôle et vérifiez que la relation de confiance correspond aux critères suivants :

    Entité relationnelle de confiance :

    JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Création d'un composant EC2 Image Builder

Suivez les instructions pour créer un composant à l'aide de la console Image Builder dans le guide de l'utilisateur d'Image Builder.

Entrez les détails de votre composant :

1. Dans Type, choisissez Build.
2. Pour le système d'exploitation Image (OS), choisissez Linux ou Windows.
3. Pour Nom du composant, entrez un nom significatif tel que**`research-and-engineering-studio-vdi-<operating-system>`**.
4. Entrez le numéro de version de votre composant et ajoutez éventuellement une description.
5. Pour le document de définition, entrez le fichier de définition suivant. Si vous rencontrez des erreurs, le fichier YAML est sensible à l'espace et en est la cause la plus probable.

   Linux

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-linux
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
```

```
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
```

```
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-windows
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
```

```
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
 res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
       - name: Reboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

6. Créez des balises facultatives et choisissez Créer un composant.

Préparez votre recette pour EC2 Image Builder

Une recette EC2 Image Builder définit l'image de base à utiliser comme point de départ pour créer une nouvelle image, ainsi que l'ensemble des composants que vous ajoutez pour personnaliser votre image et vérifier que tout fonctionne comme prévu. Vous devez créer ou modifier une recette pour construire l'AMI cible avec les dépendances logicielles RES nécessaires. Pour plus d'informations sur les recettes, voir Gérer les recettes.

RES prend en charge les systèmes d'exploitation d'image suivants :

- Amazon Linux 2 (x86 et ARM64)
- Ubuntu 22.04.3 (x86)
- RHEL 8 (x86) et 9 (x86)
- Windows Server 2019, 2022 (x86)
- Windows 10, 11 (x86)

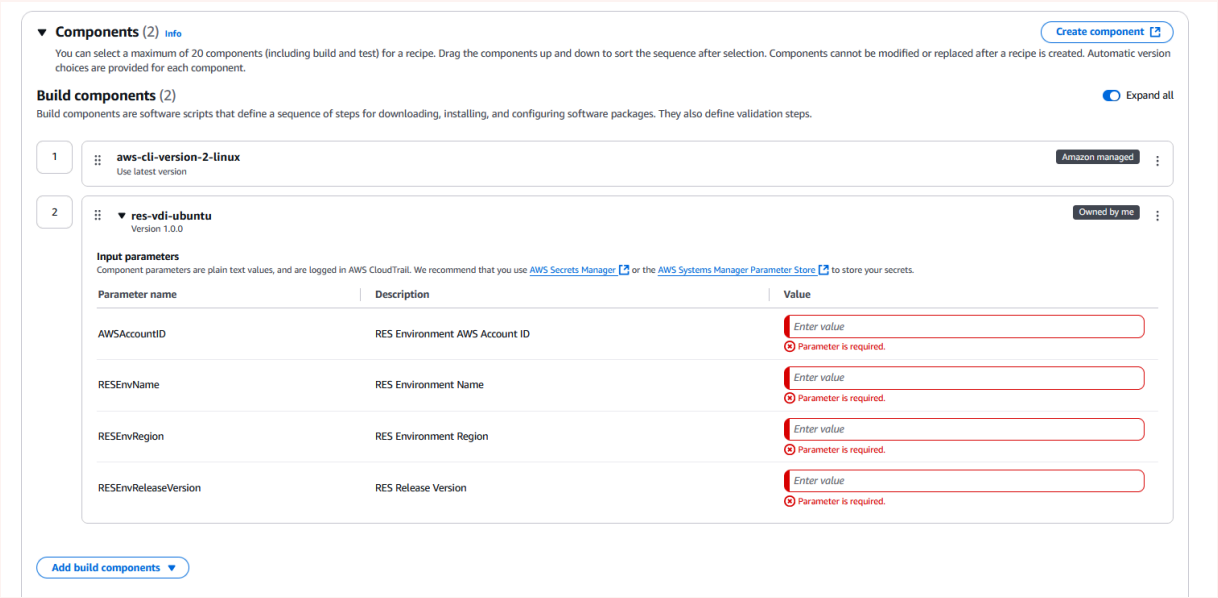
Create a new recipe

1. Ouvrez la console https://console.aws.amazon.com/imagebuilder EC2 Image Builder à l'adresse.
2. Sous Ressources enregistrées, choisissez Image recipes.
3. Choisissez Créer une recette d'image.
4. Entrez un nom unique et un numéro de version.
5. Sélectionnez une image de base prise en charge par RES.
6. Sous Configuration de l'instance, installez un agent SSM s'il n'en existe pas un préinstallé. Entrez les informations dans Données utilisateur et toute autre donnée utilisateur nécessaire.

> **Note**
>
> Pour plus d'informations sur l'installation d'un agent SSM, voir :
>
> - Installation manuelle de l'agent SSM sur les instances EC2 pour Linux.
> - Installation et désinstallation manuelles de l'agent SSM sur les instances EC2 pour Windows Server.

7. Pour les recettes basées sur Linux, ajoutez le composant de `aws-cli-version-2-linux` compilation géré par Amazon à la recette. Les scripts d'installation RES utilisent le AWS CLI pour fournir un accès VDI aux valeurs de configuration des paramètres du cluster DynamoDB. Windows n'a pas besoin de ce composant.
8. Ajoutez le composant EC2 Image Builder créé pour votre environnement Linux ou Windows et entrez les valeurs de paramètres requises. Les paramètres suivants sont obligatoires : AWSAccount ID, RESEnv Nom, RESEnv Région et RESEnvReleaseVersion.

> **Important**
>
> Pour les environnements Linux, vous devez ajouter ces composants afin que le composant de `aws-cli-version-2-linux` compilation soit ajouté en premier.



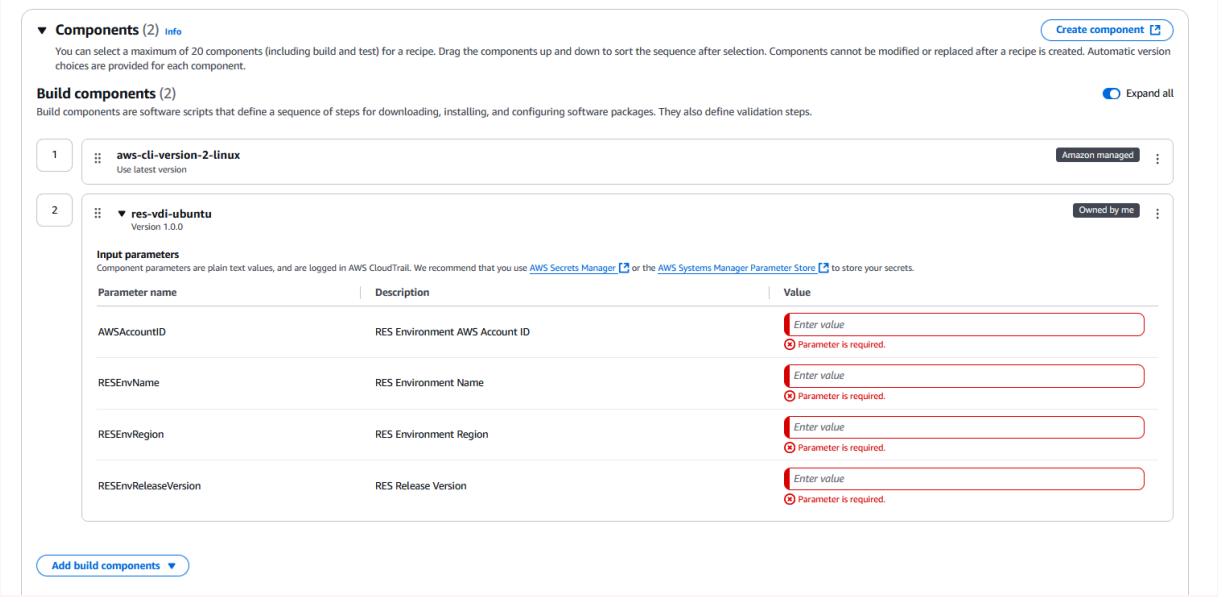
9. (Recommandé) Ajoutez le composant de `simple-boot-test-<linux-or-windows>` test géré par Amazon pour vérifier que l'AMI peut être lancée. Il s'agit d'une recommandation minimale. Vous pouvez sélectionner d'autres composants de test qui répondent à vos exigences.
10. Complétez les sections facultatives si nécessaire, ajoutez les autres composants souhaités et choisissez Créer une recette.

Modify a recipe

Si vous possédez déjà une recette EC2 Image Builder, vous pouvez l'utiliser en ajoutant les composants suivants :

1. Pour les recettes basées sur Linux, ajoutez le composant de `aws-cli-version-2-linux` compilation géré par Amazon à la recette. Les scripts d'installation RES utilisent le AWS CLI pour fournir un accès VDI aux valeurs de configuration des paramètres du cluster DynamoDB. Windows n'a pas besoin de ce composant.
2. Ajoutez le composant EC2 Image Builder créé pour votre environnement Linux ou Windows et entrez les valeurs de paramètres requises. Les paramètres suivants sont obligatoires : AWSAccount ID, RESEnv Nom, RESEnv Région et RESEnvReleaseVersion.

> **Important**
>
> Pour les environnements Linux, vous devez ajouter ces composants afin que le composant de `aws-cli-version-2-linux` compilation soit ajouté en premier.



3. Complétez les sections facultatives si nécessaire, ajoutez les autres composants souhaités et choisissez Créer une recette.

Configuration de l'infrastructure EC2 Image Builder

Vous pouvez utiliser les configurations d'infrastructure pour spécifier l'infrastructure Amazon EC2 qu'Image Builder utilise pour créer et tester votre image Image Builder. Pour une utilisation avec RES, vous pouvez choisir de créer une nouvelle configuration d'infrastructure ou d'utiliser une configuration existante.

- Pour créer une nouvelle configuration d'infrastructure, voir Création d'une configuration d'infrastructure.
- Pour utiliser une configuration d'infrastructure existante, mettez à jour une configuration d'infrastructure.

Pour configurer votre infrastructure Image Builder :

1. Pour le rôle IAM, entrez le rôle que vous avez configuré précédemment. Préparer un rôle IAM pour accéder à l'environnement RES
2. Pour le type d'instance, choisissez un type avec au moins 4 Go de mémoire et compatible avec l'architecture AMI de base que vous avez choisie. Consultez la section Types d'instances Amazon EC2.
3. Pour les VPC, les sous-réseaux et les groupes de sécurité, vous devez autoriser l'accès à Internet pour télécharger des packages logiciels. L'accès doit également être autorisé à la table `cluster-settings` DynamoDB et au compartiment de cluster Amazon S3 de l'environnement RES.

Configurer le pipeline d'images Image Builder

Le pipeline d'images Image Builder assemble l'image de base, les composants pour la création et les tests, la configuration de l'infrastructure et les paramètres de distribution. Pour configurer un pipeline d'images pour qu' AMIsil soit prêt pour RES, vous pouvez choisir de créer un nouveau pipeline ou d'utiliser un pipeline existant. Pour plus d'informations, consultez la section Création et mise à jour de pipelines d'images AMI dans le guide de l'utilisateur d'Image Builder.

Create a new Image Builder pipeline

1. Ouvrez la console Image Builder à l'adressehttps://console.aws.amazon.com/imagebuilder.
2. Dans le volet de navigation, choisissez Image pipelines.
3. Choisissez Créer un pipeline d'images.
4. Spécifiez les détails de votre pipeline en saisissant un nom unique, une description facultative, un calendrier et une fréquence.
5. Pour Choisir une recette, choisissez Utiliser une recette existante et sélectionnez la recette créée dansPréparez votre recette pour EC2 Image Builder. Vérifiez que les détails de votre recette sont corrects.

6. Pour Définir le processus de création d'image, choisissez le flux de travail par défaut ou personnalisé selon le cas d'utilisation. Dans la plupart des cas, les flux de travail par défaut sont suffisants. Pour plus d'informations, consultez Configurer les flux de travail d'imagerie pour votre pipeline EC2 Image Builder.
7. Pour Définir la configuration de l'infrastructure, choisissez Choisir la configuration d'infrastructure existante et sélectionnez la configuration d'infrastructure créée dansConfiguration de l'infrastructure EC2 Image Builder. Vérifiez que les détails de votre infrastructure sont corrects.
8. Pour Définir les paramètres de distribution, choisissez Créer les paramètres de distribution à l'aide des paramètres de distribution par défaut du service. L'image de sortie doit se trouver dans le même environnement RES Région AWS que celui de votre environnement RES. En utilisant les paramètres par défaut du service, l'image sera créée dans la région où Image Builder est utilisé.
9. Passez en revue les détails du pipeline et choisissez Create pipeline.

Modify an existing Image Builder pipeline

1. Pour utiliser un pipeline existant, modifiez les détails afin d'utiliser la recette créée dansPréparez votre recette pour EC2 Image Builder.
2. Sélectionnez Enregistrer les modifications.

Exécuter le pipeline d'images Image Builder

Pour produire l'image de sortie configurée, vous devez lancer le pipeline d'images. Le processus de création peut prendre jusqu'à une heure selon le nombre de composants contenus dans la recette d'image.

Pour exécuter le pipeline d'images :

1. Dans Pipelines d'images, sélectionnez le pipeline créé dansConfigurer le pipeline d'images Image Builder.
2. Dans Actions, sélectionnez Exécuter le pipeline.

Enregistrez une nouvelle pile logicielle dans RES

1. Suivez les instructions the section called “Piles de logiciels () AMIs” pour enregistrer une pile logicielle.
2. Pour l'ID AMI, entrez l'ID AMI de l'image de sortie intégréeExécuter le pipeline d'images Image Builder.

Guide de l'administrateur

Ce guide de l'administrateur fournit des instructions supplémentaires à un public technique sur la manière de personnaliser et d'intégrer davantage le studio de recherche et d'ingénierie sur le AWS produit.

Rubriques

Gestion des secrets

Le studio de recherche et d'ingénierie conserve les secrets suivants en utilisant AWS Secrets Manager. RES crée automatiquement des secrets lors de la création de l'environnement. Les secrets saisis par l'administrateur lors de la création de l'environnement sont saisis en tant que paramètres.

Nom du secret	Description	RES généré	Admin saisi
`<envname> -sso-client-secret`	Secret du OAuth2 client Single Sign-On pour l'environnement	✓	
`<envname> -vdc-client-secret`	vdc ClientSecret	✓	
`<envname> -vdc-client-id`	vdc ClientId	✓	
`<envname> -vdc-gateway-`	Certificat autosigné , clé privée pour le domaine	✓	

Nom du secret	Description	RES généré	Admin saisi
`certificate-private-key`			
<envname> `-vdc-gateway-certificate-certificate`	Certificat auto-signé pour le domaine	✓	
<envname> `-cluster-manager-client-secret`	gestionnaire de clusters ClientSecret	✓	
<envname> `-cluster-manager-client-id`	gestionnaire de clusters ClientId	✓	
<envname> `-external-private-key`	Certificat autosigné, clé privée pour le domaine	✓	
<envname> `-external-certificate`	Certificat auto-signé pour le domaine	✓	
<envname> `-internal-private-key`	Certificat autosigné, clé privée pour le domaine	✓	
<envname> `-internal-certificate`	Certificat auto-signé pour le domaine	✓	

Nom du secret	Description	RES généré	Admin saisi
<envname> -directoryservice-ServiceAccountUserDN	L'attribut Distinguished Name (DN) de l' ServiceAccount utilisateur.	✓	

Les valeurs ARN secrètes suivantes figurent dans le *<envname>*-cluster-settings tableau de DynamoDB :

Clé	Source
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	pile
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	pile
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	pile
directoryservice.root_username_secret_arn	
vdc.client_secret	pile
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	pile
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	pile
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	

Clé	Source
`cluster.load_balancers.external_alb.certificates.private_key_secret_arn`	pile
`cluster-manager.client_secret`	

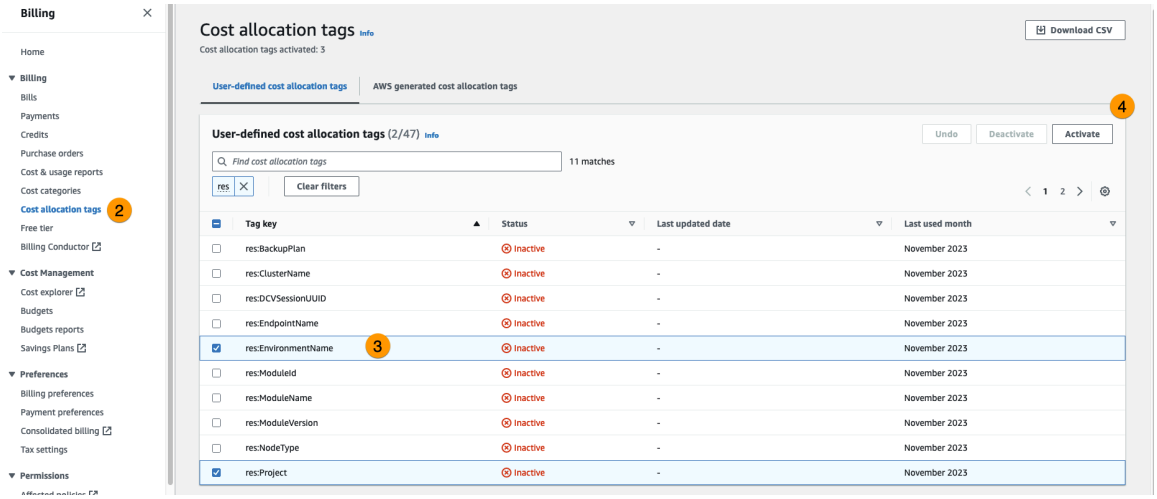
Surveillance et contrôle des coûts

> **Note**
>
> L'association de projets de studios de recherche et d'ingénierie à des projets n' AWS Budgets est pas prise en charge dans AWS GovCloud (US).

Nous vous recommandons de créer un budget via AWS Cost Explorer pour faciliter la gestion des coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chacun desthe section called "AWS services inclus dans ce produit".

Pour faciliter le suivi des coûts, vous pouvez associer des projets RES aux budgets créés dans ce cadre AWS Budgets. Vous devez d'abord activer les balises d'environnement dans les balises de répartition des coûts de facturation.

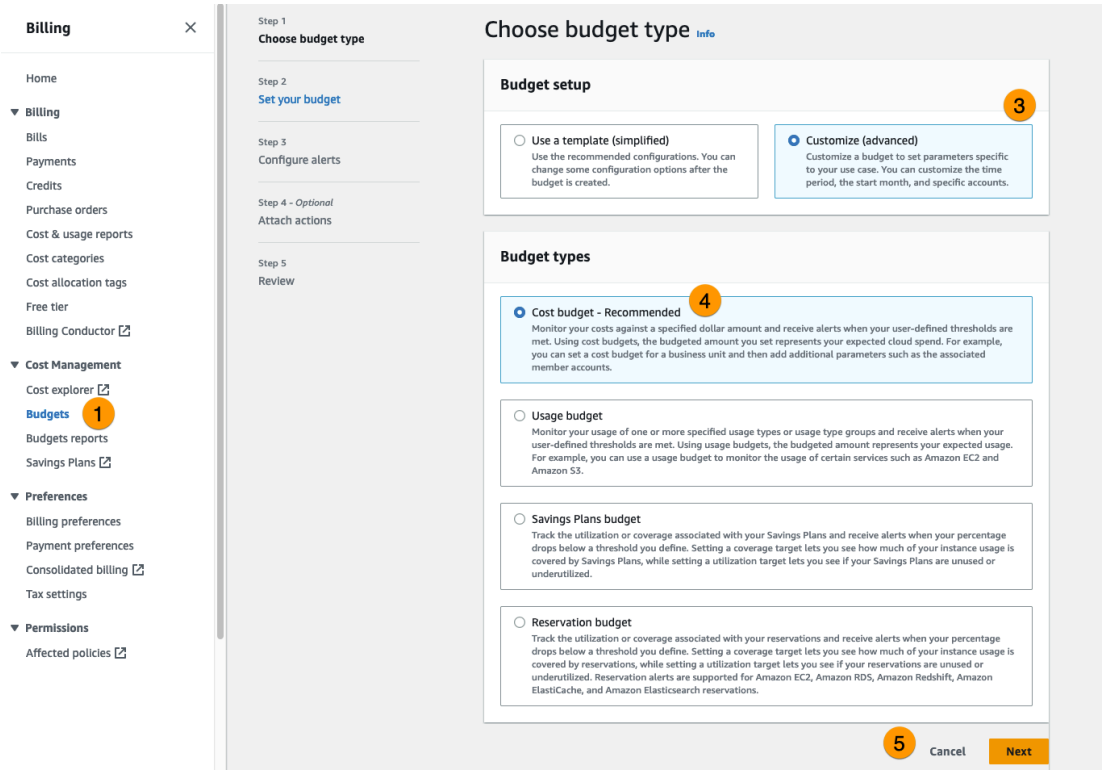
1. Connectez-vous à la AWS Billing and Cost Management console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/costmanagement/.
2. Choisissez les balises de répartition des coûts.
3. Recherchez et sélectionnez les `res:EnvironmentName` balises `res:Project` et.
4. Choisissez Activer.



> **Note**
>
> L'affichage des balises RES après le déploiement peut prendre jusqu'à un jour.

Pour créer un budget pour les ressources RES :

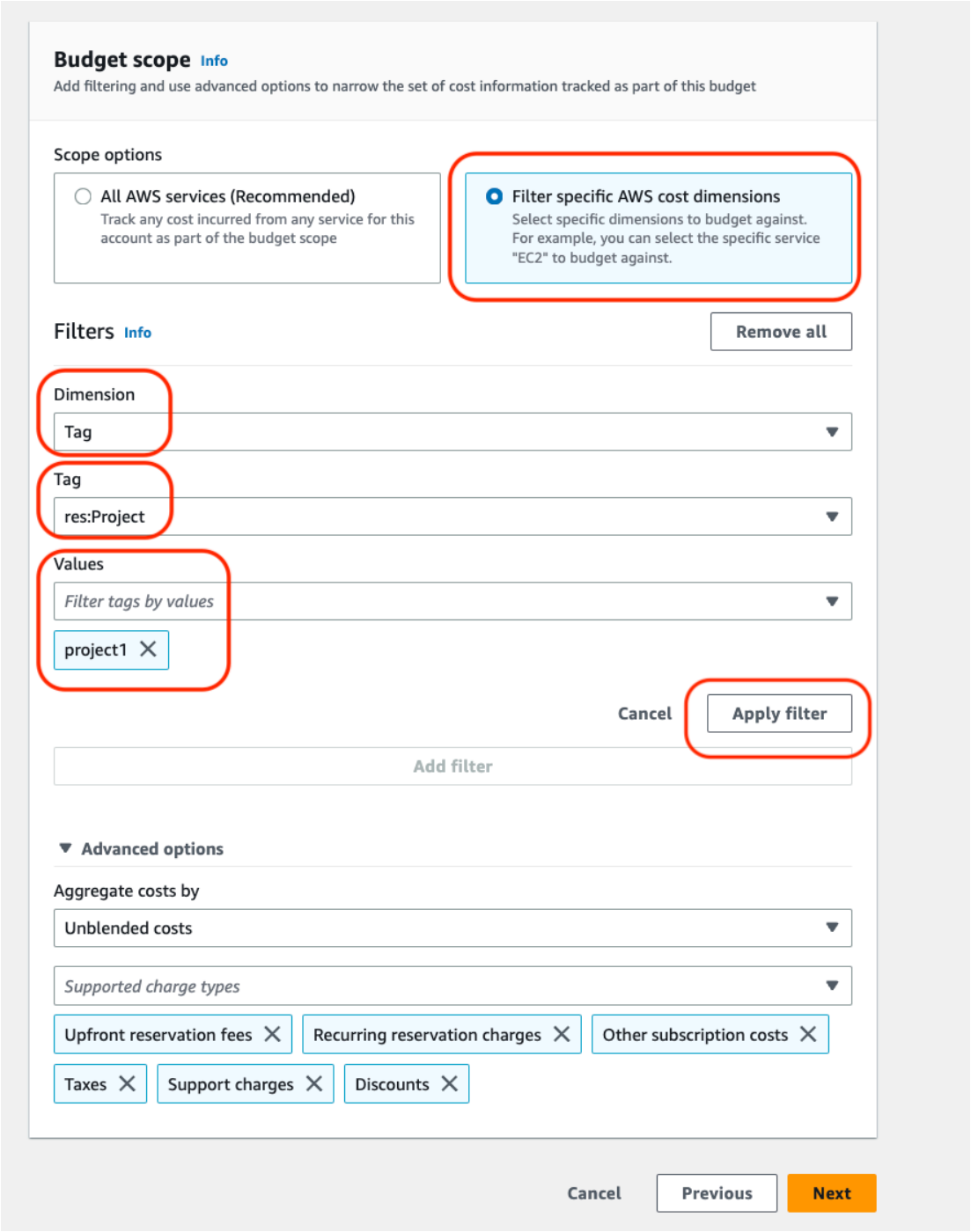
1. Dans la console de facturation, sélectionnez Budgets.
2. Choisissez Créer un budget.
3. Sous Configuration du budget, choisissez Personnaliser (avancé).
4. Sous Types de budget, sélectionnez Budget des coûts - Recommandé.
5. Choisissez Suivant.



6. Sous Détails, saisissez un nom de budget significatif pour votre budget afin de le distinguer des autres budgets de votre compte. Par exemple, *<EnvironmentName>-<ProjectName>-<BudgetName>*.
7. Sous Définir le montant du budget, entrez le montant budgétisé pour votre projet.
8. Sous Étendue du budget, choisissez Filtrer les dimensions de AWS coût spécifiques.
9. Choisissez Add filter.
10. Sous Dimension, choisissez Tag.
11. Sous Tag, sélectionnez RES:Project.

> **Note**
>
> La disponibilité des balises et des valeurs peut prendre jusqu'à deux jours. Vous pouvez créer un budget une fois que le nom du projet sera disponible.

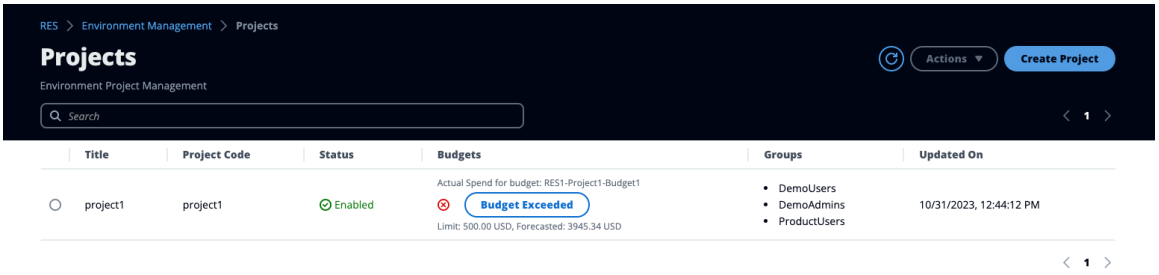
12. Sous Valeurs, sélectionnez le nom du projet.
13. Choisissez Appliquer le filtre pour associer le filtre de projet au budget.
14. Choisissez Suivant.



15. (Facultatif.) Ajoutez un seuil d'alerte.
16. Choisissez Suivant.
17. (Facultatif.) Si une alerte a été configurée, utilisez Attacher des actions pour configurer les actions souhaitées avec l'alerte.
18. Choisissez Suivant.

19. Vérifiez la configuration du budget et confirmez que la balise correcte a été définie sous Paramètres budgétaires supplémentaires.
20. Choisissez Créer un budget.

Maintenant que le budget a été créé, vous pouvez activer le budget pour les projets. Pour activer les budgets d'un projet, voirthe section called "Modifier un projet". Le lancement des bureaux virtuels sera bloqué si le budget est dépassé. Si le budget est dépassé lors du lancement d'un ordinateur de bureau, celui-ci continuera à fonctionner.



Si vous devez modifier votre budget, revenez à la console pour modifier le montant du budget. La prise en compte de la modification dans RES peut prendre jusqu'à quinze minutes. Vous pouvez également modifier un projet pour désactiver un budget.

Tableau de bord d'analyse des coûts

Le tableau de bord d'analyse des coûts permet aux administrateurs RES de surveiller les budgets et les coûts des projets au fil du temps à partir du portail RES. Les coûts peuvent être filtrés au niveau du projet.

Rubriques

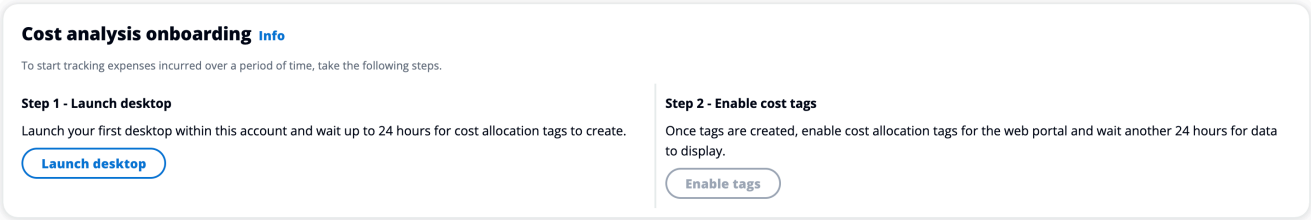
- Conditions préalables
- Projets avec tableau du budget attribué
- Tableau de l'analyse des coûts au fil du temps
- Téléchargement d'un fichier CSV

Conditions préalables

Pour utiliser le tableau de bord des coûts pour Research and Engineering Studio, vous devez d'abord :

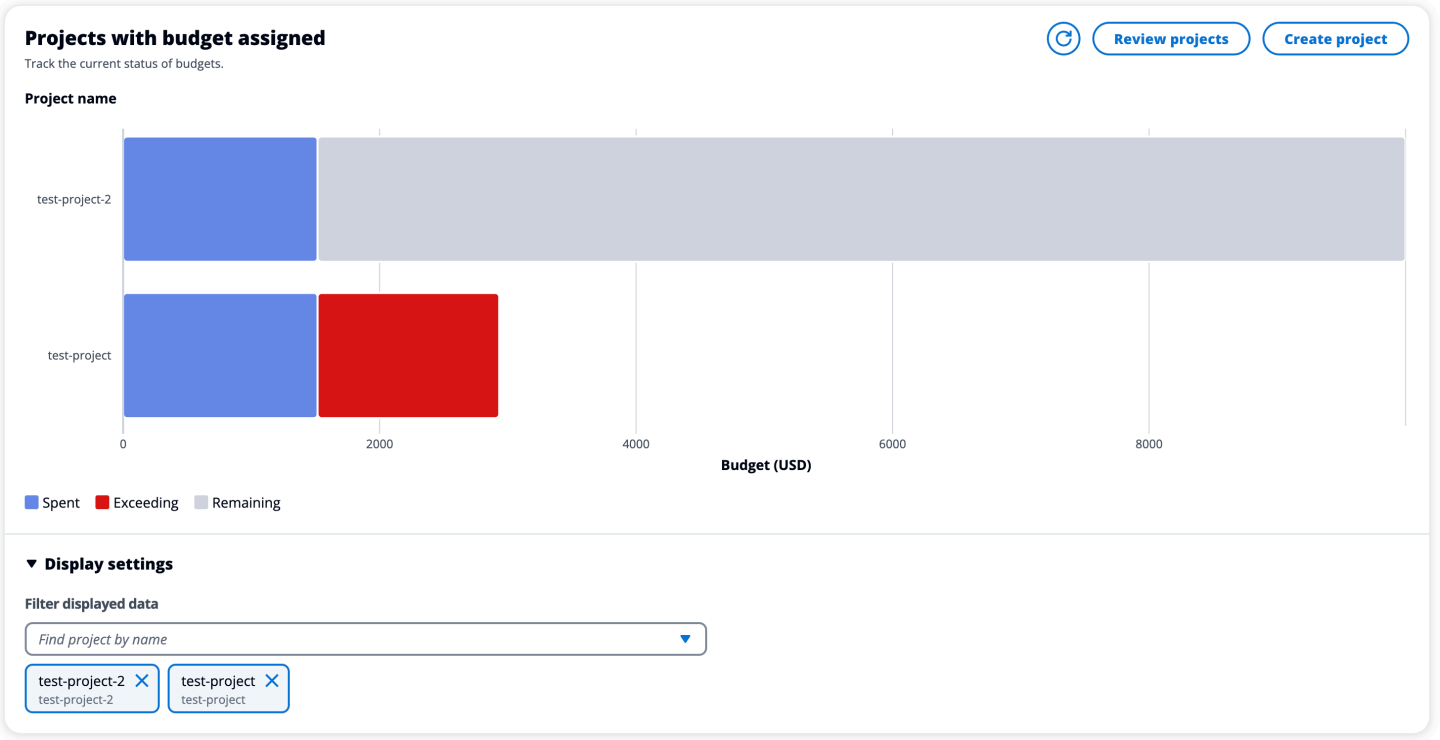
- Création d'un projet.
- Créez un budget dans la console AWS Billing and Cost Management.
- Joignez le budget au projet (voirModifier un projet).
- Activez le tableau d'analyse des coûts pour les comptes dotés de nouveaux déploiements RES. Pour cela, procédez comme suit :

  1. Déployez un VDI pour le projet que vous avez créé. Cela approvisionne le `res:Project` tag dans le AWS Cost Explorer, ce qui peut prendre jusqu'à 24 heures.
  2. Une fois le tag créé, le bouton Activer les tags est activé. Cliquez sur le bouton pour activer les balises dans Cost Explorer. Ce processus peut prendre 24 heures supplémentaires.



Projets avec tableau du budget attribué

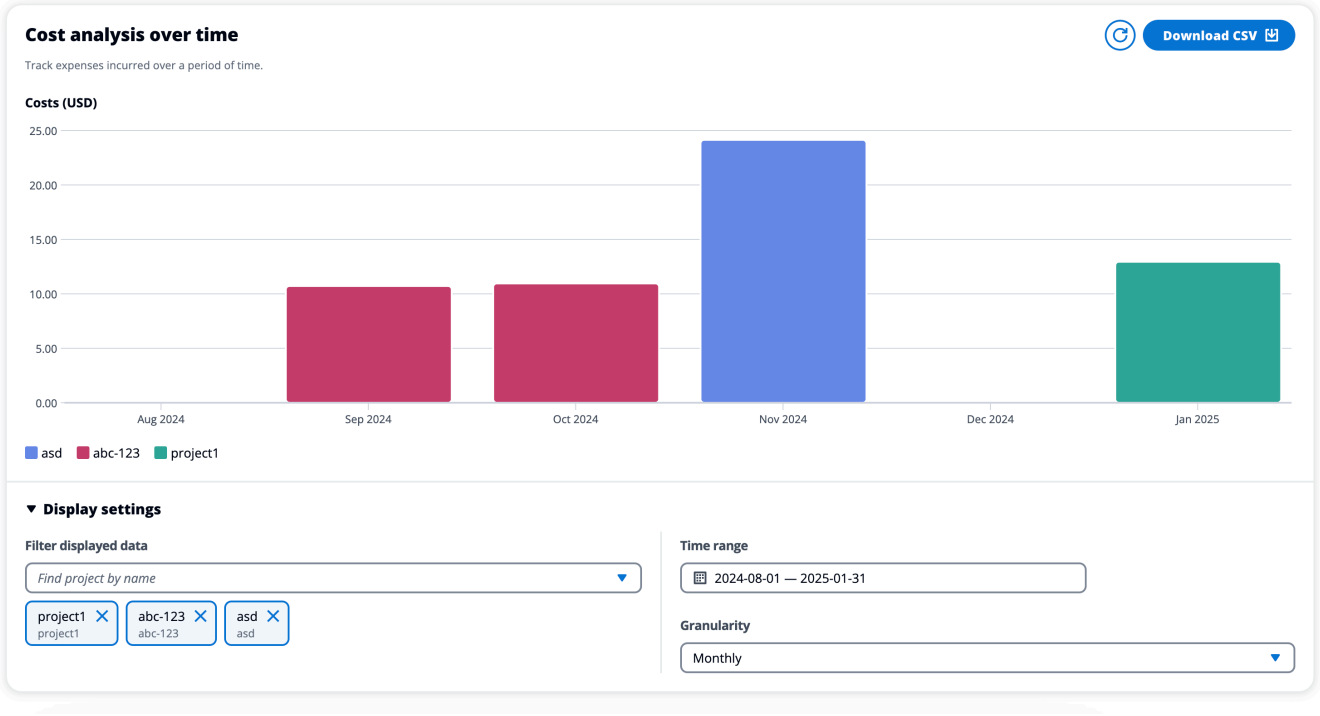
Le graphique Projets avec budget attribué affiche l'état du budget des projets dans l'environnement RES auxquels des budgets leur ont été affectés. Par défaut, le graphique affiche les 5 meilleurs projets par montant budgétaire. Vous pouvez sélectionner des projets spécifiques dans le menu déroulant Filtrer les données affichées qui charge la liste complète des projets affectés au budget.



Le graphique affiche les montants dépensés, restants et excédentaires pour chaque budget en dollars américains. Passez le curseur sur une barre pour afficher les montants exacts en dollars américains pour chaque catégorie. Vous pouvez également ouvrir les pages Projets et Créer un projet en cliquant sur les boutons Réviser les projets et Créer un projet dans le coin supérieur droit, respectivement.

Tableau de l'analyse des coûts au fil du temps

Le graphique de l'analyse des coûts dans le temps affiche la répartition des coûts par projet sur une période donnée. Par défaut, le graphique affiche les données de chacun des 6 derniers mois. Il affiche les 5 meilleurs projets en termes de coût total sur la période sélectionnée avec la granularité que vous sélectionnez. Tous les autres projets sélectionnés, à l'exception des 5 premiers, sont regroupés dans une autre catégorie.

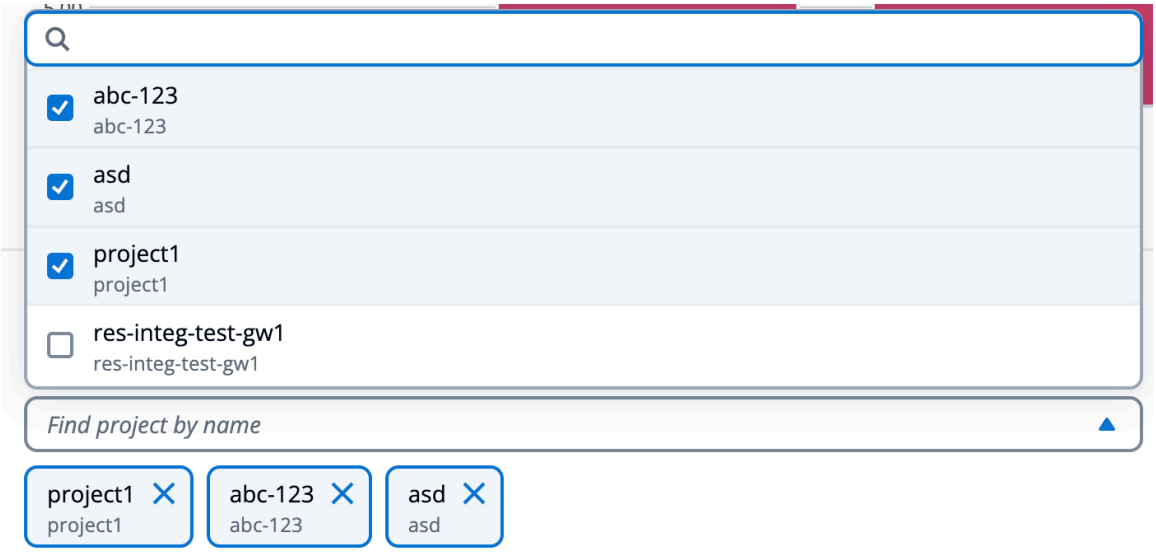


Filtres

Vous pouvez filtrer par projet, par plage de temps et par granularité pour personnaliser l'affichage graphique de l'analyse des coûts au fil du temps. Si des combinaisons de filtres non valides sont sélectionnées, une fenêtre modale apparaît qui vous permet de revenir à la configuration précédente ou d'accepter une suggestion pour la combinaison de filtres mise à jour.

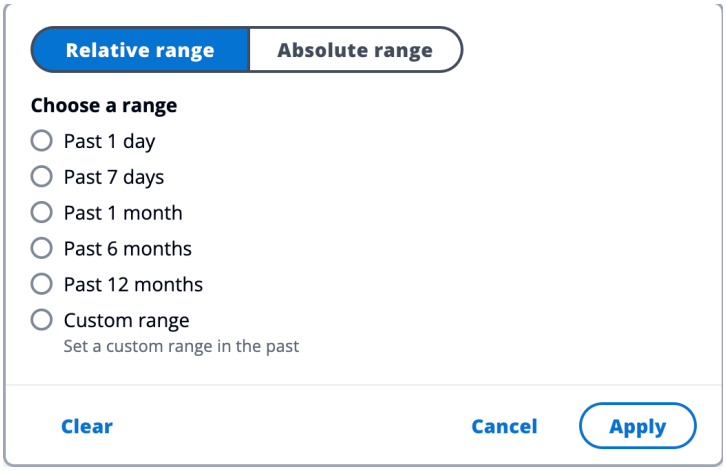
Project

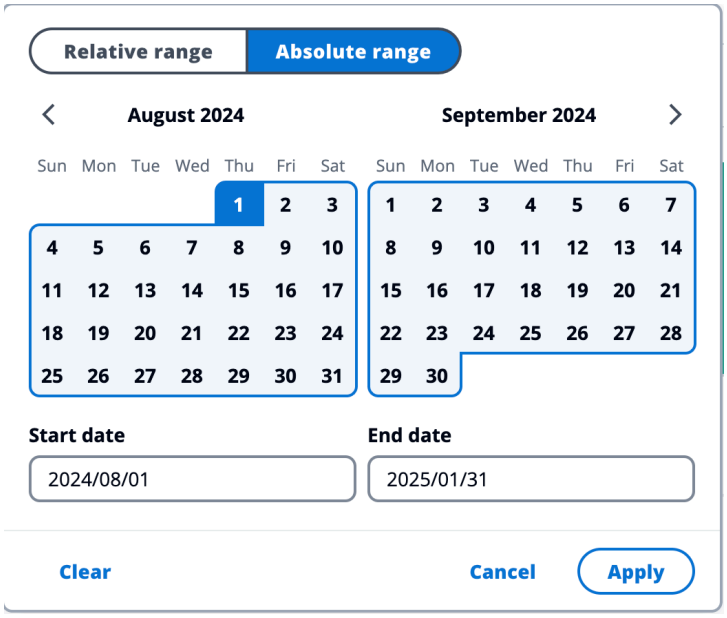
Lorsque vous choisissez le menu déroulant Filtrer les données affichées, vous pouvez voir une liste complète des projets dans votre environnement RES actuel. Vous voyez le nom du projet, avec le code du projet affiché en dessous.



Spécification de l'intervalle de temps

Vous pouvez choisir d'utiliser une plage absolue ou une plage relative lorsque vous spécifiez une plage de dates. Lorsque vous sélectionnez une plage relative, les dates sont calculées en utilisant des unités de temps complètes. Par exemple, si vous sélectionnez l'option 6 derniers mois en février 2025, cela se traduira par une plage de temps comprise entre le 1er août et le 31 janvier 2025.



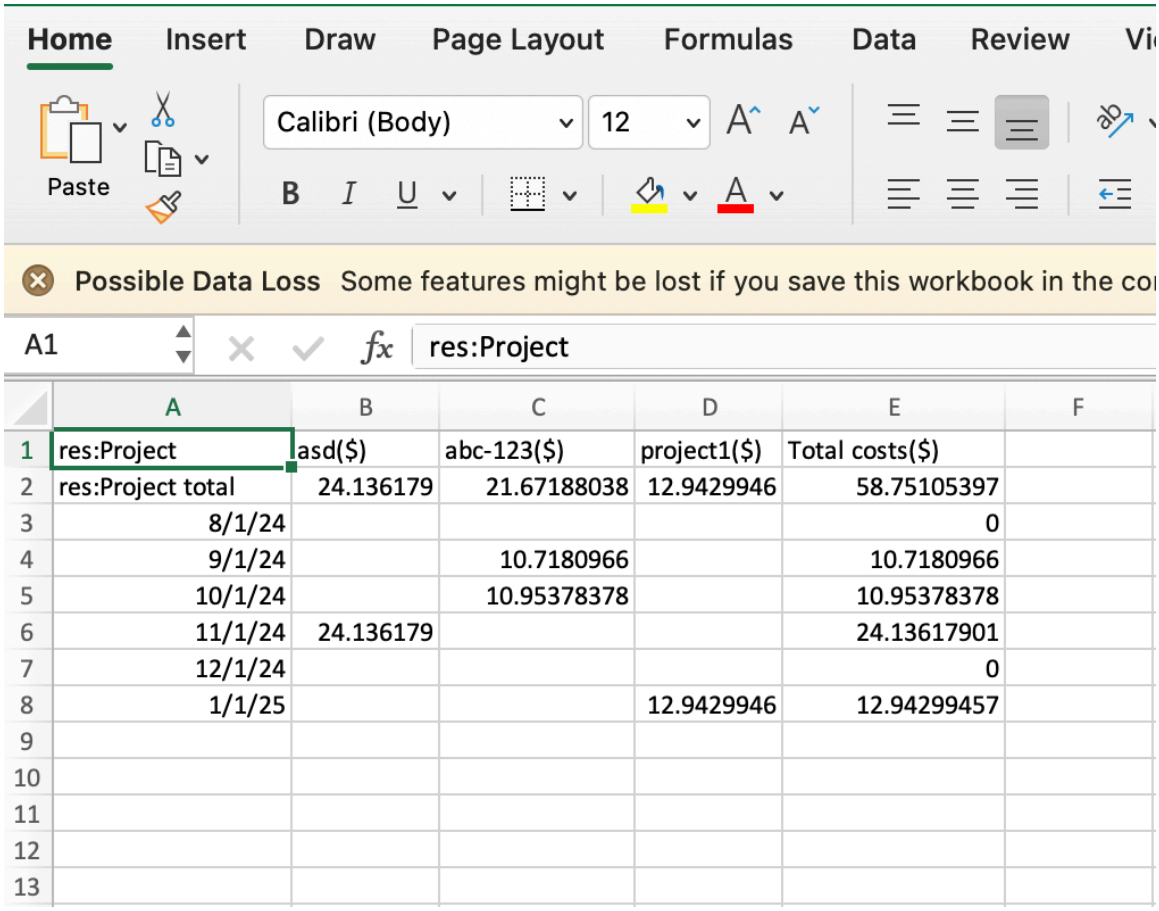


Granularité

Vous pouvez choisir d'afficher les données avec une granularité mensuelle, quotidienne ou horaire. La granularité horaire ne prend en charge qu'une plage de dates allant jusqu'à 14 jours. La granularité quotidienne ne prend en charge qu'une plage de dates allant jusqu'à 14 mois.

Téléchargement d'un fichier CSV

Pour exporter la vue d'analyse des coûts actuelle, choisissez Télécharger le fichier CSV en haut à droite du graphique Analyse des coûts au fil du temps. Le fichier CSV téléchargé contient les informations sur les coûts de chaque projet sélectionné pour la période spécifiée, ainsi que les coûts totaux par projet et par période.



	A	B	C	D	E	F
1	res:Project	asd($)	abc-123($)	project1($)	Total costs($)	
2	res:Project total	24.136179	21.67188038	12.9429946	58.75105397	
3	8/1/24				0	
4	9/1/24		10.7180966		10.7180966	
5	10/1/24		10.95378378		10.95378378	
6	11/1/24	24.136179			24.13617901	
7	12/1/24				0	
8	1/1/25			12.9429946	12.94299457	
9						
10						
11						
12						
13						

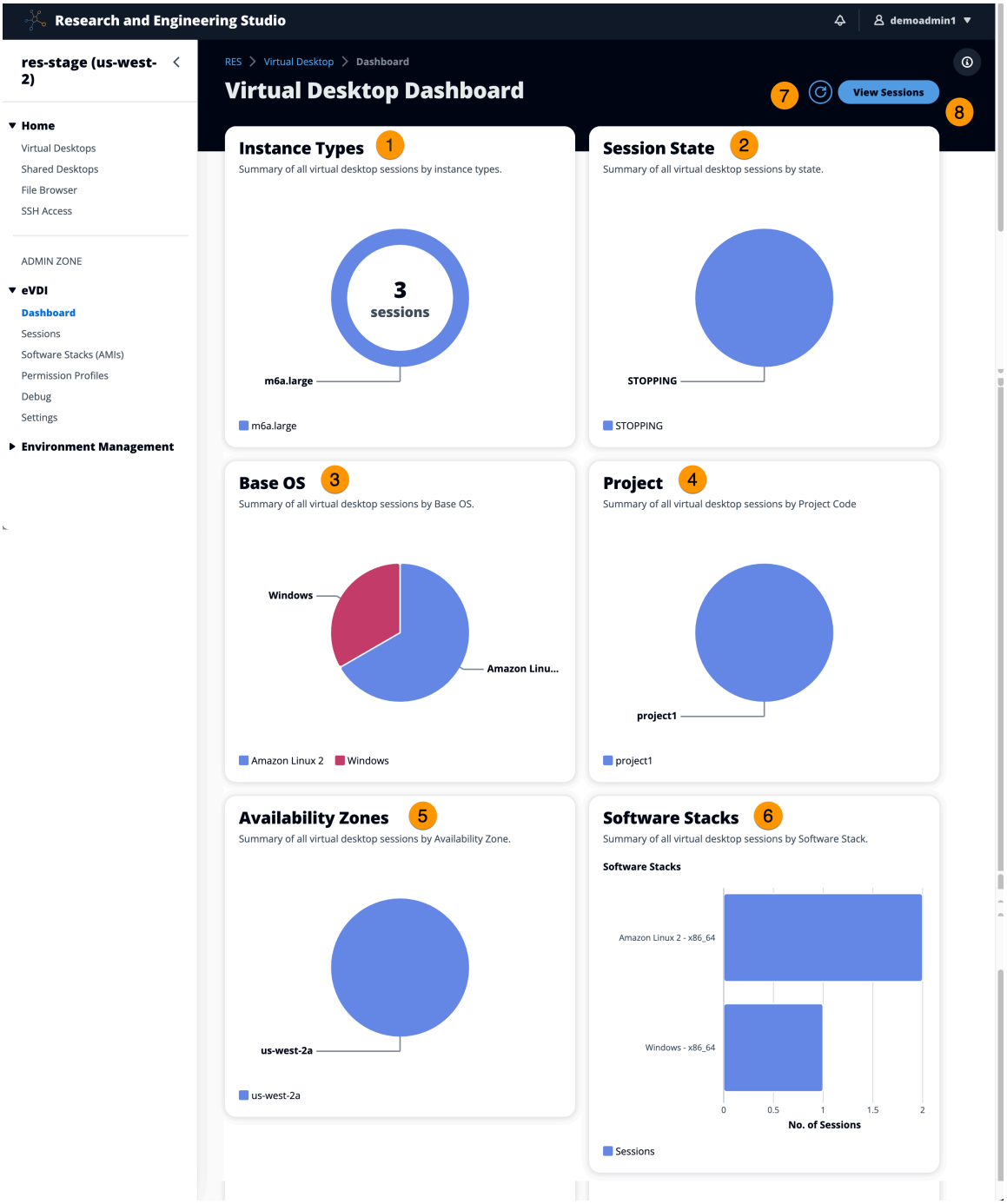
Gestion de session

La gestion des sessions fournit un environnement flexible et interactif pour le développement et le test des sessions. En tant qu'utilisateur administratif, vous pouvez autoriser les utilisateurs à créer et à gérer des sessions interactives au sein de leur environnement de projet.

Rubriques

- Tableau de bord
- Séances
- Piles de logiciels () AMIs
- Débogage
- Réglages du bureau

Tableau de bord



Le tableau de bord de gestion des sessions fournit aux administrateurs un aperçu rapide des éléments suivants :

1. Types d'instances
2. États de session

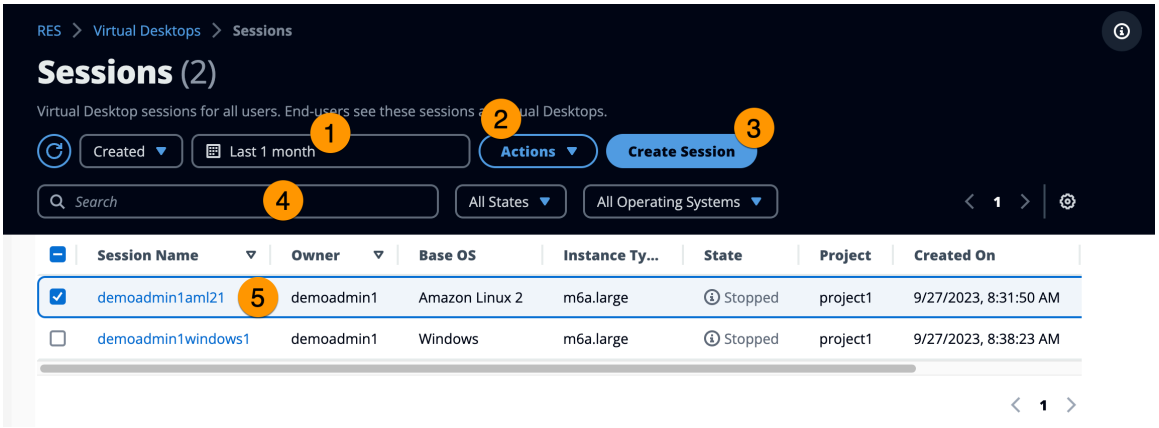
3. Système d'exploitation de base
4. Projets
5. Zones de disponibilité
6. Piles de logiciels

En outre, les administrateurs peuvent :

7. Actualisez le tableau de bord pour mettre à jour les informations.
8. Choisissez Afficher les sessions pour accéder aux sessions.

Séances

Sessions affiche tous les bureaux virtuels créés dans Research and Engineering Studio. Sur la page Sessions, vous pouvez filtrer et afficher les informations de session ou créer une nouvelle session.

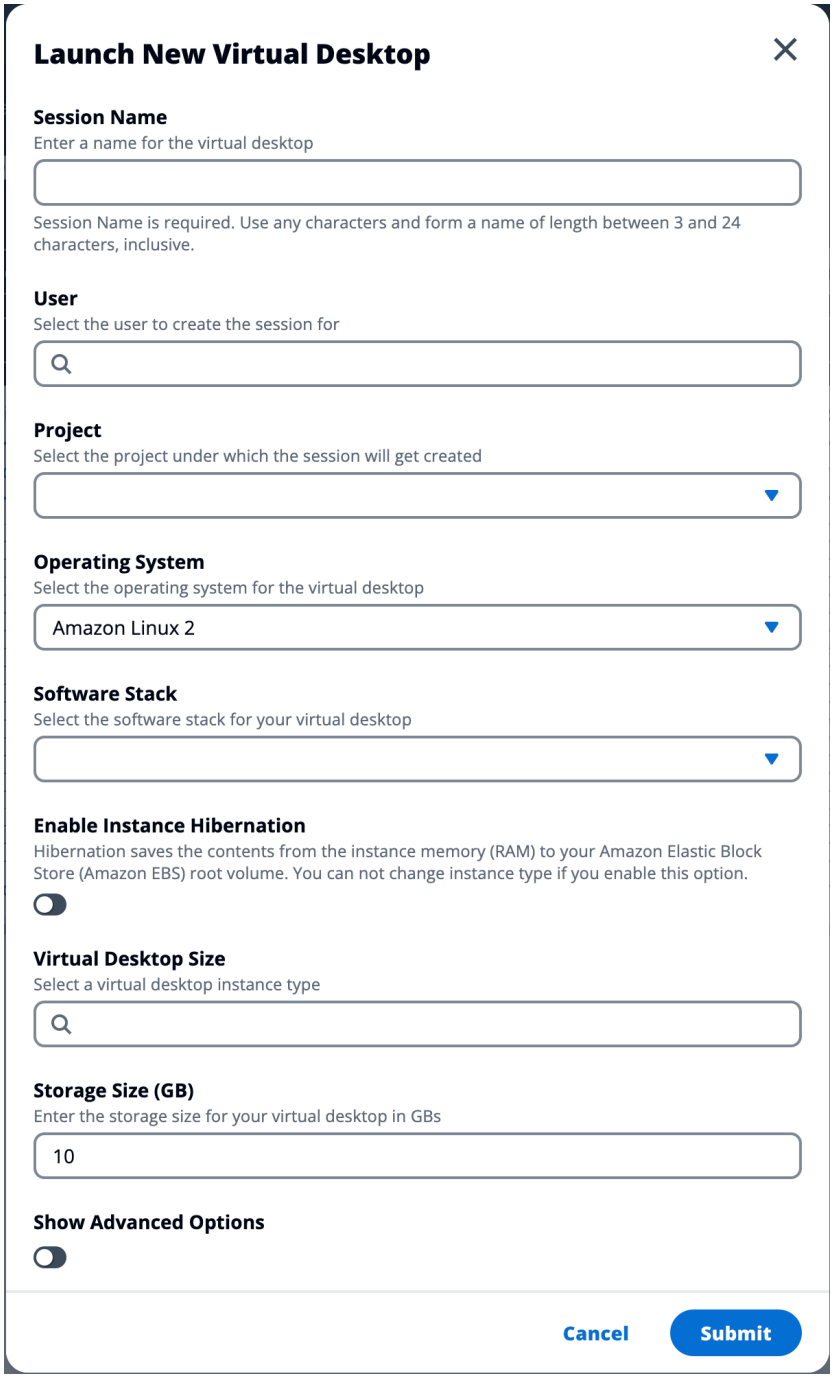


1. Utilisez le menu pour filtrer les résultats par sessions créées ou mises à jour au cours d'une période spécifiée.
2. Sélectionnez une session et utilisez le menu Actions pour :
   a. Reprendre une ou plusieurs sessions
   b. Stop/Hibernate Séance (s)
   c. Stop/Hibernate Séance (s) forcée (s)
   d. Terminer une ou plusieurs sessions
   e. Forcer la fermeture d'une ou de plusieurs sessions
   f. Séance (s) Santé
   g. Créez une pile de logiciels

3. Choisissez Create Session pour créer une nouvelle session.
4. Recherchez une session par nom et filtrez par état et système d'exploitation.
5. Sélectionnez le nom de la session pour afficher plus de détails.

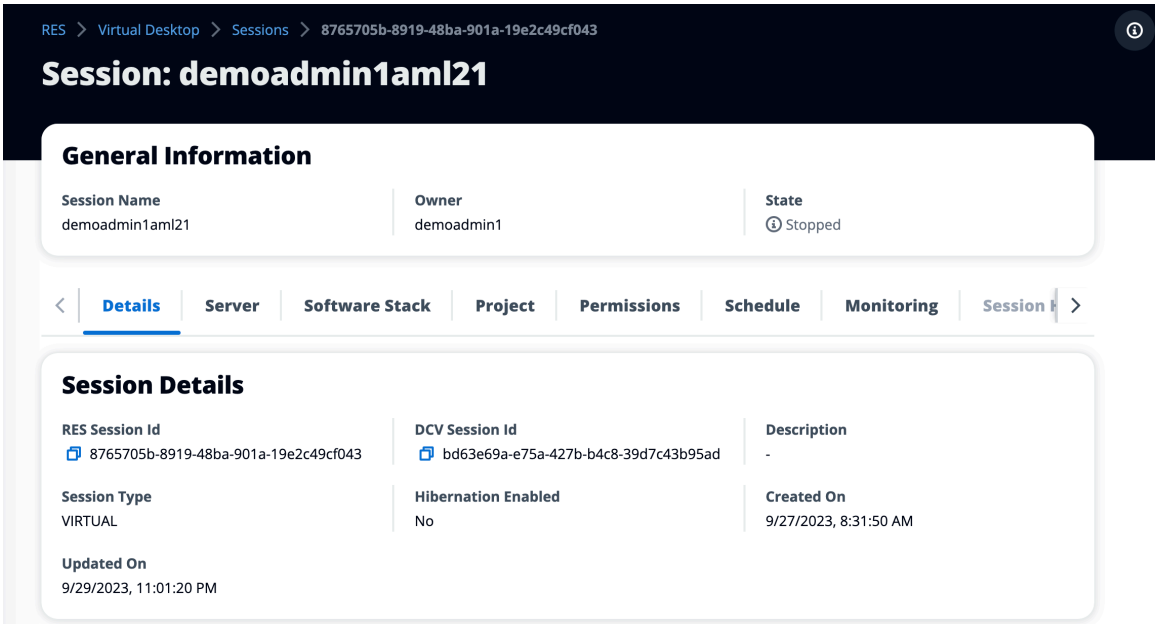
Créer une session

1. Choisissez Create Session. Le modal Launch New Virtual Desktop s'ouvre.
2. Entrez les détails de la nouvelle session.
3. (Facultatif.) Activez Afficher les options avancées pour fournir des informations supplémentaires telles que l'ID de sous-réseau et le type de session DCV.
4. Sélectionnez Soumettre.



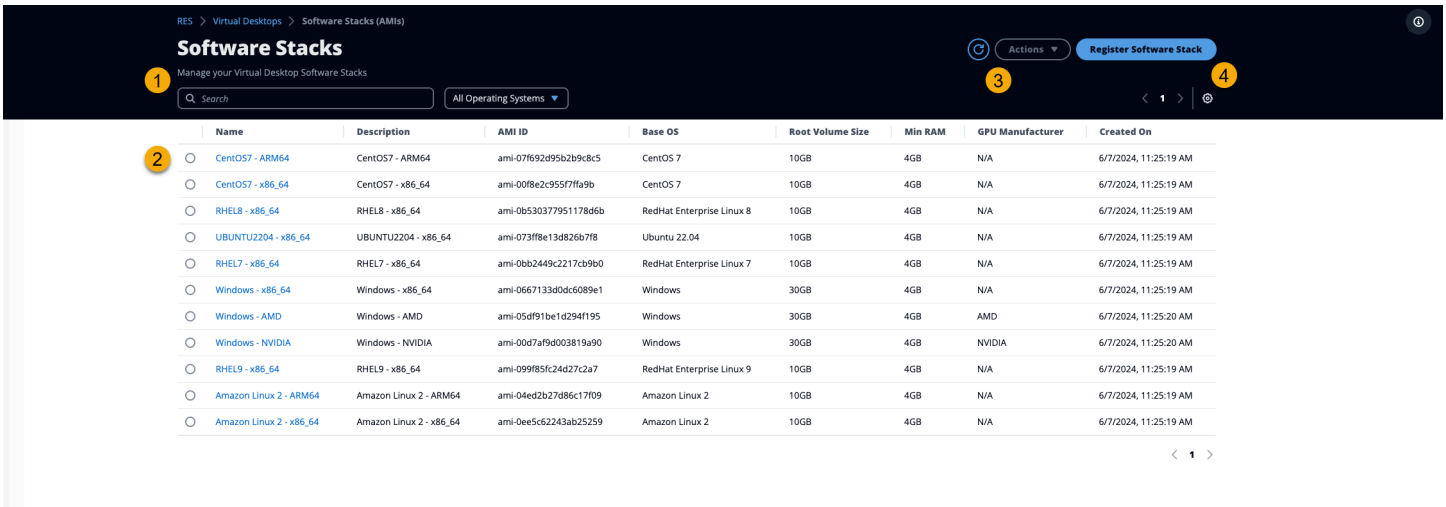
Détails de la session

Dans la liste des sessions, sélectionnez le nom de la session pour afficher les détails de la session.



Piles de logiciels () AMIs

Sur la page Software Stacks, vous pouvez configurer Amazon Machine Images (AMIs) ou gérer les images existantes.

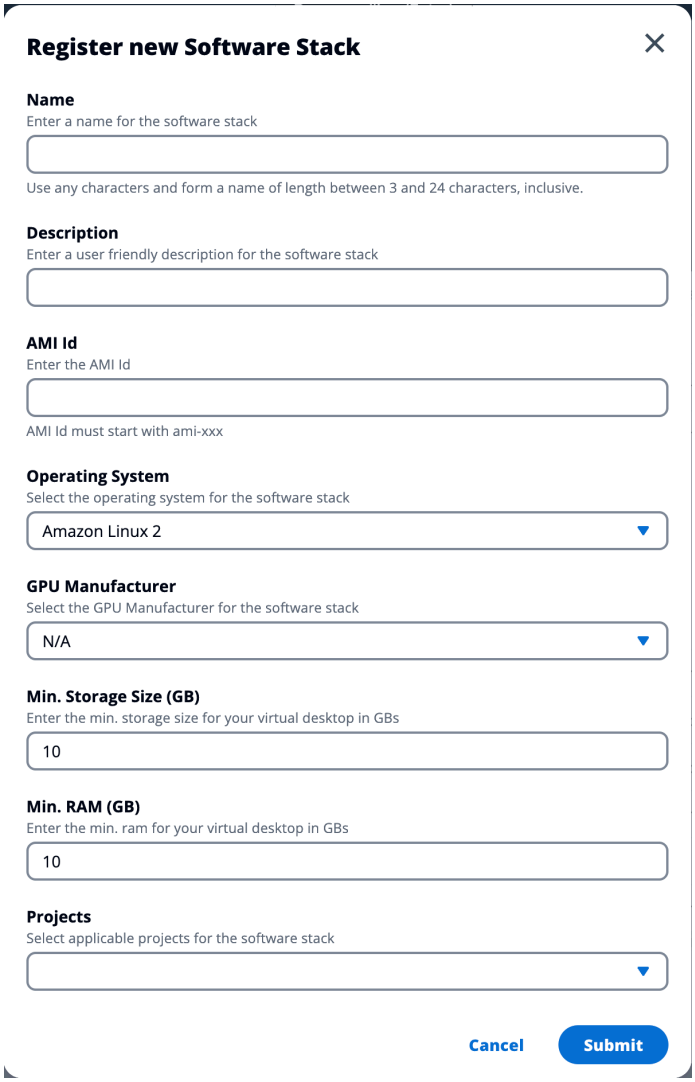


1. Pour rechercher une pile logicielle existante, utilisez le menu déroulant du système d'exploitation pour filtrer par système d'exploitation.
2. Sélectionnez le nom d'une pile logicielle pour afficher les détails de la pile.
3. Cliquez sur le bouton radio situé à côté d'une pile logicielle, puis utilisez le menu Actions pour modifier la pile et l'attribuer à un projet.
4. Cliquez sur le bouton Register Software Stack pour créer une nouvelle pile.

Enregistrer une nouvelle pile logicielle

Le bouton Register Software Stack vous permet de créer une nouvelle pile :

1. Choisissez Register Software Stack.
2. Entrez les détails de la nouvelle pile logicielle.
3. Sélectionnez Soumettre.

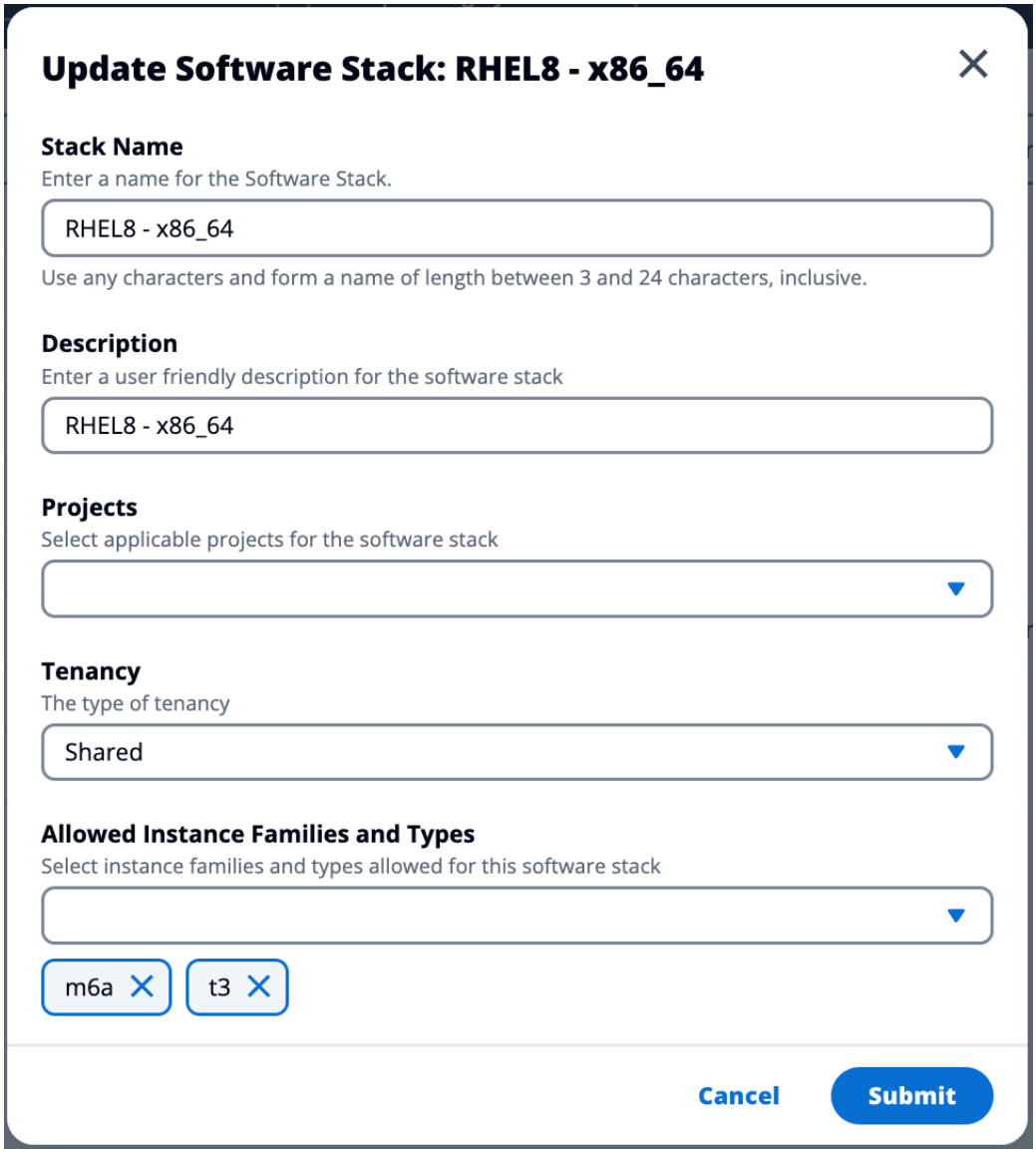


Attribuer une pile logicielle à un projet

Lorsque vous créez une nouvelle pile logicielle, vous pouvez l'attribuer à des projets. Toutefois, si vous devez ajouter la pile à un projet après sa création initiale, procédez comme suit :

> **Note**
>
> Vous ne pouvez attribuer des piles de logiciels qu'aux projets dont vous êtes membre.

1. Sur la page Software Stacks, sélectionnez le bouton radio correspondant à la pile logicielle que vous souhaitez ajouter à un projet.
2. Choisissez Actions.
3. Choisissez Modifier.
4. Utilisez le menu déroulant Projets pour sélectionner le projet.

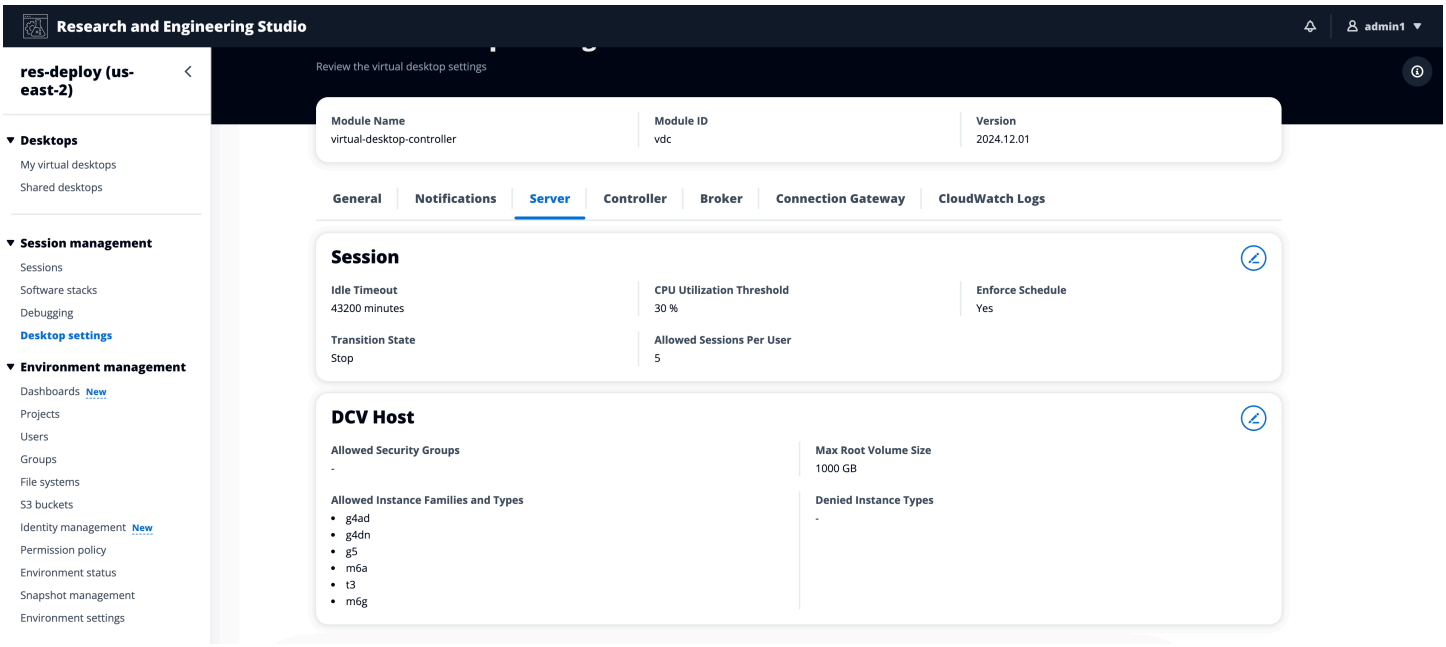


5. Sélectionnez Soumettre.

Vous pouvez également modifier la pile logicielle depuis la page des détails de la pile.

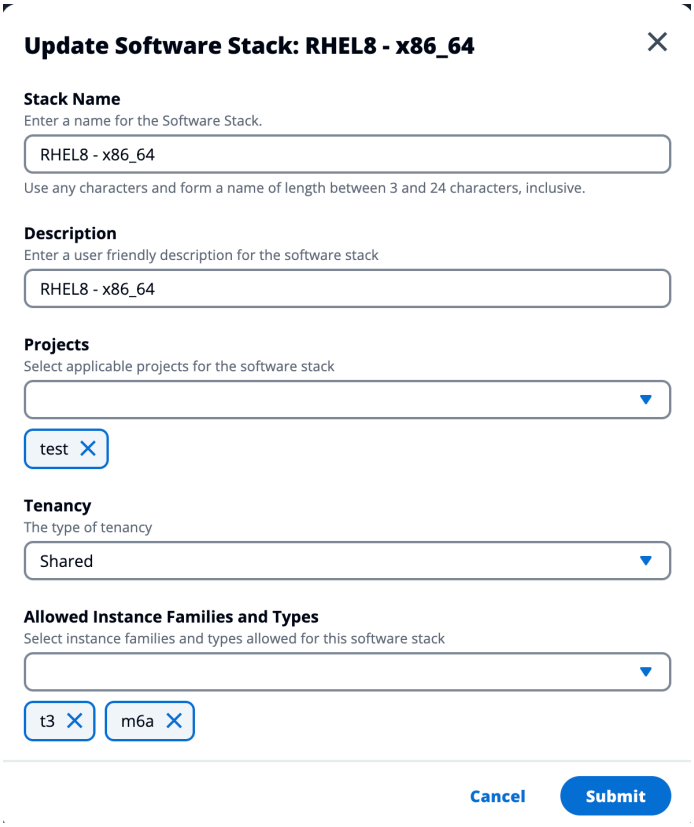
Modifier la liste des instances VDI de la pile logicielle

Pour chaque pile logicielle enregistrée, vous pouvez choisir les familles et les types d'instances autorisés. La liste des options pour chaque pile logicielle est filtrée en fonction des options définies dans les paramètres du bureau. Vous pouvez y trouver et modifier les familles et types d'instances autorisés globaux.



Pour modifier l'attribut Familles et types d'instances autorisés d'une pile logicielle :

1. Sur la page Software Stacks, cliquez sur le bouton radio correspondant à la pile logicielle.
2. Choisissez Actions, puis sélectionnez Modifier la pile.
3. Choisissez les familles et types d'instances souhaités dans la liste déroulante située sous Familles et types d'instances autorisés.



4. Sélectionnez Soumettre.

> **Note**
>
> Si l'ensemble global de familles et de types d'instances autorisés inclut une famille d'instances et un type d'instance au sein de cette famille (par exemple `t3` et`t3.large`), les options disponibles pour l'attribut Familles et types d'instances autorisés d'une pile logicielle incluront uniquement la famille d'instances.

> **Important**
>
> - Lorsqu'une instance type/family est supprimée de la liste d'autorisation au niveau de l'environnement, elle doit être automatiquement supprimée de toutes les piles logicielles.
> - Les instances types/familles ajoutées au niveau de l'environnement ne sont pas automatiquement ajoutées aux piles logicielles.

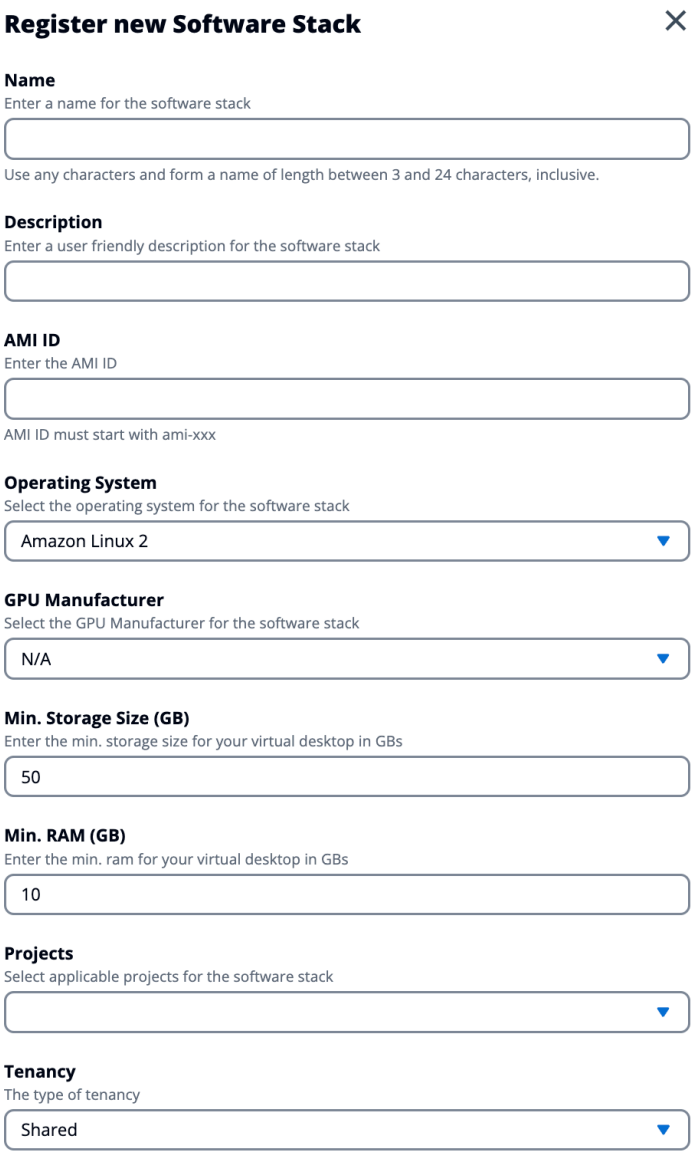
Afficher les détails de la pile logicielle

Sur la page Software Stacks, sélectionnez le nom de la pile logicielle pour en afficher les détails. Vous pouvez également sélectionner le bouton radio correspondant à une pile logicielle, choisir Actions et sélectionner Modifier pour modifier la pile logicielle.

Assistance à la location VDI

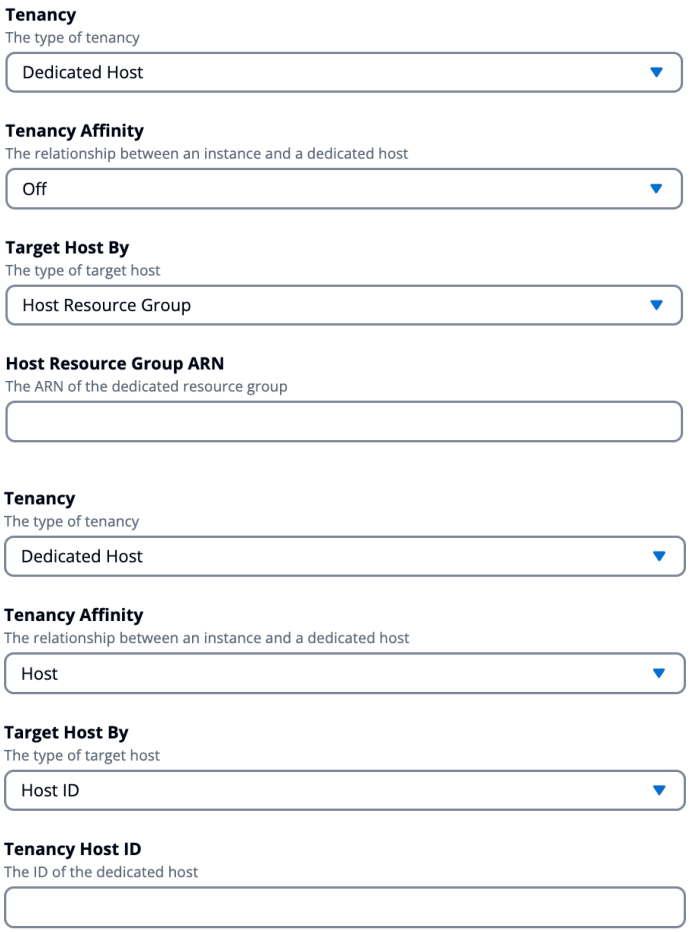
Lorsque vous enregistrez une nouvelle pile logicielle ou que vous modifiez une pile logicielle existante, vous pouvez sélectionner la location de la pile logicielle VDIs lancée à partir de cette pile logicielle. Les trois locations suivantes sont prises en charge :

- Partagé (par défaut) - Exécuter VDIs avec des instances matérielles partagées
- Instance dédiée - Exécutée VDIs avec des instances dédiées
- Hôte dédié : fonctionne VDIs avec un hôte dédié



Lorsque vous sélectionnez le type de location d'hôte dédié, vous devez également sélectionner l'affinité de location et le type d'hôte cible. Les types d'hôtes cibles suivants sont pris en charge :

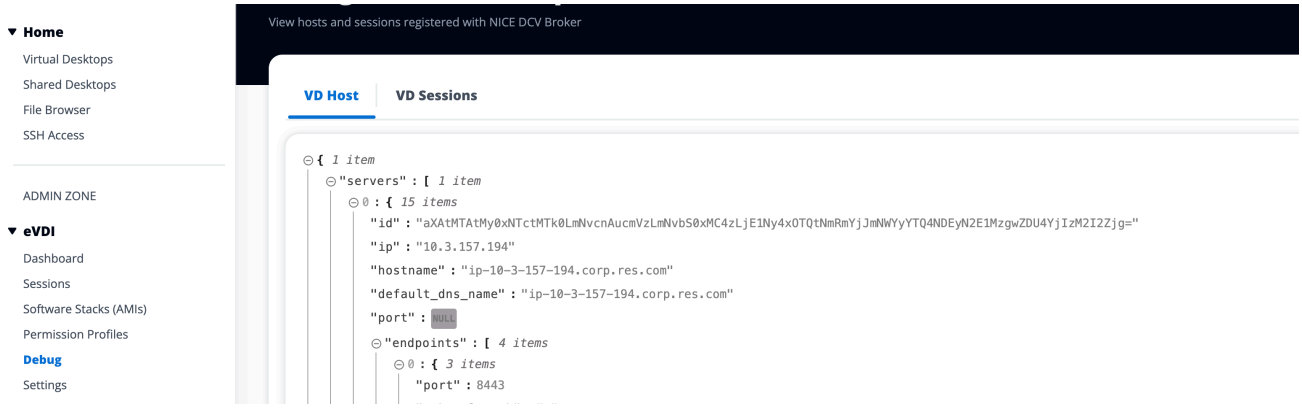
- Host Resource Group : groupe de ressources hôte créé dans AWS License Manager
- ID d'hôte : identifiant d'hôte spécifique



Pour spécifier les licences autogérées dont vous avez besoin VDIs lorsque vous les lancez avec la location d'hôte dédiée, associez les licences à votre AMI en suivant la procédure Associating self-managed licenses et AMIs dans le guide de l'utilisateur du AWS License Manager.

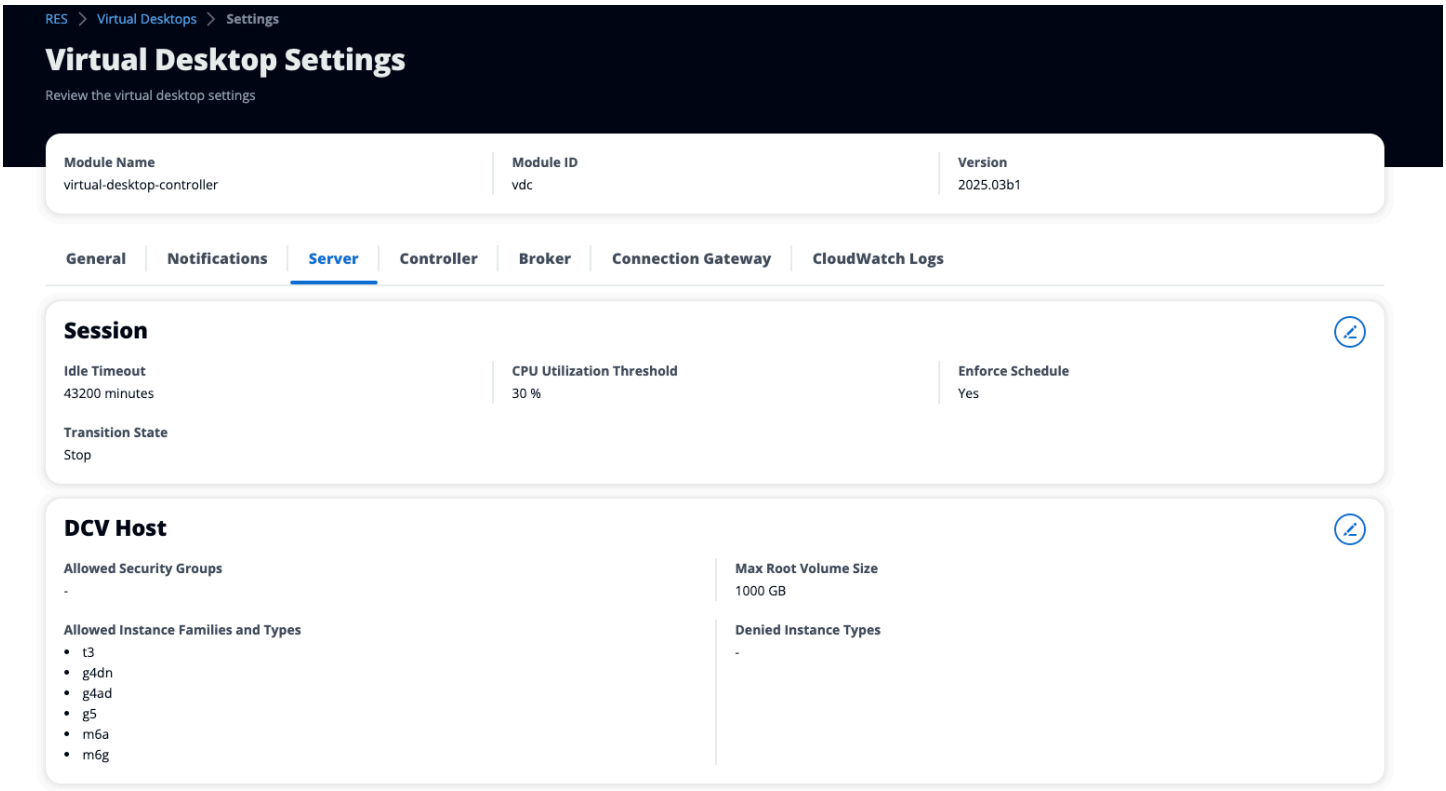
Débogage

Le panneau de débogage affiche le trafic de messages associé aux bureaux virtuels. Vous pouvez utiliser ce panneau pour observer l'activité entre les hôtes. L'onglet VD Host affiche l'activité spécifique à l'instance, et l'onglet VD Sessions affiche l'activité de session en cours.



Réglages du bureau

Vous pouvez utiliser la page Paramètres du bureau pour configurer les ressources associées aux bureaux virtuels.



Général

L'onglet Général permet d'accéder à des paramètres tels que :

QUIC

Active QUIC en faveur du protocole TCP en tant que protocole de streaming par défaut pour tous vos bureaux virtuels.

Type de session DCV par défaut

Type de session DCV par défaut utilisé pour tous les bureaux virtuels. Ce paramètre ne s'applique pas aux bureaux créés précédemment. Cela ne s'applique que dans les cas où le type d'instance et le système d'exploitation prennent en charge les types de session virtuelle ou de console.

Sessions autorisées par défaut par utilisateur et par projet

La valeur par défaut du nombre autorisé de sessions VDI par utilisateur et par projet.

de bases de données

L'onglet Serveur permet d'accéder à des paramètres tels que :

Expiration du délai d'inactivité de la session DCV

Durée après laquelle la session DCV sera automatiquement déconnectée. Cela ne change pas l'état de la session de bureau, cela ferme uniquement la session à partir du client DCV ou du navigateur Web.

Avertissement d'expiration du délai d'inactivité

Durée après laquelle un avertissement d'inactivité sera envoyé au client.

Seuil d'utilisation du processeur

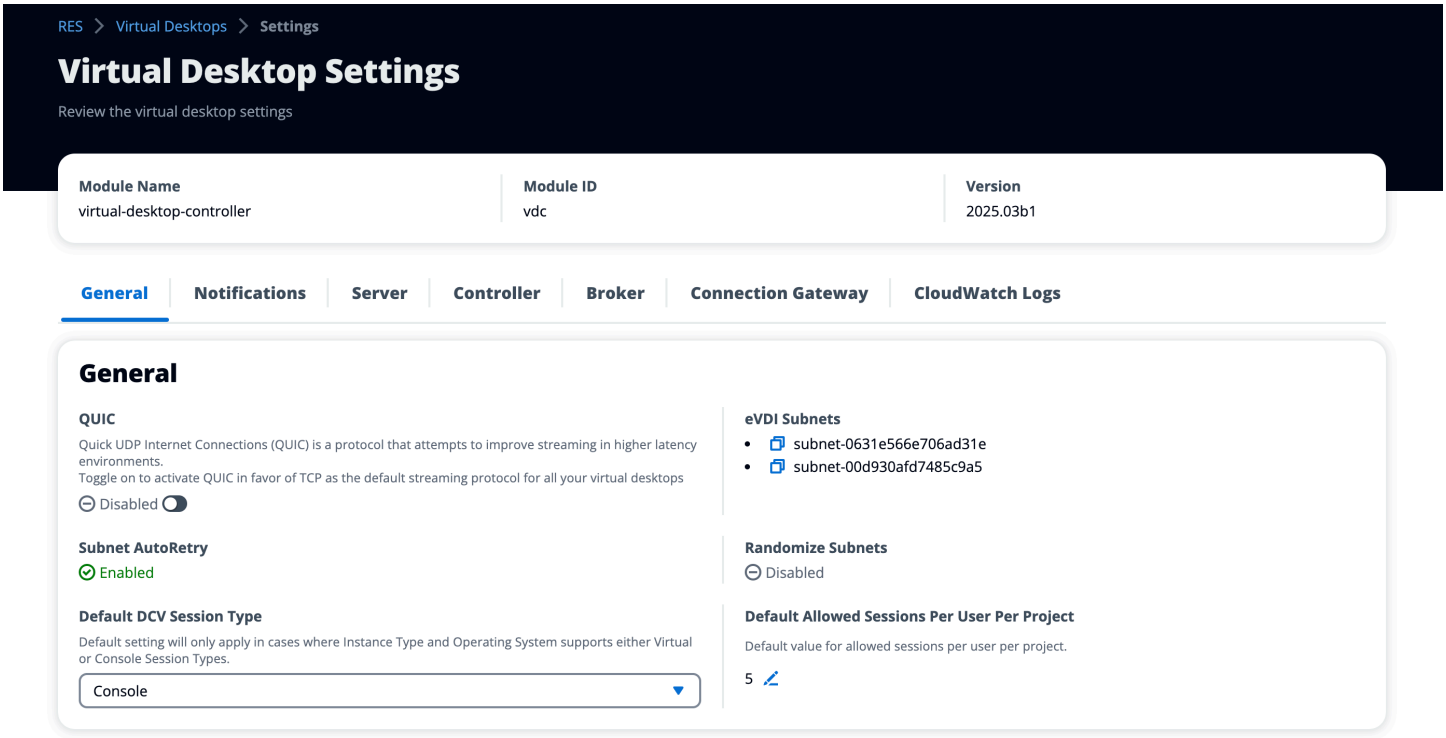
L'utilisation du processeur doit être considérée comme inactive.

Taille maximale du volume racine

Taille par défaut du volume racine sur les sessions de bureau virtuel.

Types d'instances autorisés

Liste des familles et tailles d'instances pouvant être lancées pour cet environnement RES. Les combinaisons de familles et de tailles d'instances sont toutes deux acceptées. Par exemple, si vous spécifiez « m7a », toutes les tailles de la famille m7a pourront être lancées sous forme de sessions VDI. Si vous spécifiez « m7a.24xlarge », seul m7a.24xlarge pourra être lancé en tant que session VDI. Cette liste concerne tous les projets dans l'environnement.



Gestion de l'environnement

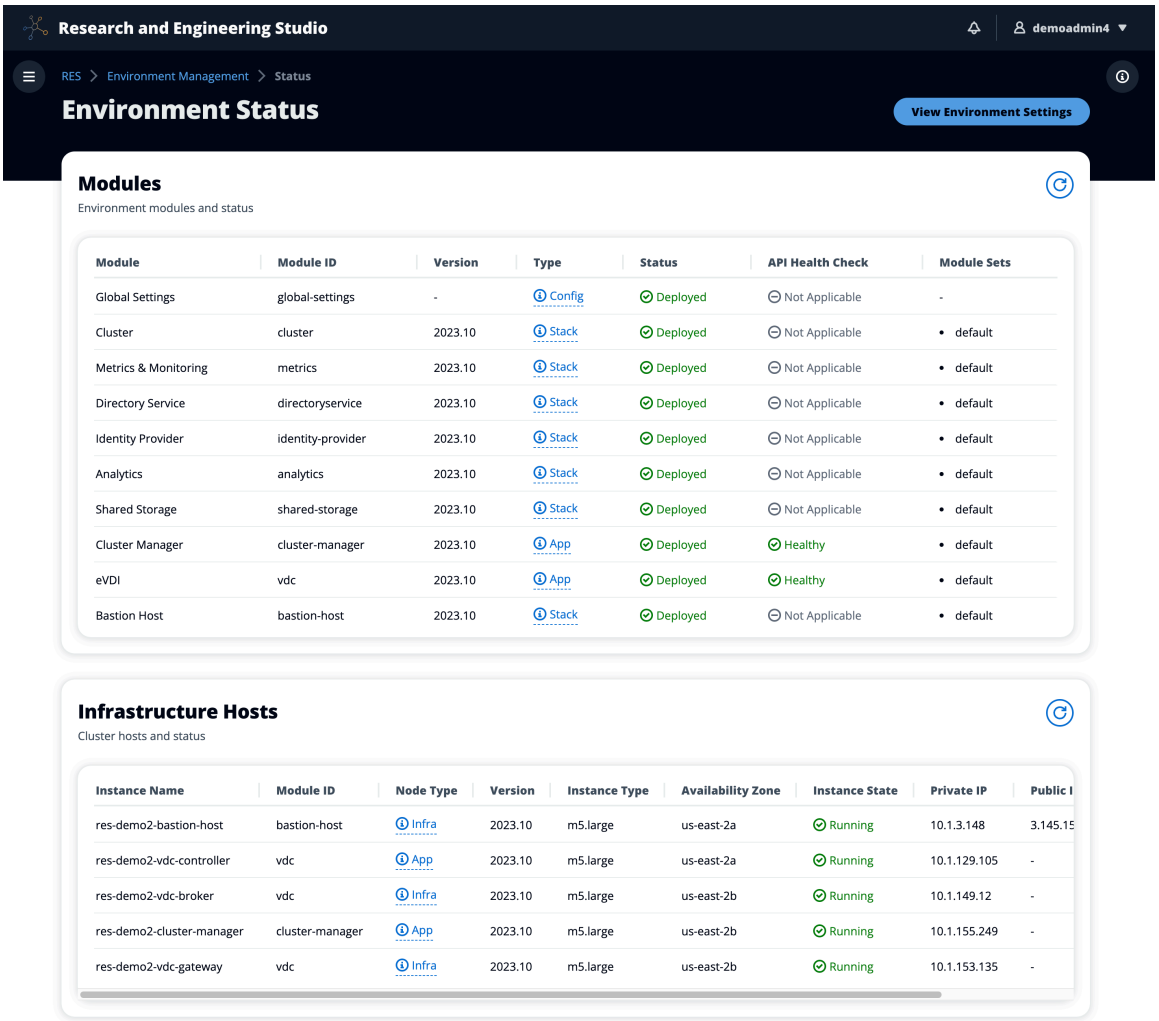
Dans la section Gestion de l'environnement de Research and Engineering Studio, les utilisateurs administratifs peuvent créer et gérer des environnements isolés pour leurs projets de recherche et d'ingénierie. Ces environnements peuvent inclure des ressources informatiques, du stockage et d'autres composants nécessaires, le tout dans un environnement sécurisé. Les utilisateurs peuvent configurer et personnaliser ces environnements pour répondre aux exigences spécifiques de leurs projets, ce qui facilite l'expérimentation, le test et l'itération de leurs solutions sans impact sur les autres projets ou environnements.

Rubriques

- Gestion des instantanés
- Compartiments Amazon S3

État de l'environnement

La page État de l'environnement affiche le logiciel déployé et les hôtes du produit. Il inclut des informations telles que la version du logiciel, les noms des modules et d'autres informations système.



Paramètres d'environnement

La page des paramètres d'environnement affiche les détails de configuration du produit, tels que :

- Général

Affiche des informations telles que le nom d'utilisateur de l'administrateur et l'adresse e-mail de l'utilisateur qui a approvisionné le produit. Vous pouvez modifier le titre du portail Web et le texte du copyright.

- Fournisseur d'identité

  Affiche des informations telles que l'état de l'authentification unique.

- Réseau

  Affiche l'ID VPC et la liste IDs des préfixes pour l'accès.

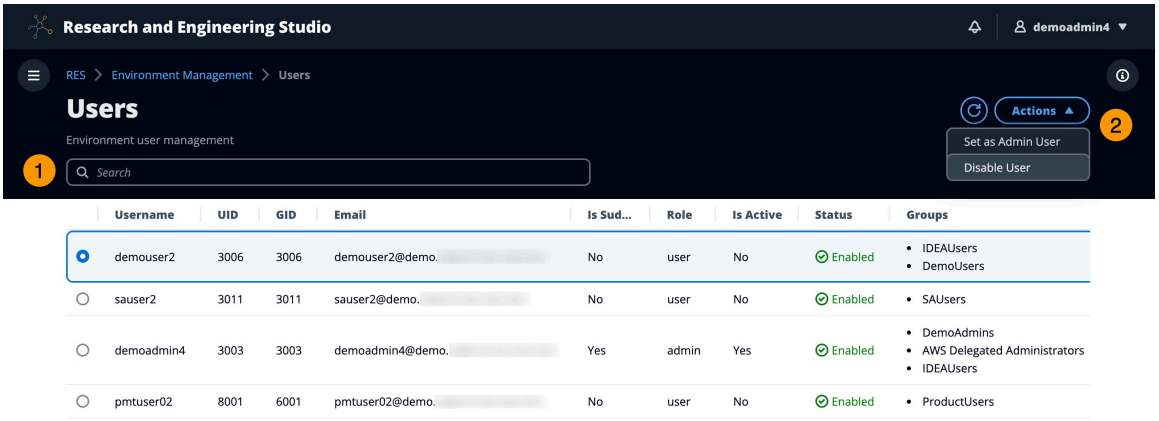
- Directory Service

  Affiche les paramètres Active Directory et l'ARN du gestionnaire de secrets des comptes de service pour le nom d'utilisateur et le mot de passe.

Utilisateurs

Tous les utilisateurs synchronisés depuis votre Active Directory apparaîtront sur la page Utilisateurs. Les utilisateurs sont synchronisés par l'utilisateur cluster-admin lors de la configuration du produit. Pour plus d'informations sur la configuration utilisateur initiale, consultez leGuide de configuration.

> **Note**
>
> Les administrateurs ne peuvent créer des sessions que pour les utilisateurs actifs. Par défaut, tous les utilisateurs seront inactifs jusqu'à ce qu'ils se connectent à l'environnement du produit. Si un utilisateur est inactif, demandez-lui de se connecter avant de créer une session pour lui.

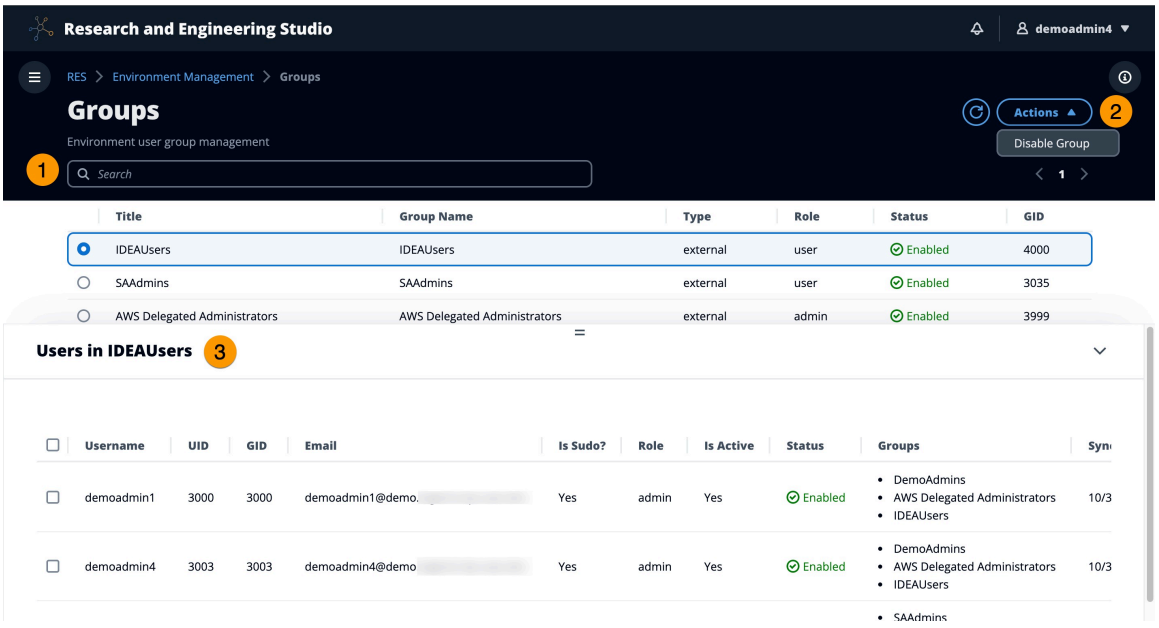


Depuis la page Utilisateurs, vous pouvez :

1. Recherche des utilisateurs.
2. Lorsqu'un nom d'utilisateur est sélectionné, utilisez le menu Actions pour :
    a. Définir en tant qu'utilisateur administrateur
    b. Désactiver l'utilisateur

Groupes

Tous les groupes synchronisés depuis Active Directory apparaissent sur la page Groupes. Pour plus d'informations sur la configuration et la gestion des groupes, consultez leGuide de configuration.



Sur la page Groupes, vous pouvez :

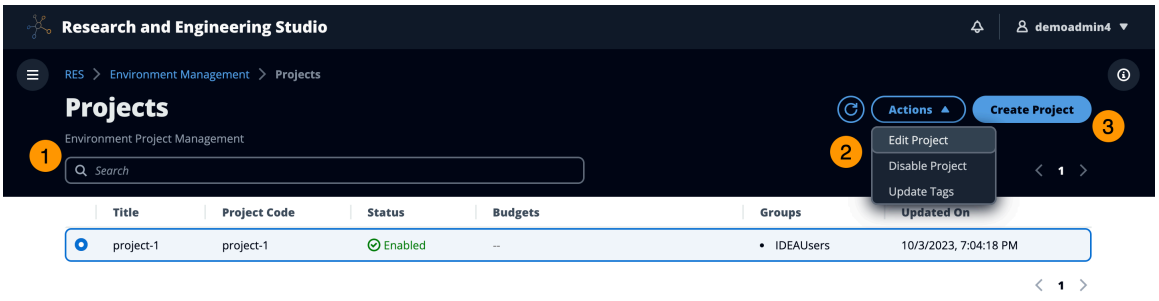
1. Recherchez des groupes d'utilisateurs.
2. Lorsqu'un groupe d'utilisateurs est sélectionné, utilisez le menu Actions pour activer ou désactiver un groupe.
3. Lorsqu'un groupe d'utilisateurs est sélectionné, vous pouvez développer le volet Utilisateurs en bas de l'écran pour afficher les utilisateurs du groupe.

Projets

Les projets constituent une limite pour les bureaux virtuels, les équipes et les budgets. Lorsque vous créez un projet, vous définissez ses paramètres, tels que le nom, la description et la configuration de l'environnement. Les projets incluent généralement un ou plusieurs environnements, qui peuvent être personnalisés pour répondre aux exigences spécifiques de votre projet, telles que le type et la taille des ressources informatiques, la pile logicielle et la configuration réseau.

Rubriques

Afficher les projets



Le tableau de bord des projets fournit une liste des projets mis à votre disposition. Depuis le tableau de bord des projets, vous pouvez :

1. Vous pouvez utiliser le champ de recherche pour trouver des projets.
2. Lorsqu'un projet est sélectionné, vous pouvez utiliser le menu Actions pour :
   a. Modifier un projet
   b. Activer ou désactiver un projet
   c. Mettre à jour les balises du projet
   d. Supprime un projet.
3. Vous pouvez choisir Create Project pour créer un nouveau projet.

Création d'un projet

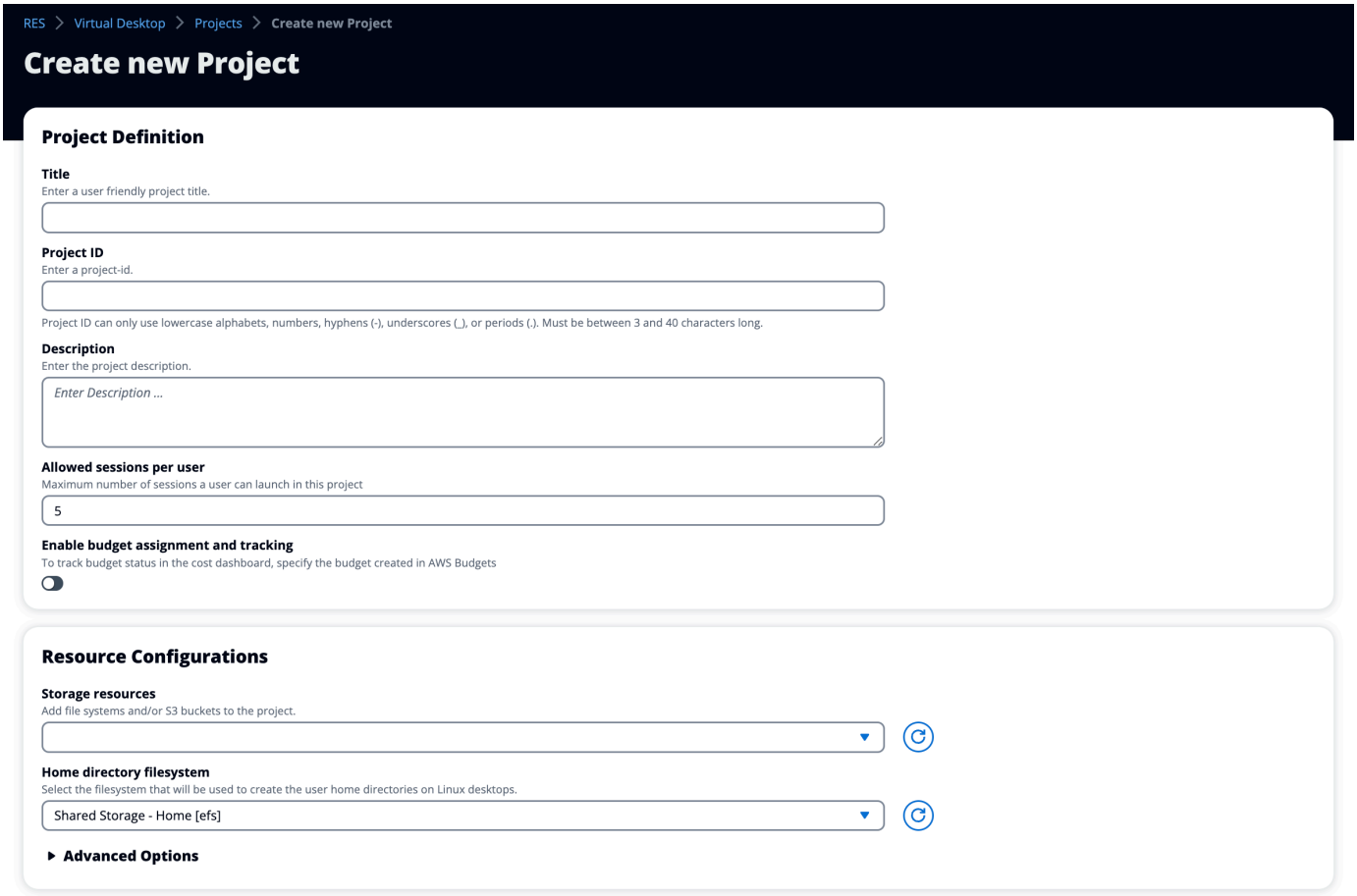
1. Choisissez Create Project (Créer un projet).
2. Entrez les détails du projet.

   L'ID de projet est une balise de ressource qui peut être utilisée pour suivre la répartition des coûts dans AWS Cost Explorer Service. Pour plus d'informations, consultez la section Activation des balises de répartition des coûts définies par l'utilisateur.

   > **Important**
   >
   > L'ID du projet ne peut pas être modifié après sa création.

   Pour plus d'informations sur les options avancées, consultezAjouter un modèle de lancement.
3. (Facultatif) Activez les budgets pour le projet. Pour plus d'informations sur les budgets, voirSurveillance et contrôle des coûts.
4. Le système de fichiers du répertoire de base peut utiliser le système de fichiers personnel partagé (par défaut), EFS, FSx pour le stockage de volumes Lustre, FSx NetApp ONTAP ou EBS.

   Il est important de noter que le système de fichiers d'accueil partagé, EFS, FSx pour Lustre et FSx NetApp ONTAP peut être partagé entre plusieurs projets et. VDIs Cependant, l'option de stockage en volume EBS exigera que chaque VDI de ce projet possède son propre répertoire personnel qui n'est pas partagé entre VDIs d'autres projets.



5. Attribuez aux and/or groupes d'utilisateurs le rôle approprié (« Membre du projet » ou « Propriétaire du projet »). Découvrez Profils d'autorisations par défaut les actions que chaque rôle peut entreprendre.
6. Sélectionnez Soumettre.

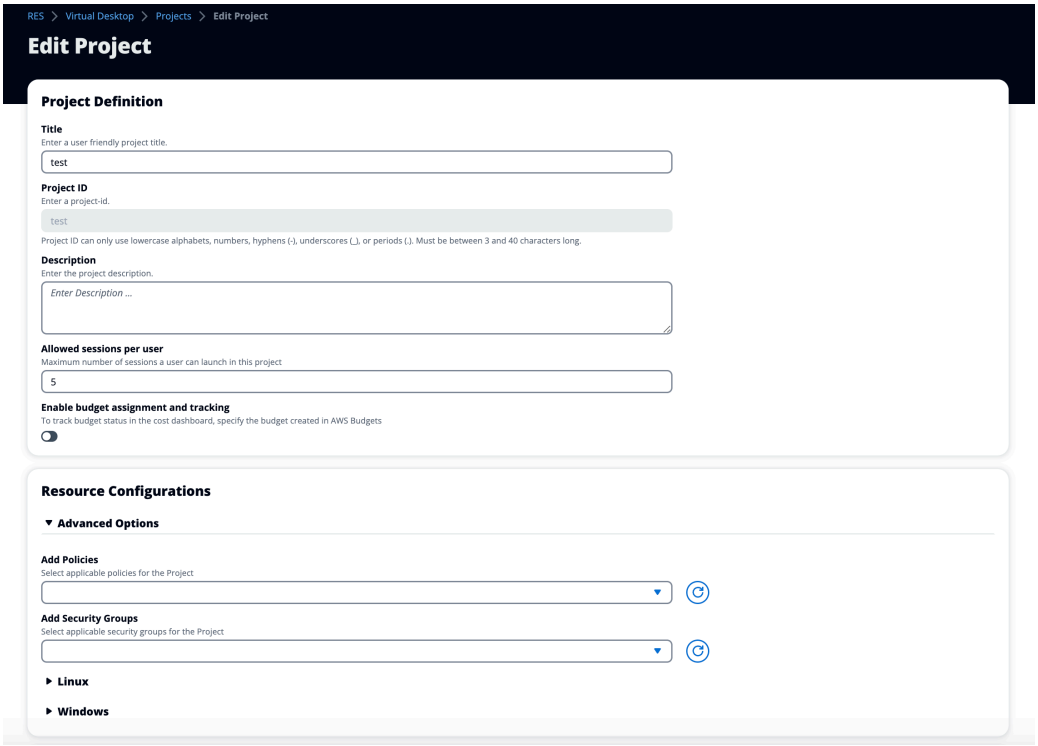
Modifier un projet

1. Sélectionnez un projet dans la liste des projets.
2. Dans le menu Actions, choisissez Modifier le projet.
3. Entrez vos mises à jour.

   Si vous avez l'intention d'activer les budgets, consultez Surveillance et contrôle des coûts pour plus d'informations. Lorsque vous choisissez un budget pour le projet, le chargement des options de la liste déroulante du budget peut prendre quelques secondes. Si vous ne voyez pas le budget que vous venez de créer, veuillez sélectionner le bouton d'actualisation à côté de la liste déroulante.

Pour plus d'informations sur les options avancées, consultezAjouter un modèle de lancement.

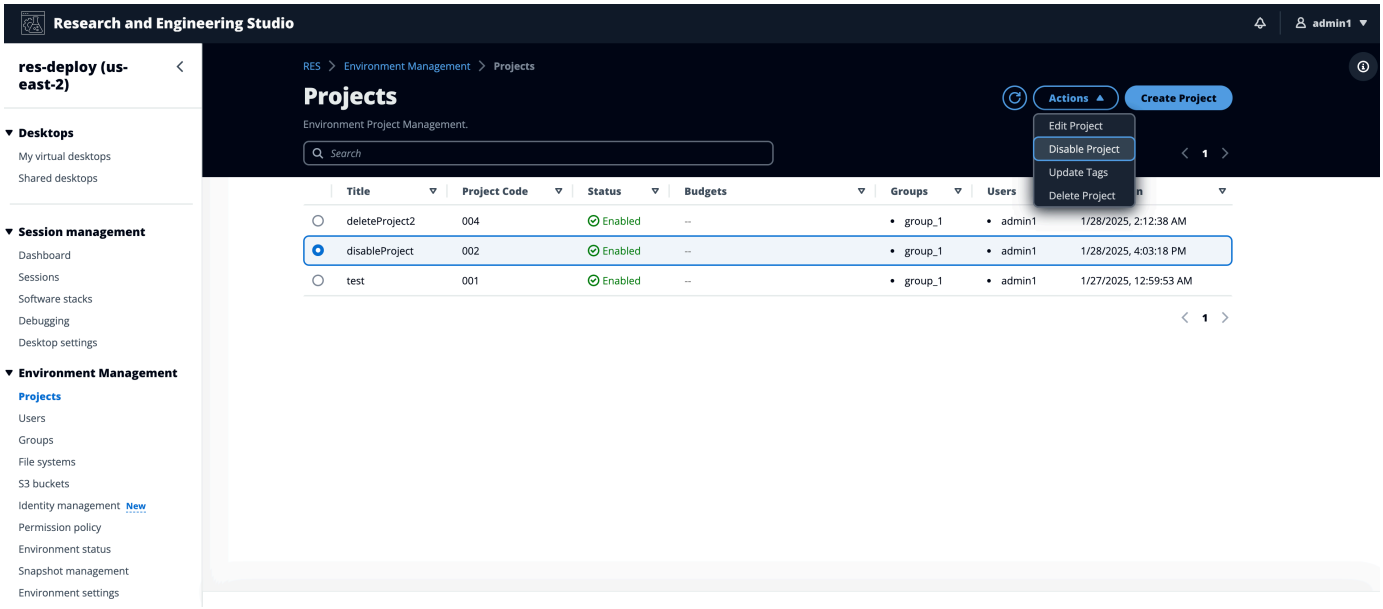
4. Sélectionnez Soumettre.



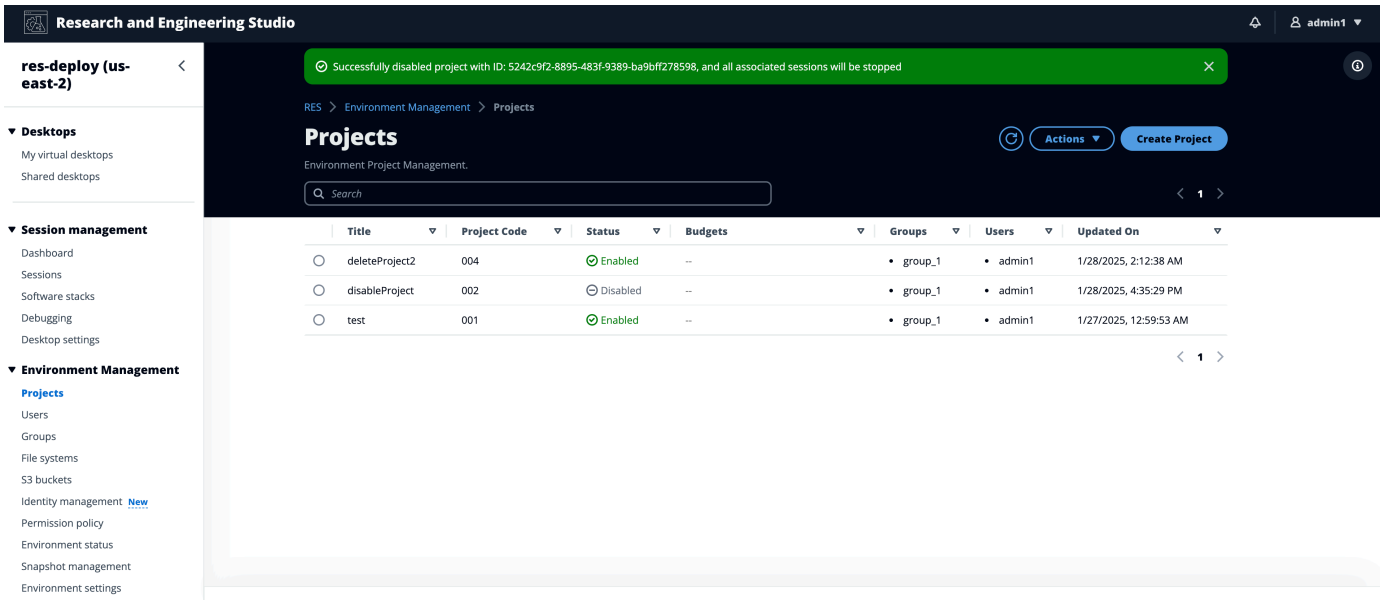
Désactiver un projet

Pour désactiver un projet, procédez comme suit :

1. Sélectionnez un projet dans la liste des projets.
2. Dans le menu Actions, choisissez Désactiver le projet.



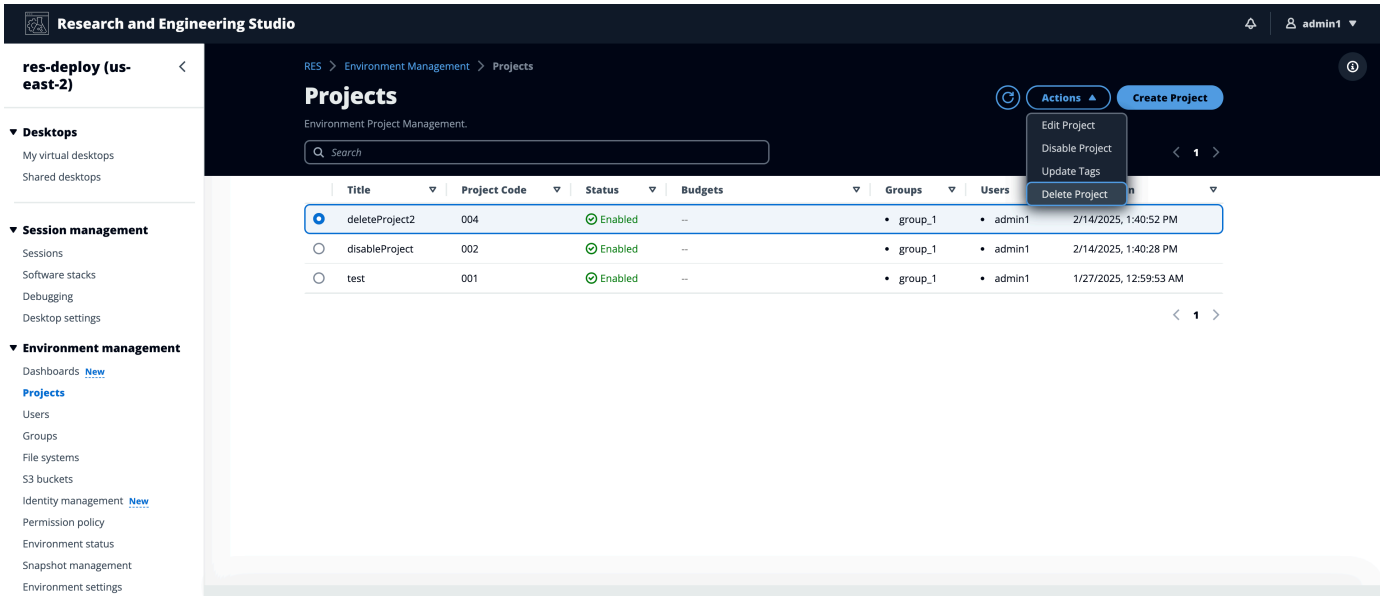
3. Si un projet est désactivé, toutes les sessions VDI associées à ce projet sont arrêtées. Ces sessions ne peuvent pas être redémarrées tant que le projet est désactivé.



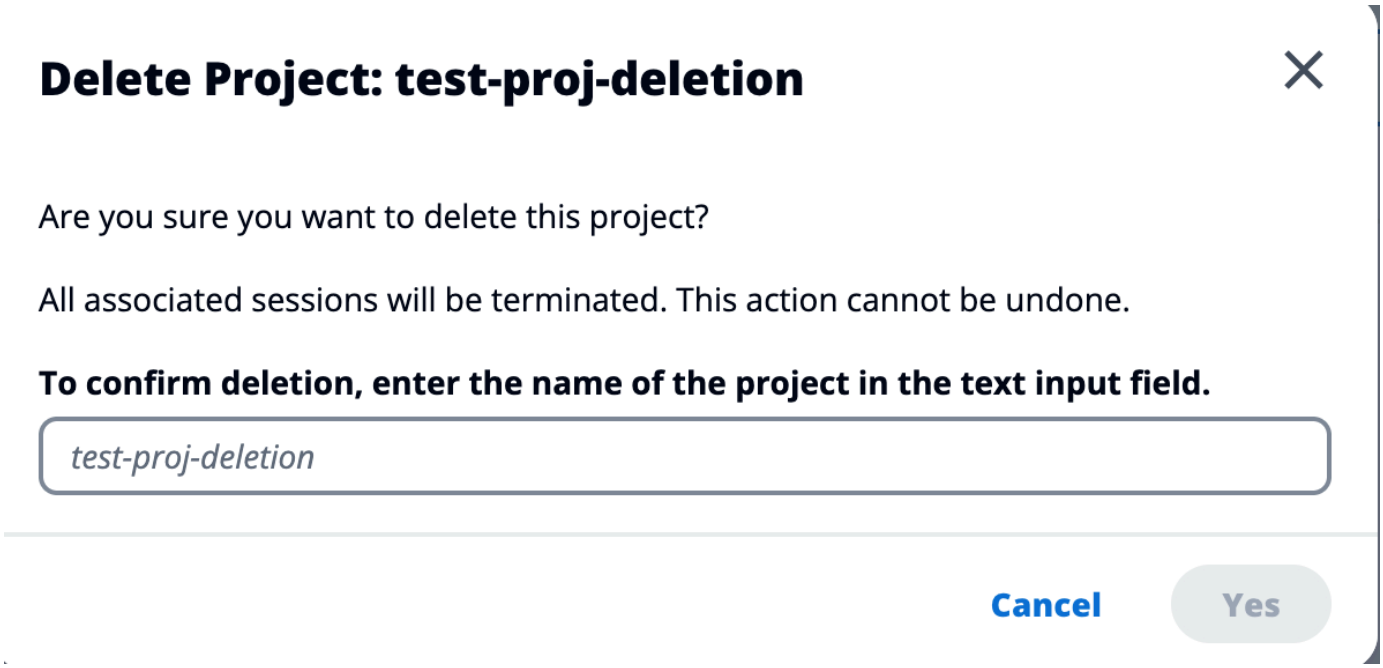
Supprime un projet.

Pour supprimer un projet, procédez comme suit :

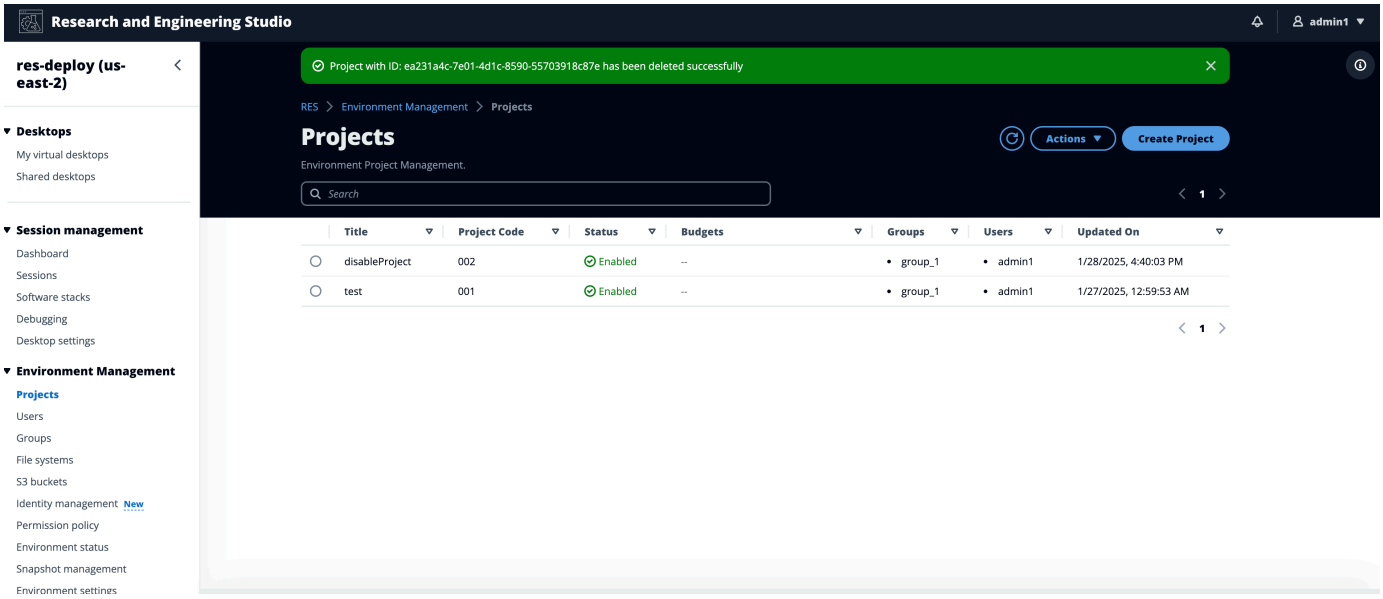
1. Sélectionnez un projet dans la liste des projets.
2. Dans le menu Actions, choisissez Supprimer le projet.



3. Une fenêtre contextuelle de confirmation s'affiche. Entrez le nom du projet, puis choisissez Oui pour le supprimer.



4. Si un projet est supprimé, toutes les sessions VDI associées à ce projet sont interrompues.



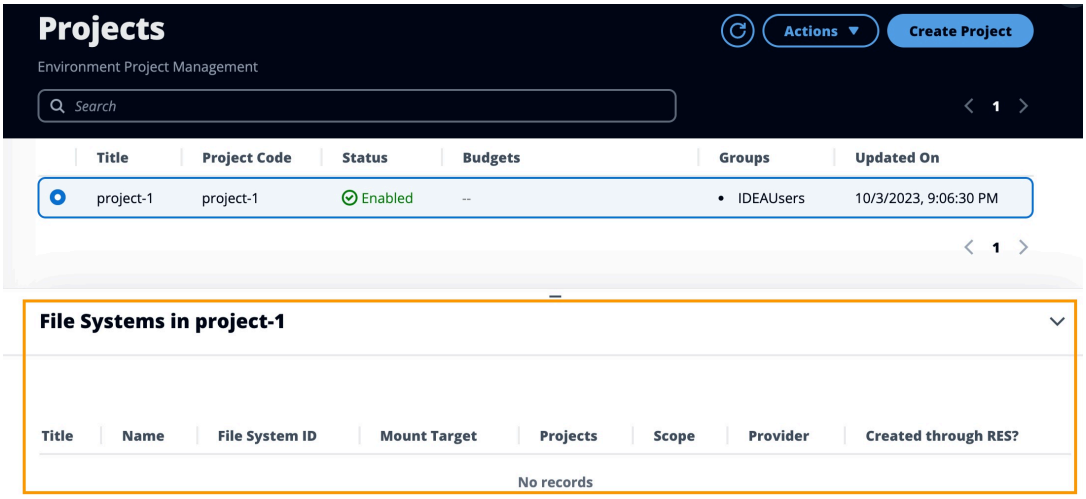
Ajouter ou supprimer des balises dans un projet

Les balises de projet attribueront des balises à toutes les instances créées dans le cadre de ce projet.

1. Sélectionnez un projet dans la liste des projets.
2. Dans le menu Actions, choisissez Mettre à jour les balises.
3. Choisissez Ajouter des balises et entrez une valeur pour Key.
4. Pour supprimer des balises, choisissez Supprimer à côté de la balise que vous souhaitez supprimer.

Afficher les systèmes de fichiers associés à un projet

Lorsqu'un projet est sélectionné, vous pouvez développer le volet Systèmes de fichiers en bas de l'écran pour afficher les systèmes de fichiers associés au projet.



Ajouter un modèle de lancement

Lorsque vous créez ou modifiez un projet, vous pouvez ajouter des modèles de lancement à l'aide des options avancées de la configuration du projet. Les modèles de lancement fournissent des configurations supplémentaires, telles que des groupes de sécurité, des politiques IAM et des scripts de lancement pour toutes les instances VDI du projet.

Ajouter des politiques

Vous pouvez ajouter une politique IAM pour contrôler l'accès VDI pour toutes les instances déployées dans le cadre de votre projet. Pour intégrer une politique, balisez-la avec la paire clé-valeur suivante :

```
res:Resource/vdi-host-policy
```

Pour plus d'informations sur les rôles IAM, consultez la section Politiques et autorisations dans IAM.

Ajout de groupes de sécurité

Vous pouvez ajouter un groupe de sécurité pour contrôler les données de sortie et d'entrée pour toutes les instances VDI de votre projet. Pour intégrer un groupe de sécurité, balisez-le avec la paire clé-valeur suivante :

```
res:Resource/vdi-security-group
```

Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôler le trafic vers vos AWS ressources à l'aide de groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Ajouter des scripts de lancement

Vous pouvez ajouter des scripts de lancement qui seront lancés sur toutes les sessions VDI de votre projet. RES prend en charge l'initiation de scripts pour Linux et Windows. Pour lancer le script, vous pouvez choisir l'une des options suivantes :

Exécuter le script au démarrage du VDI

Cette option lance le script au début d'une instance VDI avant l'exécution de toute configuration ou installation RES.

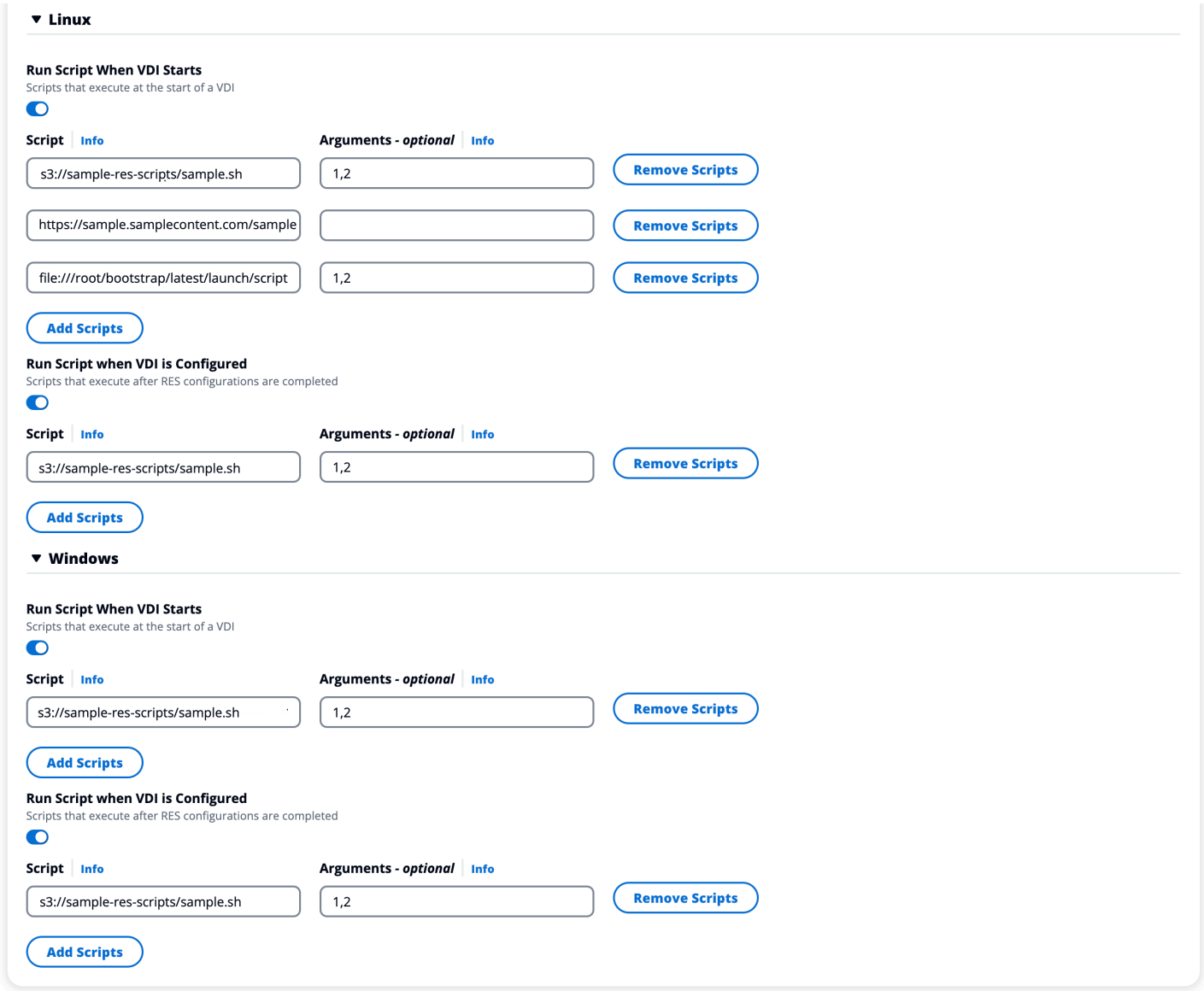
Exécuter le script lorsque le VDI est configuré

Cette option lance le script une fois les configurations RES terminées.

Les scripts prennent en charge les options suivantes :

Configuration du script	Exemple
S3 URI	s3://bucketname/script.sh
URL HTTPS	https://sample.samplecontent.com/échantillon
Fichier local	fichier :///.sh user/scripts/example

Pour Arguments, fournissez tous les arguments séparés par une virgule.



Exemple de configuration de projet

Stratégie d'autorisation

Research and Engineering Studio (RES) permet à un utilisateur administratif de créer des profils d'autorisation personnalisés qui accordent aux utilisateurs sélectionnés des autorisations supplémentaires pour gérer le projet auquel ils participent. Chaque projet est fourni avec deux profils d'autorisation par défaut, « Membre du projet » et « Propriétaire du projet », qui peuvent être personnalisés après le déploiement.

À l'heure actuelle, les administrateurs peuvent accorder deux ensembles d'autorisations à l'aide d'un profil d'autorisation :

1. Les autorisations de gestion de projet consistent à « mettre à jour l'adhésion au projet », qui permet à un utilisateur désigné d'ajouter d'autres utilisateurs et groupes à un projet ou de les en retirer, et à « mettre à jour le statut du projet », qui permet à un utilisateur désigné d'activer ou de désactiver un projet.
2. Les autorisations de gestion de session VDI consistent en « Créer une session » qui permet à un utilisateur désigné de créer une session VDI dans son projet, et « Créer/mettre fin à la session d'un autre utilisateur » qui permet à un utilisateur désigné de créer ou de terminer les sessions d'autres utilisateurs au sein d'un projet.

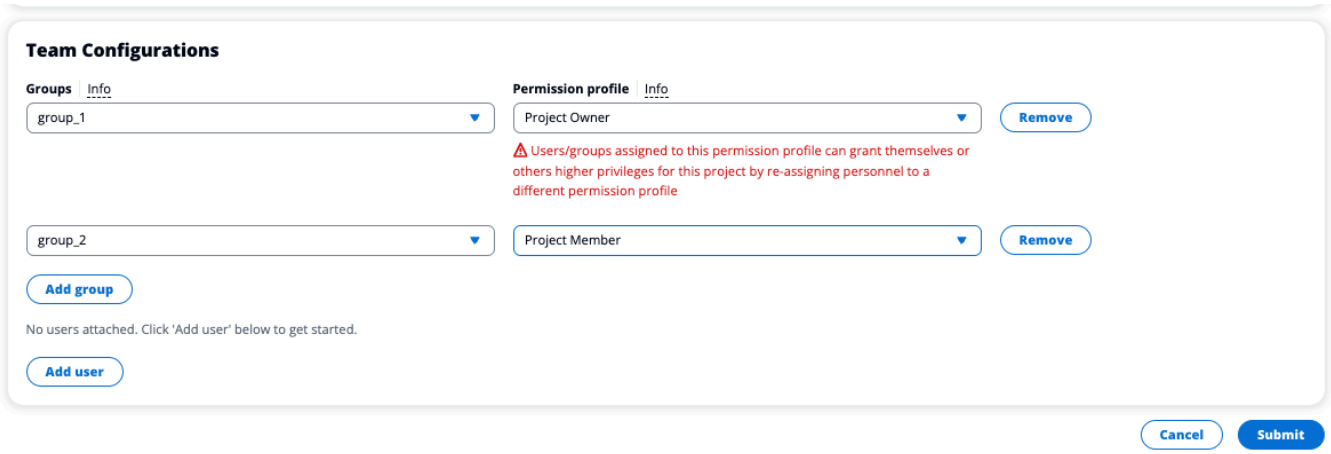
De cette façon, les administrateurs peuvent déléguer des autorisations basées sur des projets à des non-administrateurs de leur environnement.

Rubriques

Autorisations de gestion de projet

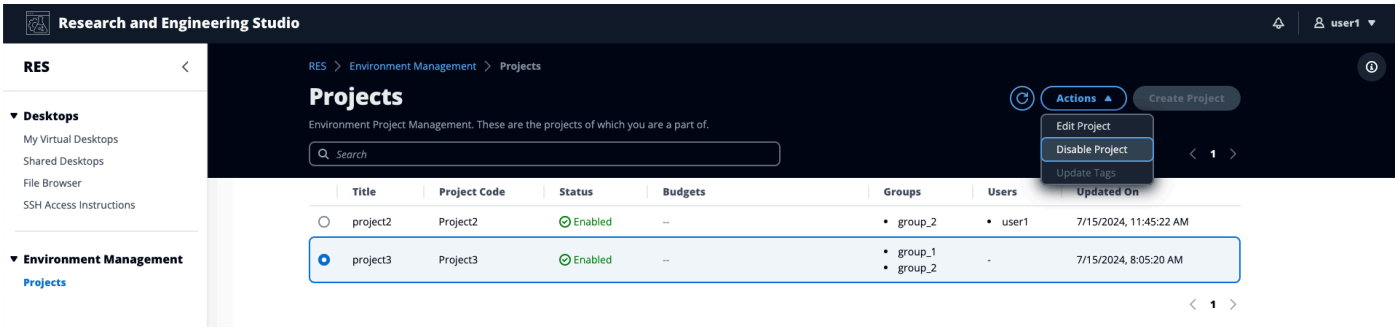
Mettre à jour l'adhésion au projet

> Cette autorisation permet aux utilisateurs non administrateurs qui l'ont accordée d'ajouter et de supprimer des utilisateurs ou des groupes d'un projet. Cela leur permet également de définir le profil d'autorisation et de décider du niveau d'accès pour tous les autres utilisateurs et groupes associés à ce projet.



Mettre à jour le statut du projet

Cette autorisation permet aux utilisateurs non administrateurs qui l'ont accordée d'activer ou de désactiver un projet à l'aide du bouton Actions de la page Projets.

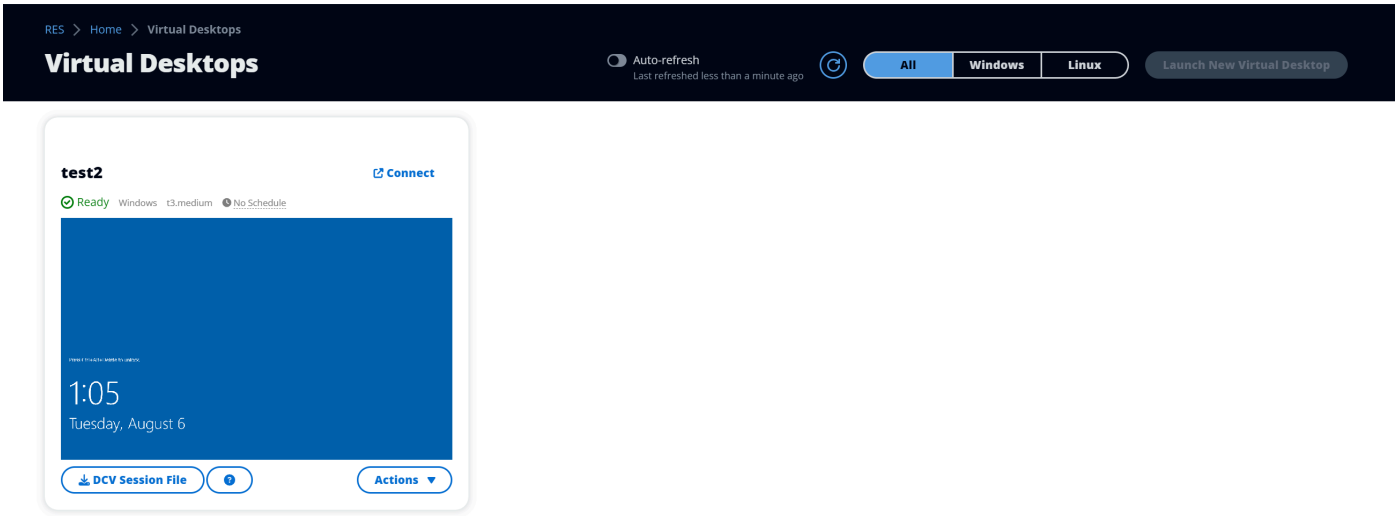


Autorisations de gestion des sessions VDI

Créer une session

Contrôle si un utilisateur est autorisé ou non à lancer sa propre session VDI depuis la page Mes bureaux virtuels. Désactivez cette option pour empêcher les utilisateurs non administrateurs de lancer leurs propres sessions VDI. Les utilisateurs peuvent toujours arrêter et terminer leurs propres sessions VDI.

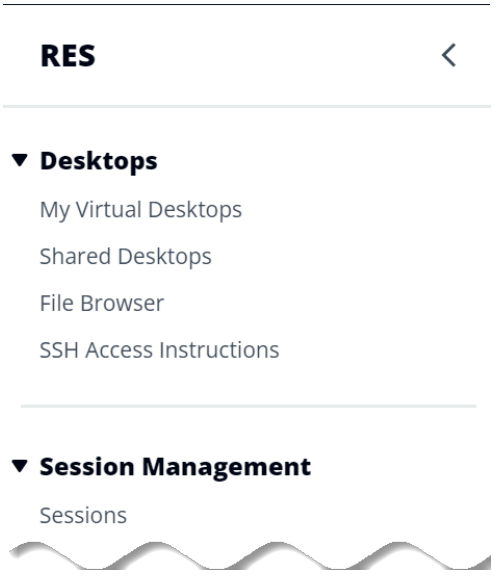
Si un utilisateur non administrateur n'est pas autorisé à créer une session, le bouton Lancer un nouveau bureau virtuel sera désactivé pour lui, comme indiqué ici :



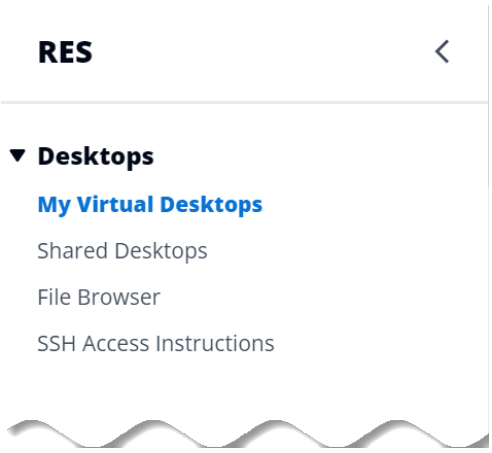
Créer ou mettre fin aux sessions des autres

Permet aux utilisateurs non administrateurs d'accéder à la page Sessions depuis le volet de navigation de gauche. Ces utilisateurs pourront lancer des sessions VDI pour d'autres utilisateurs des projets pour lesquels cette autorisation leur a été accordée.

Si un utilisateur non administrateur est autorisé à lancer des sessions pour d'autres utilisateurs, son volet de navigation de gauche affiche le lien Sessions sous Gestion des sessions, comme indiqué ici :



Si un utilisateur non administrateur n'est pas autorisé à créer des sessions pour d'autres utilisateurs, son volet de navigation de gauche n'affichera pas la gestion des sessions, comme indiqué ici :

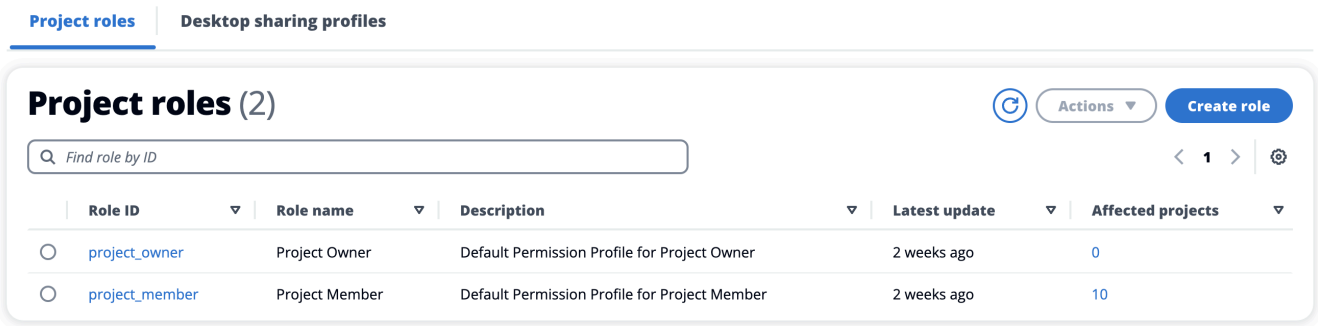


Gestion des profils d'autorisation

En tant qu'administrateur RES, vous pouvez effectuer les actions suivantes pour gérer les profils d'autorisation.

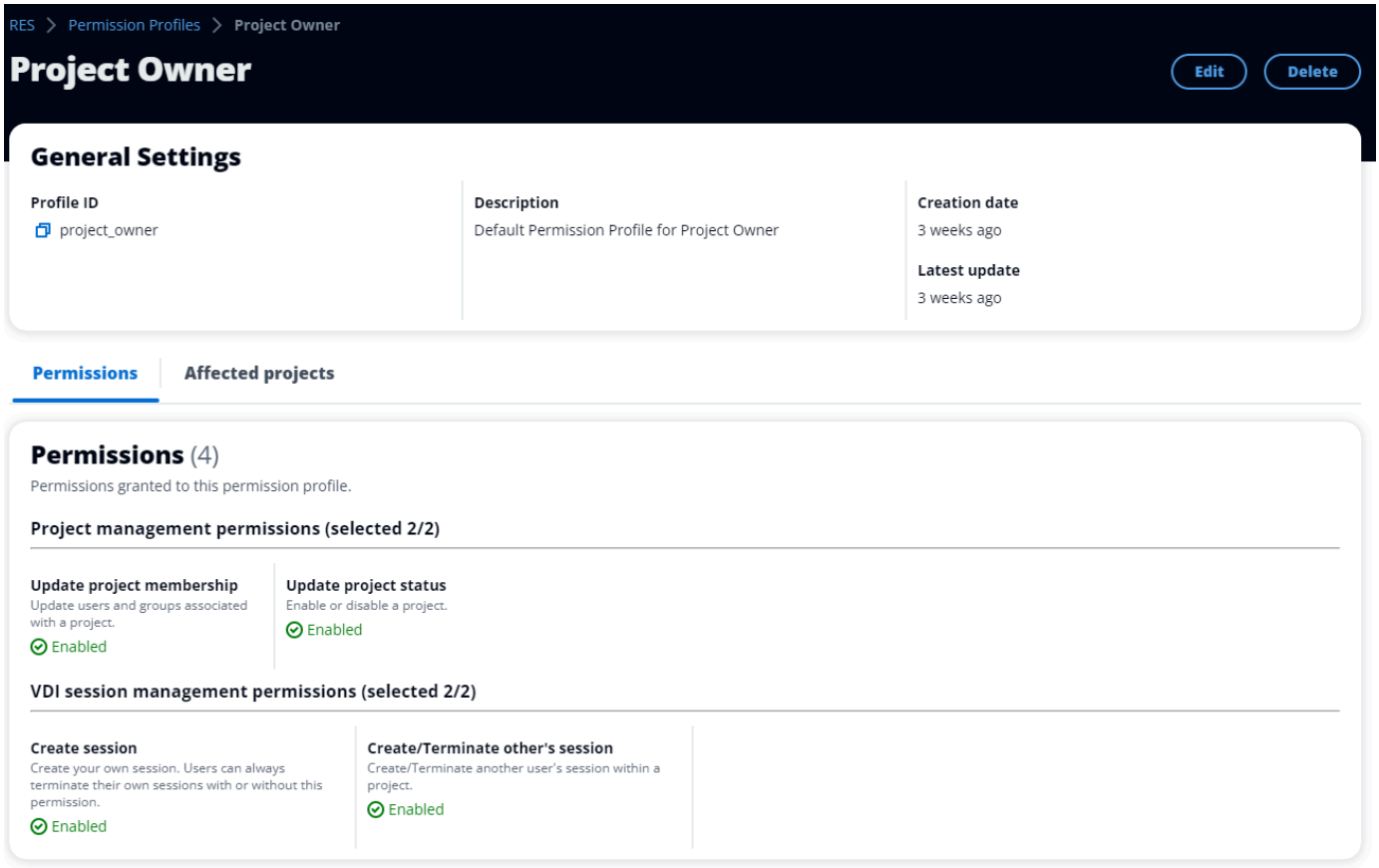
Lister les profils d'autorisation

- Sur la page de console de Research and Engineering Studio, choisissez Permission policy dans le volet de navigation de gauche. À partir de cette page, vous pouvez créer, mettre à jour, répertorier, afficher et supprimer des profils d'autorisation.

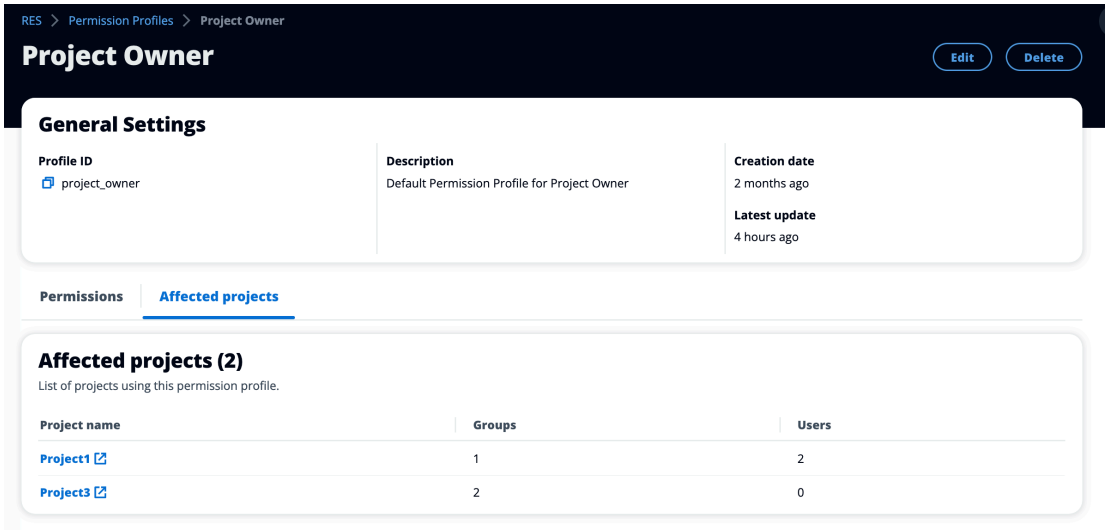


Afficher les profils d'autorisation

1. Sur la page principale des profils d'autorisation, sélectionnez le nom du profil d'autorisation que vous souhaitez consulter. Sur cette page, vous pouvez modifier ou supprimer le profil d'autorisation sélectionné.

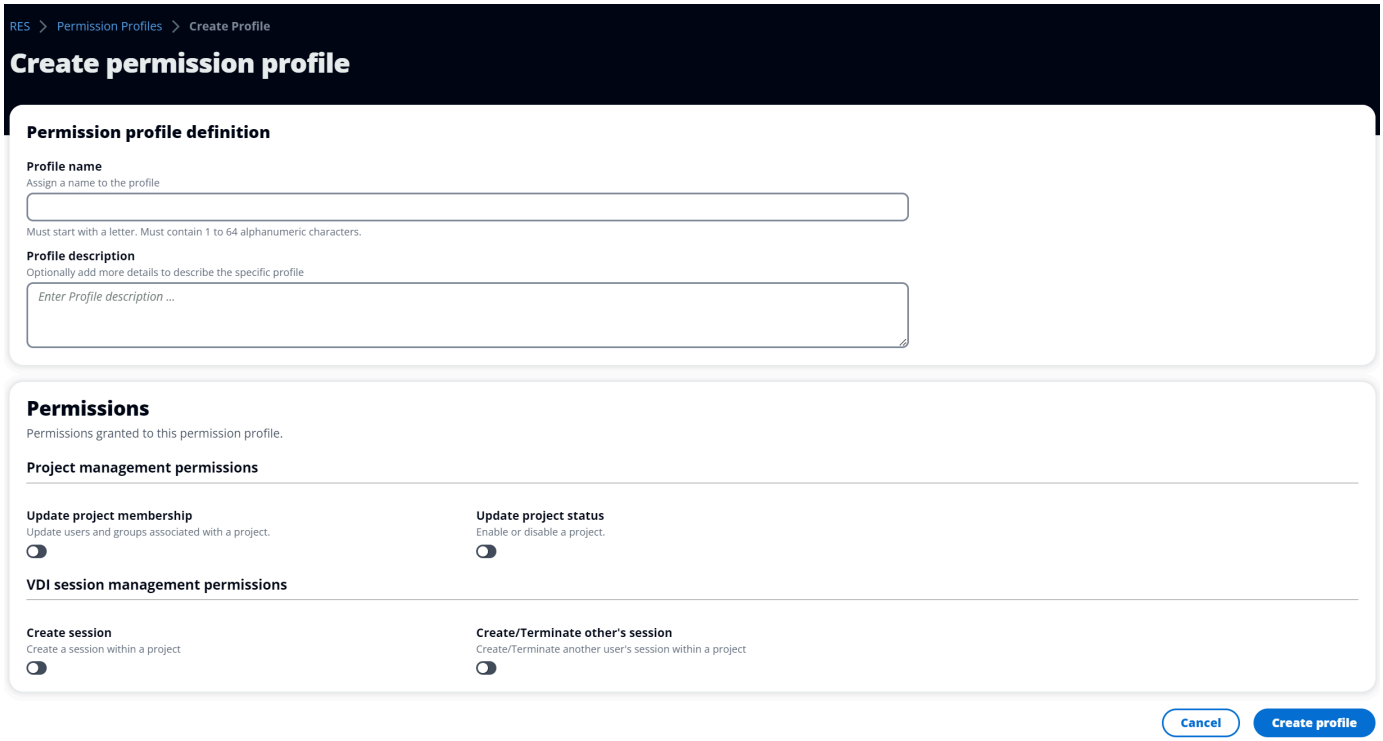


2. Sélectionnez l'onglet Projets concernés pour afficher les projets qui utilisent actuellement le profil d'autorisation.



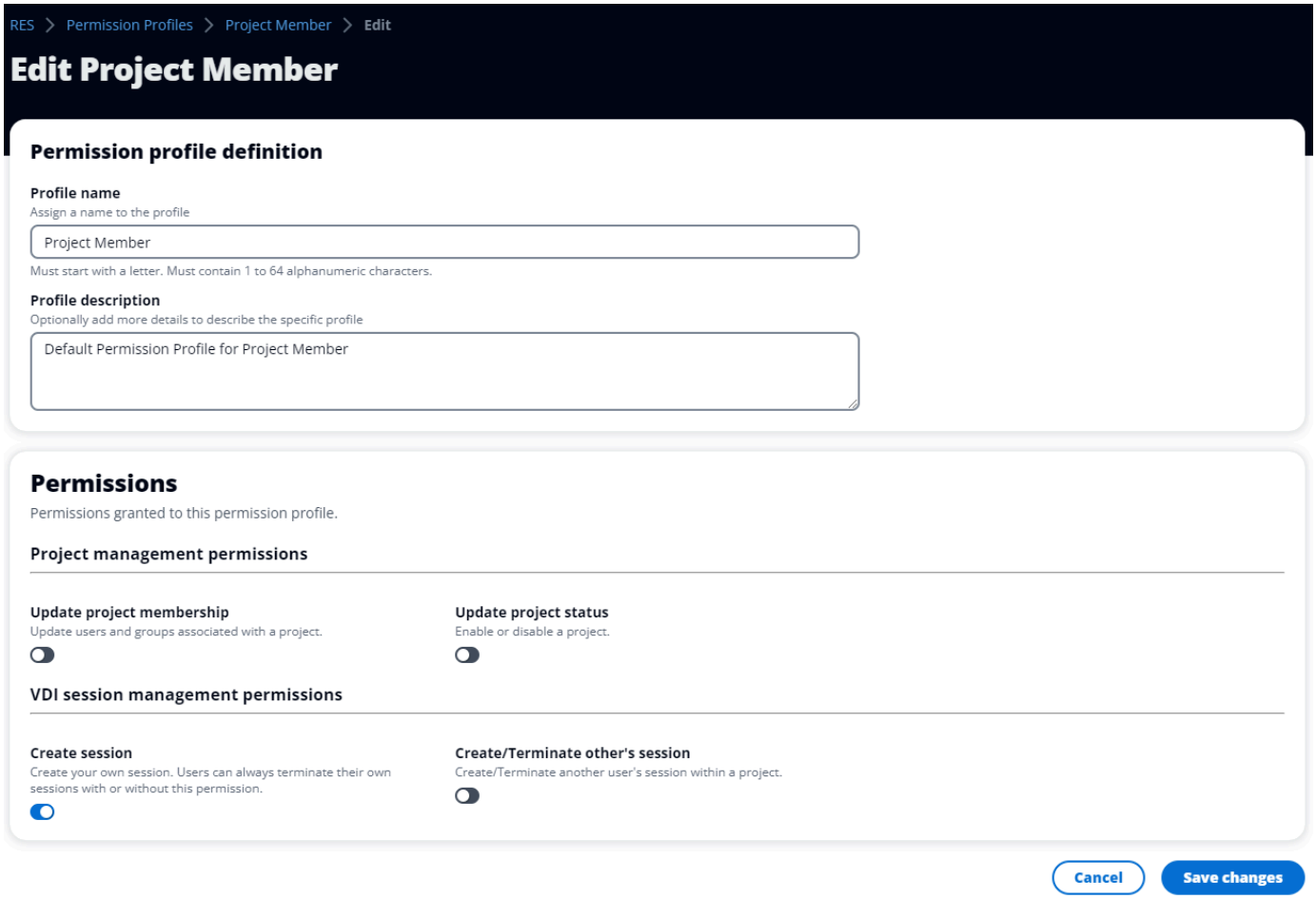
Création de profils d'autorisation

1. Sur la page principale des profils d'autorisation, choisissez Créer un profil pour créer un profil d'autorisation.
2. Entrez le nom et la description du profil d'autorisation, puis sélectionnez les autorisations à accorder aux utilisateurs ou aux groupes que vous attribuez à ce profil.



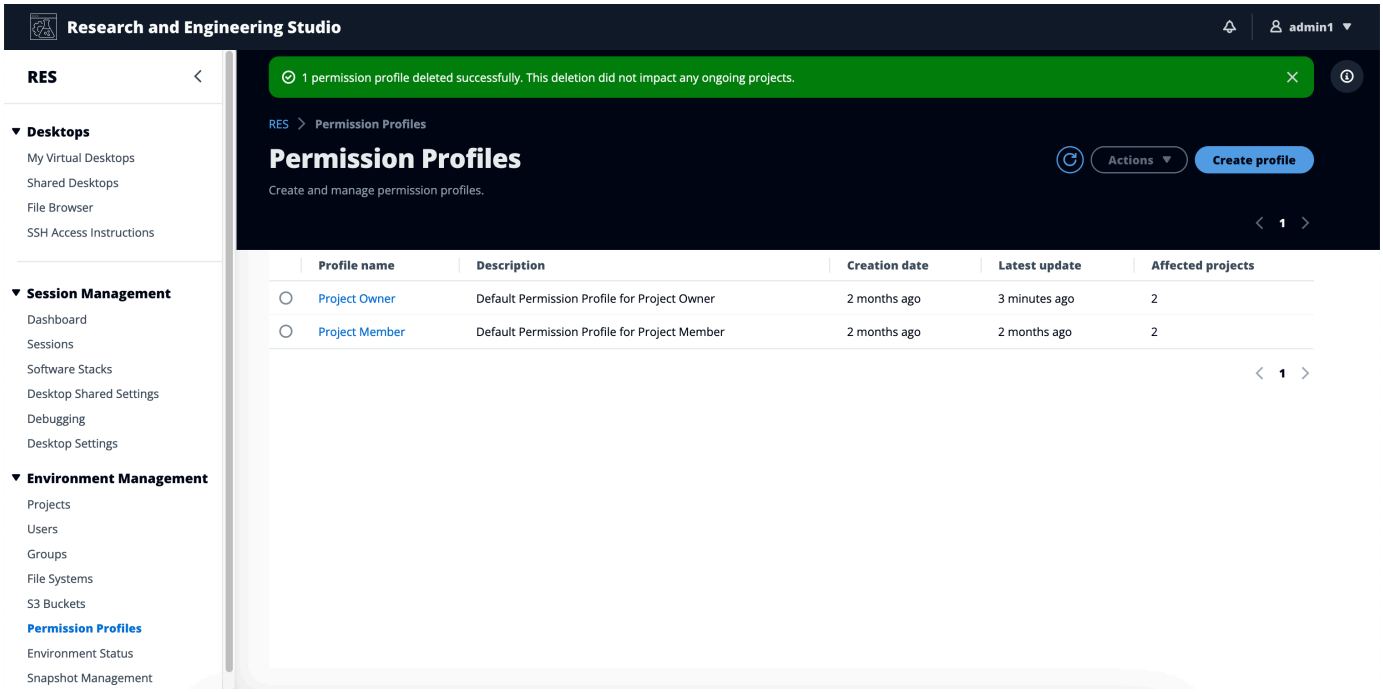
Modifier les profils d'autorisation

- Sur la page principale des profils d'autorisation, sélectionnez un profil en cliquant sur le cercle à côté de celui-ci, choisissez Actions, puis choisissez Modifier le profil pour mettre à jour ce profil d'autorisation.



Supprimer les profils d'autorisation

- Sur la page principale des profils d'autorisation, sélectionnez un profil en cliquant sur le cercle situé à côté, choisissez Actions, puis sélectionnez Supprimer le profil. Vous ne pouvez pas supprimer un profil d'autorisation utilisé par un projet existant.



Profils d'autorisations par défaut

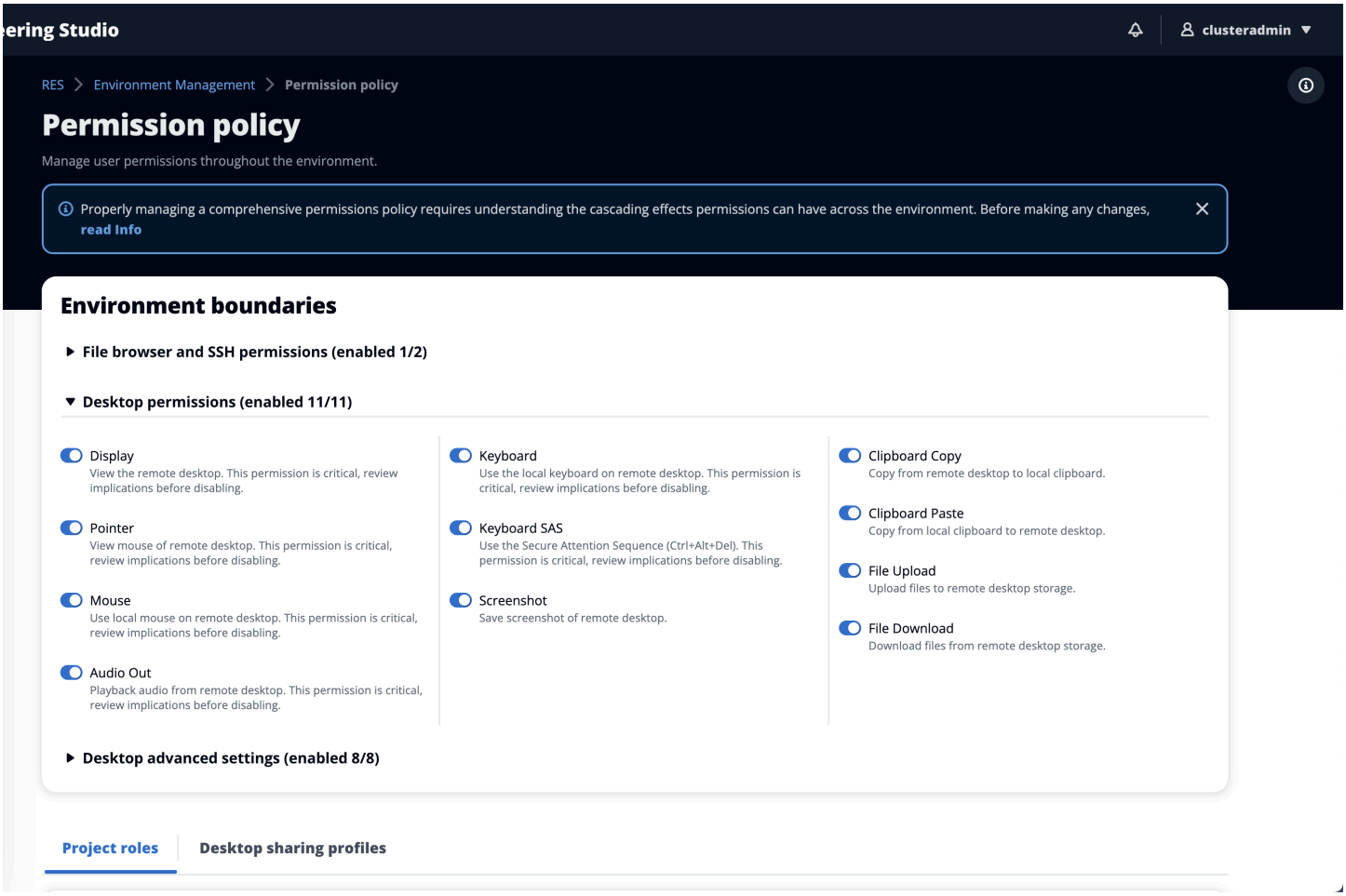
Chaque projet RES est fourni avec deux profils d'autorisation par défaut que les administrateurs globaux peuvent configurer. (En outre, les administrateurs globaux peuvent créer et modifier de nouveaux profils d'autorisation pour un projet.) Le tableau suivant indique les autorisations autorisées pour les profils d'autorisation par défaut, « Membre du projet » et « Propriétaire du projet ». Les profils d'autorisation, et les autorisations qu'ils accordent pour sélectionner les utilisateurs d'un projet, ne s'appliquent qu'au projet auquel ils appartiennent ; les administrateurs globaux sont des super utilisateurs qui disposent de toutes les autorisations ci-dessous pour tous les projets.

Permissions	Description	Membre du projet	Propriétaire du projet	
Créer une session	Créez votre propre session. Les utilisateurs peuvent toujours arrêter et terminer leurs propres sessions avec ou sans	X	X	

Permissions	Description	Membre du projet	Propriétaire du projet	
	cette autorisation.			
Créer/mettre fin aux sessions des autres	Créez ou mettez fin à la session d'un autre utilisateur au sein d'un projet.		X	
Mettre à jour l'adhésion au projet	Mettez à jour les utilisateurs et les groupes associés à un projet.		X	
Mettre à jour le statut du projet	Activez ou désactivez un projet.		X	

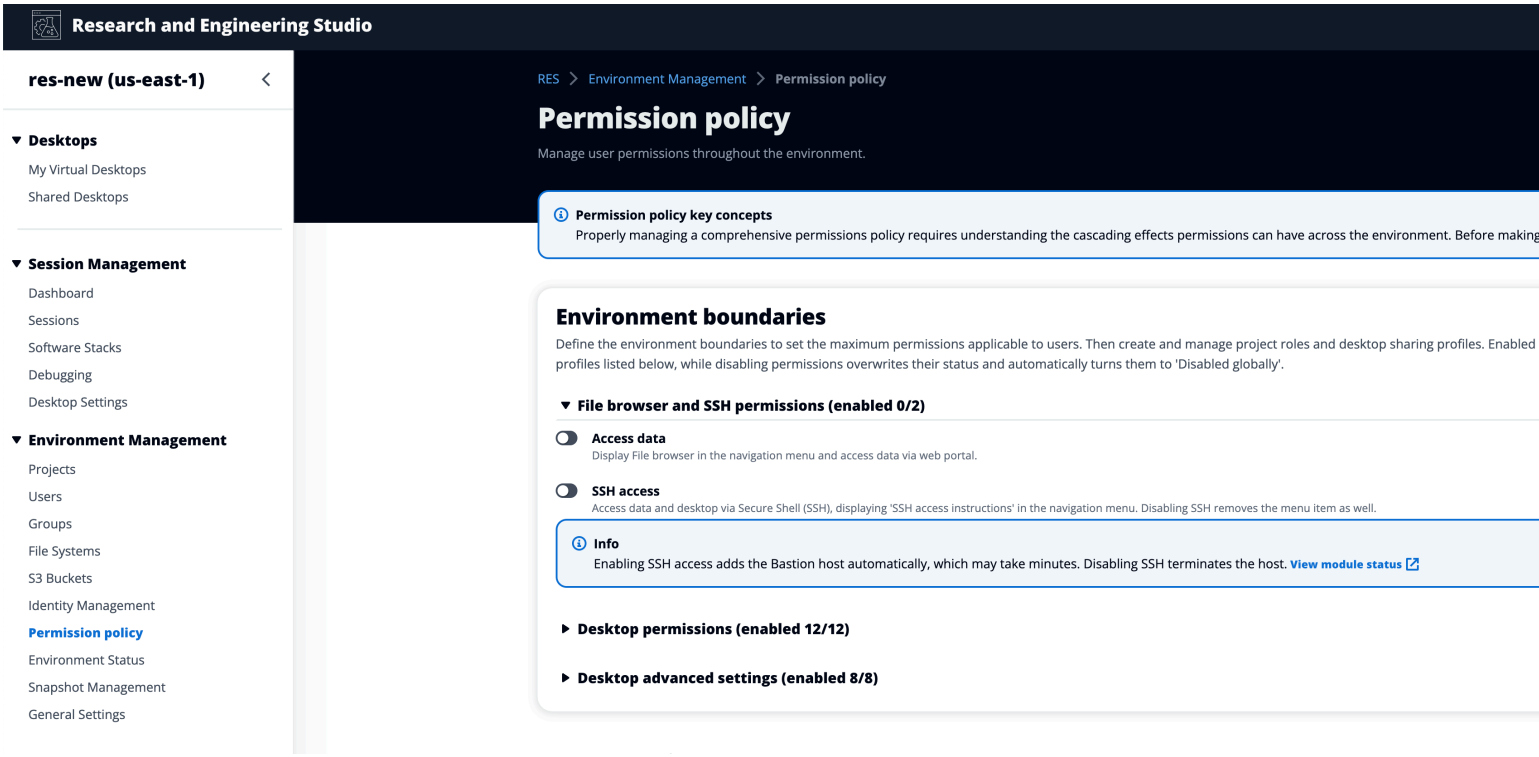
Limites de l'environnement

Les limites de l'environnement permettent aux administrateurs de Research and Engineering Studio (RES) de configurer des autorisations qui s'appliqueront globalement à tous les utilisateurs. Cela inclut les autorisations telles que le navigateur de fichiers et les autorisations SSH, les autorisations de bureau et les paramètres avancés du bureau.



Configuration de l'accès au navigateur de fichiers

Les administrateurs RES peuvent activer ou désactiver les données d'accès sous les autorisations du navigateur de fichiers. Si les données d'accès sont désactivées, les utilisateurs ne verront pas la navigation dans le navigateur de fichiers sur leur portail Web et ne pourront pas charger ou télécharger les données jointes à leur système de fichiers global. Lorsque l'accès aux données est activé, les utilisateurs ont accès à la navigation du navigateur de fichiers sur leur portail Web, ce qui leur permet de télécharger ou de télécharger les données jointes à leur système de fichiers global.



Lorsque la fonctionnalité Accès aux données est activée puis désactivée ultérieurement, les utilisateurs déjà connectés au portail Web ne pourront pas charger ou télécharger des fichiers, même s'ils se trouvent sur la page correspondante. De plus, le menu de navigation disparaît lorsqu'ils actualisent la page.

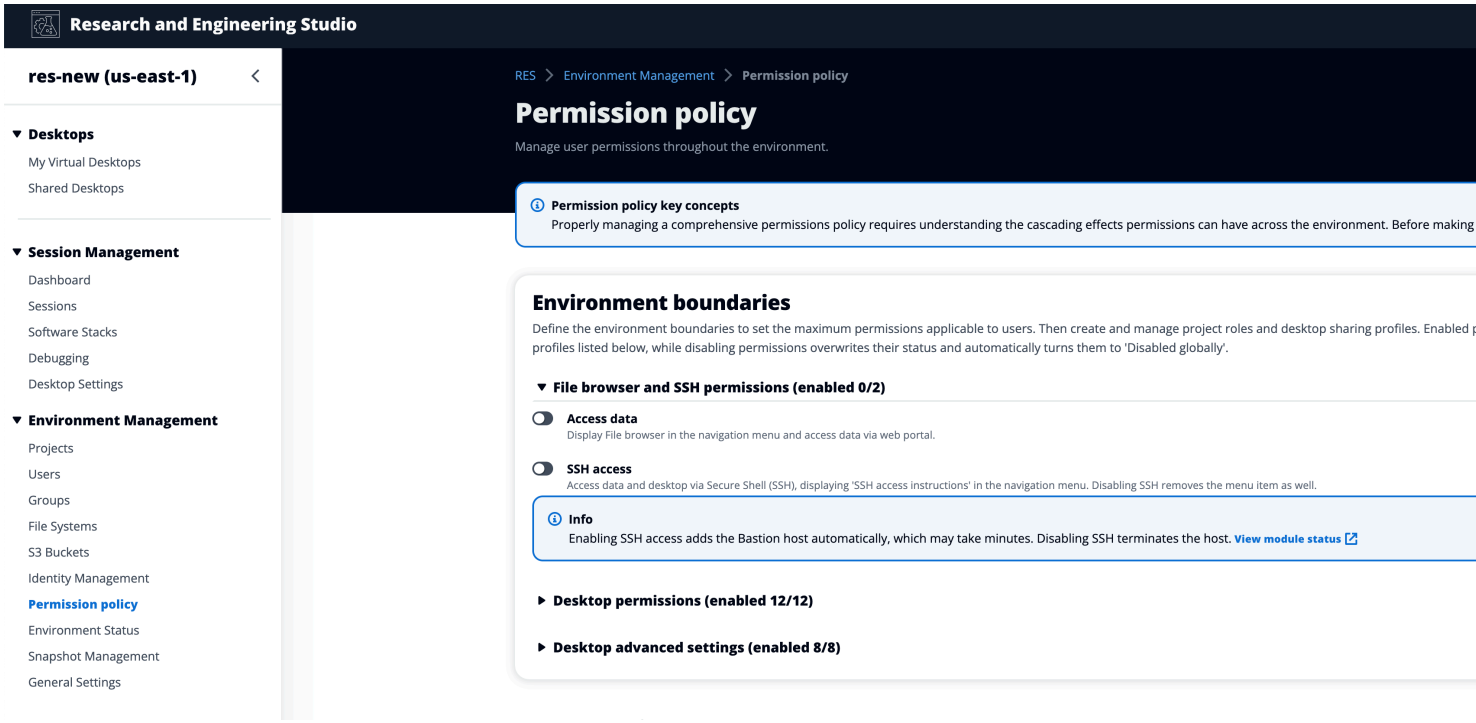
Configuration de l'accès SSH

Les administrateurs peuvent activer ou désactiver SSH pour l'environnement RES dans la section Limites de l'environnement. L'accès SSH VDIs est facilité par un hôte bastion. Lorsque vous activez cette option, RES déploie un hôte bastion et rend la page des instructions d'accès SSH visible pour les utilisateurs. Lorsque vous désactivez le bouton, RES désactive l'accès SSH, met fin à l'hôte Bastion et supprime la page d'instructions d'accès SSH pour les utilisateurs. Ce bouton est désactivé par défaut.

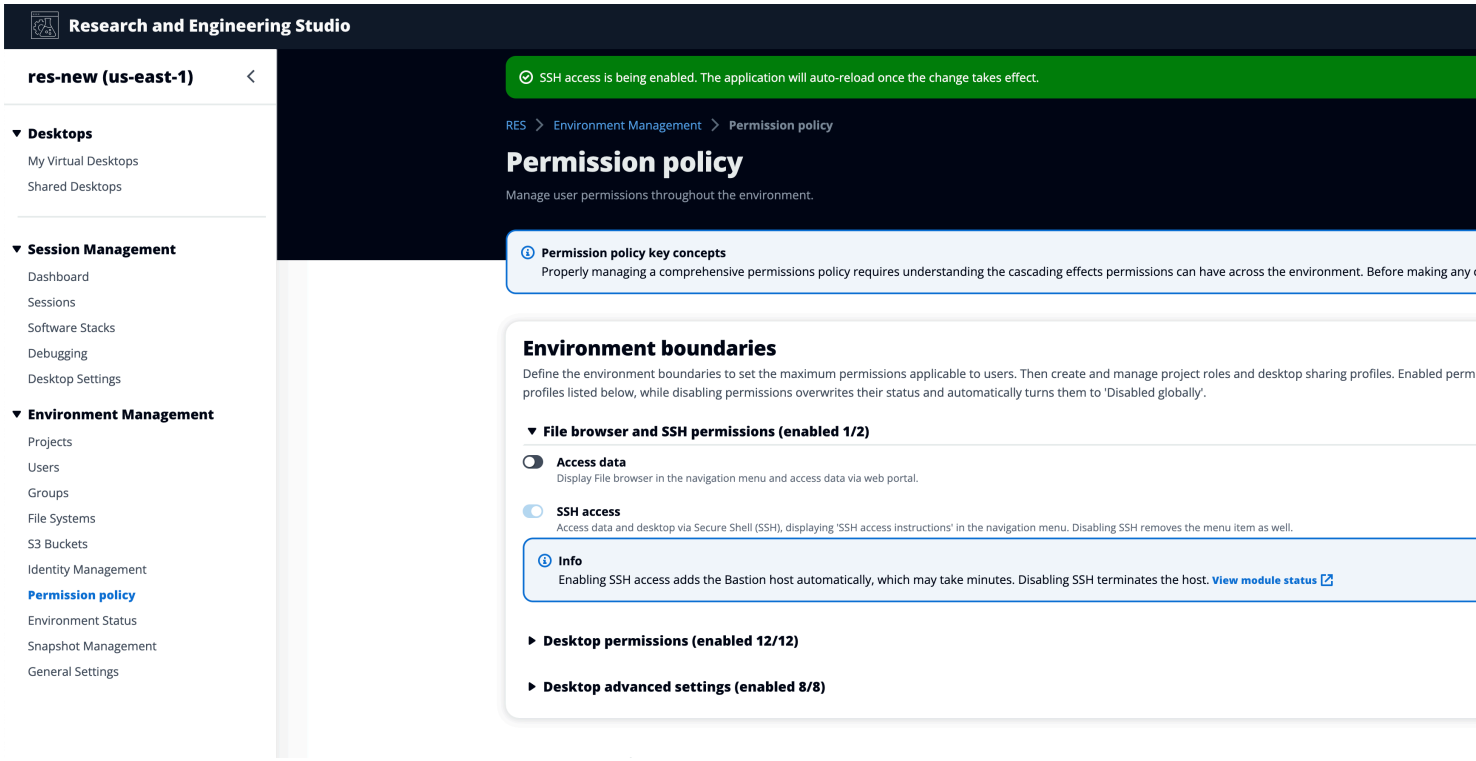
> **Note**
>
> Lorsque RES déploie un hôte bastion, il ajoute une instance Amazon `t3.medium` EC2 à votre compte. AWS Vous êtes responsable de tous les frais associés à cette instance. Consultez la page de tarification d'Amazon EC2 pour plus d'informations.

Pour activer l'accès SSH

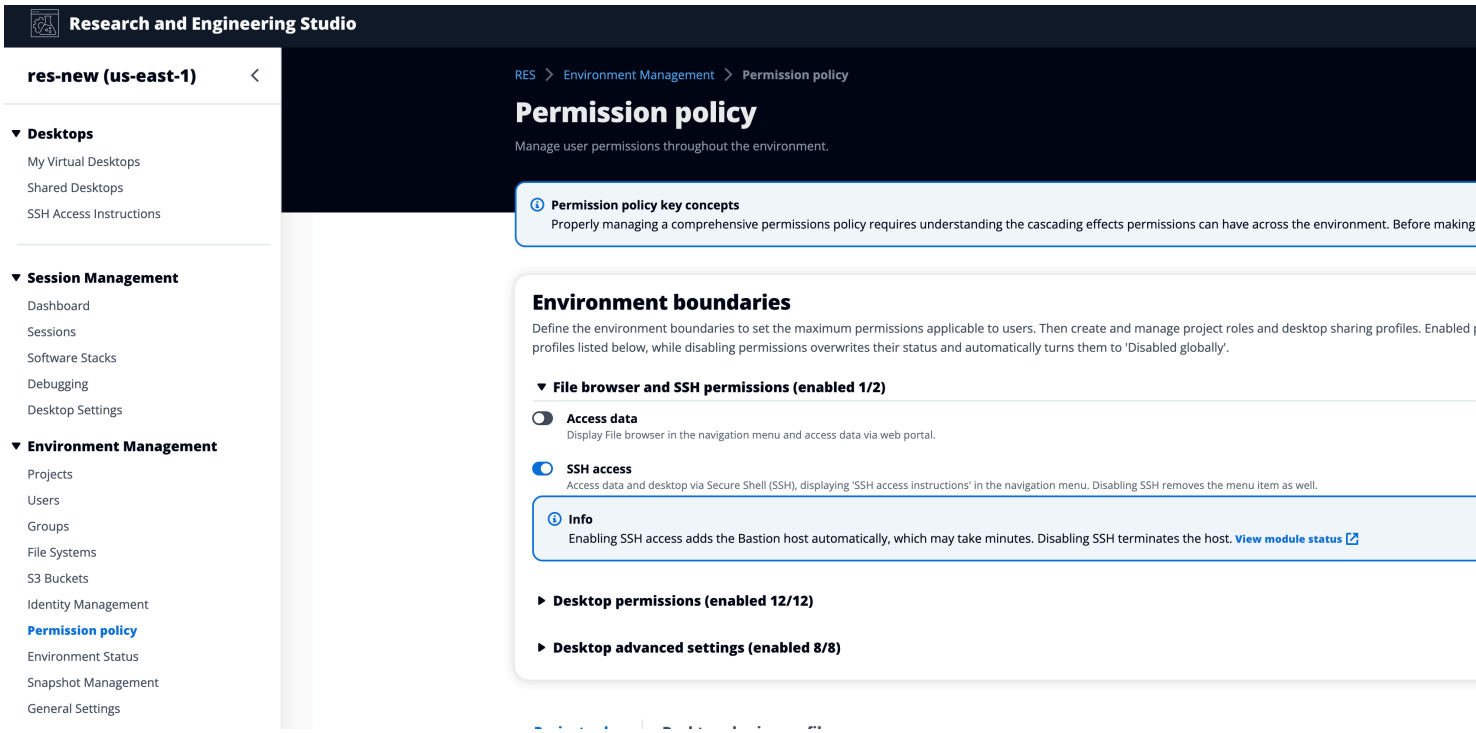
1. Dans la console RES, dans le volet de navigation de gauche, choisissez Environment Management, puis Permission Policy. Sous Limites de l'environnement, sélectionnez le bouton d'accès SSH.



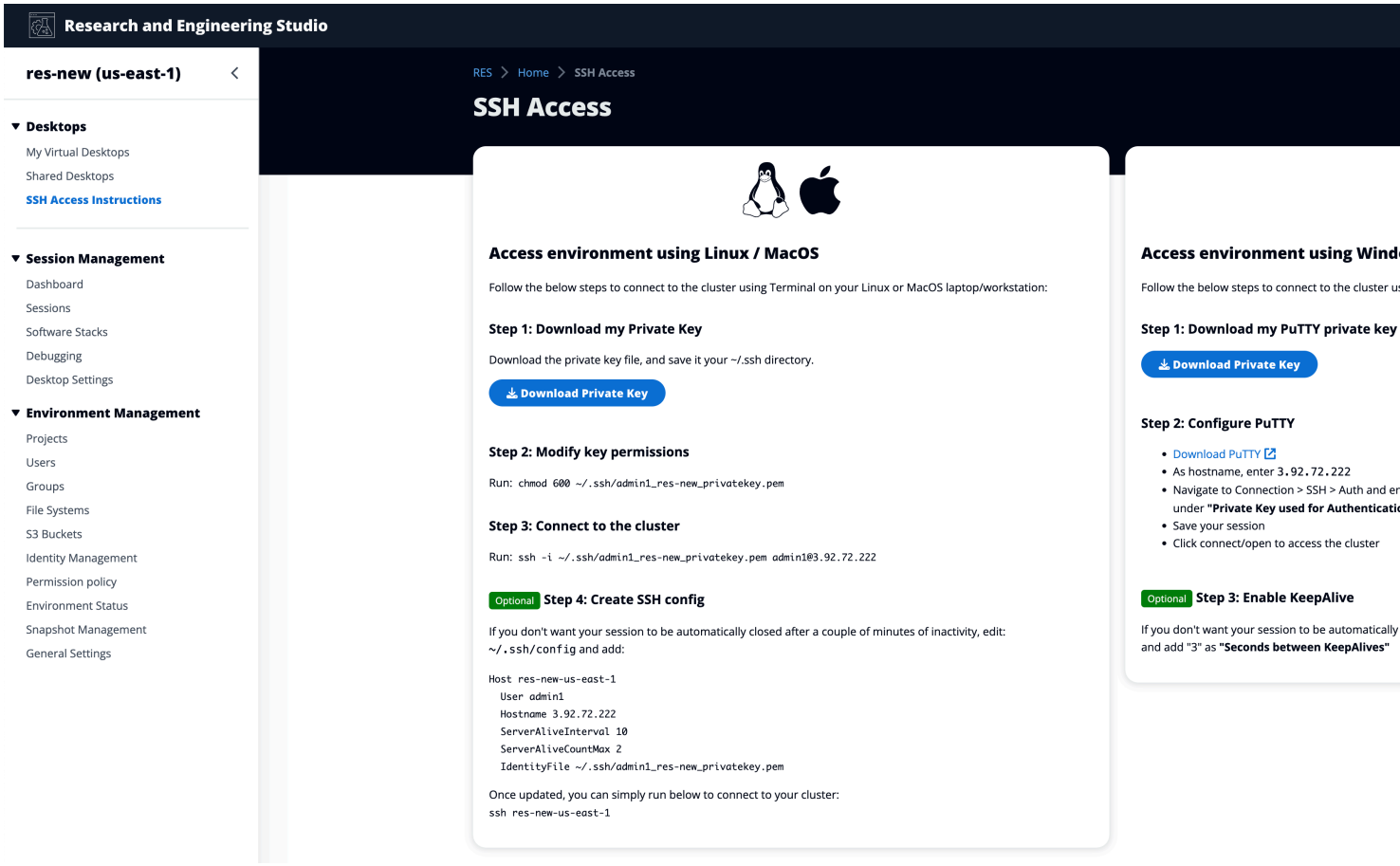
2. Attendez que l'accès SSH soit activé.



3. Une fois l'hôte Bastion ajouté, l'accès SSH est activé.

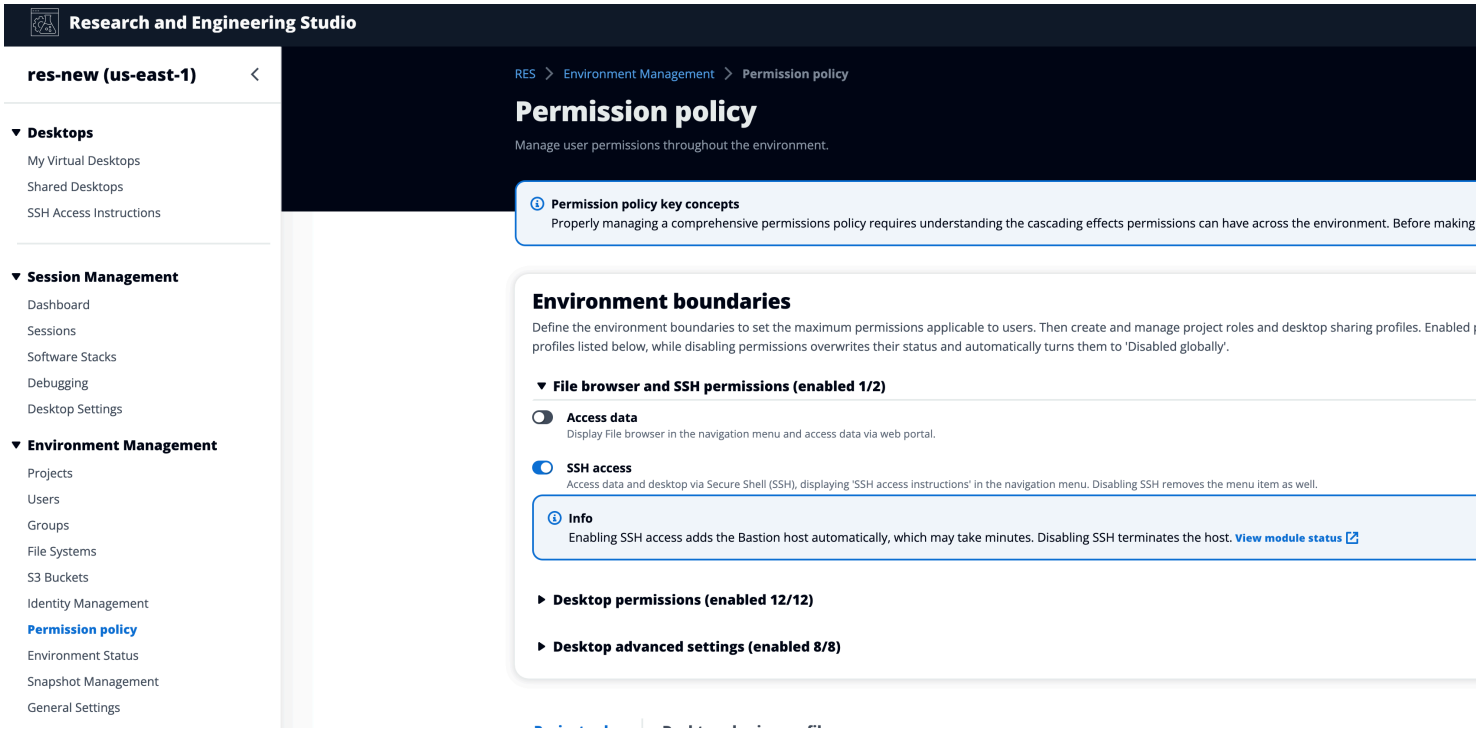


La page des instructions d'accès SSH est visible par les utilisateurs depuis le volet de navigation de gauche.

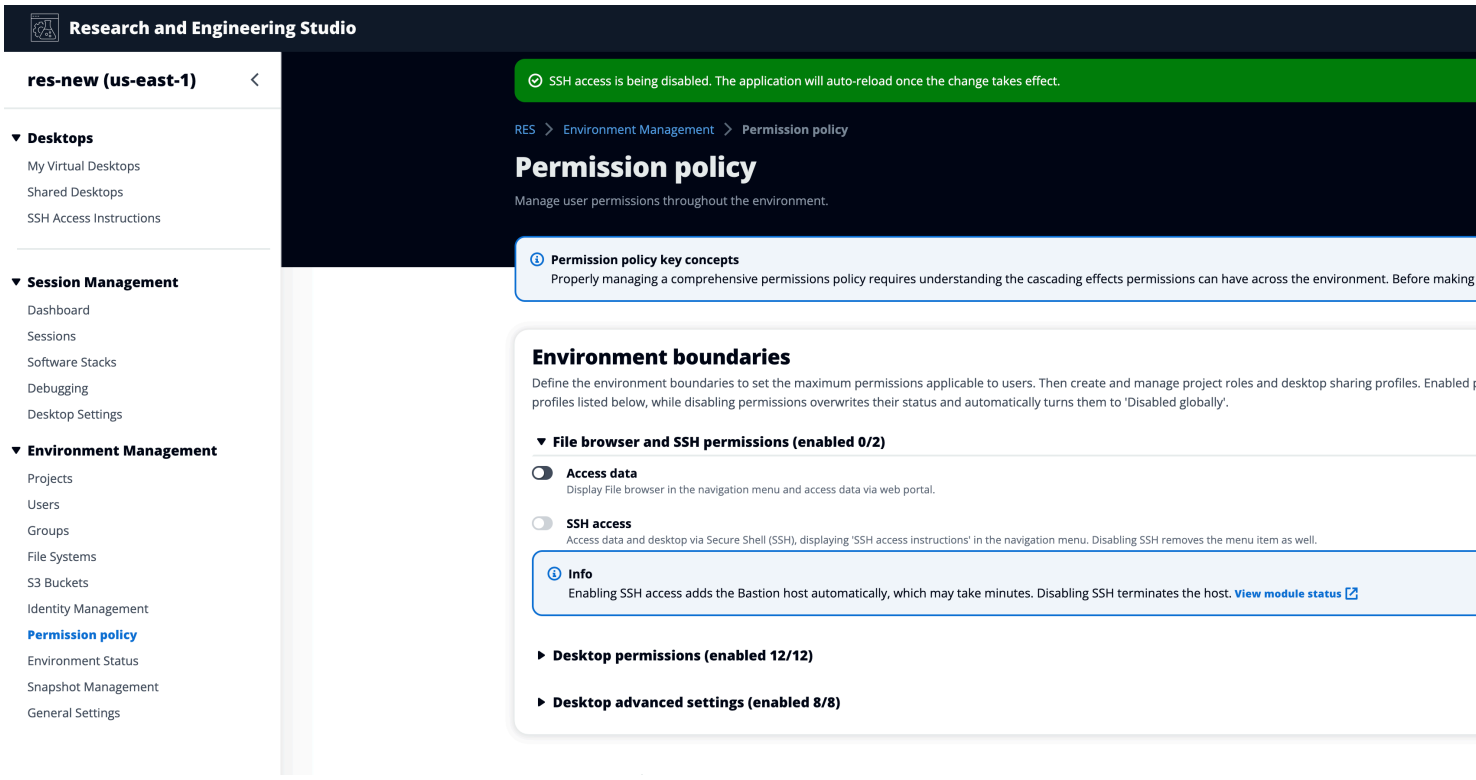


Pour désactiver l'accès SSH

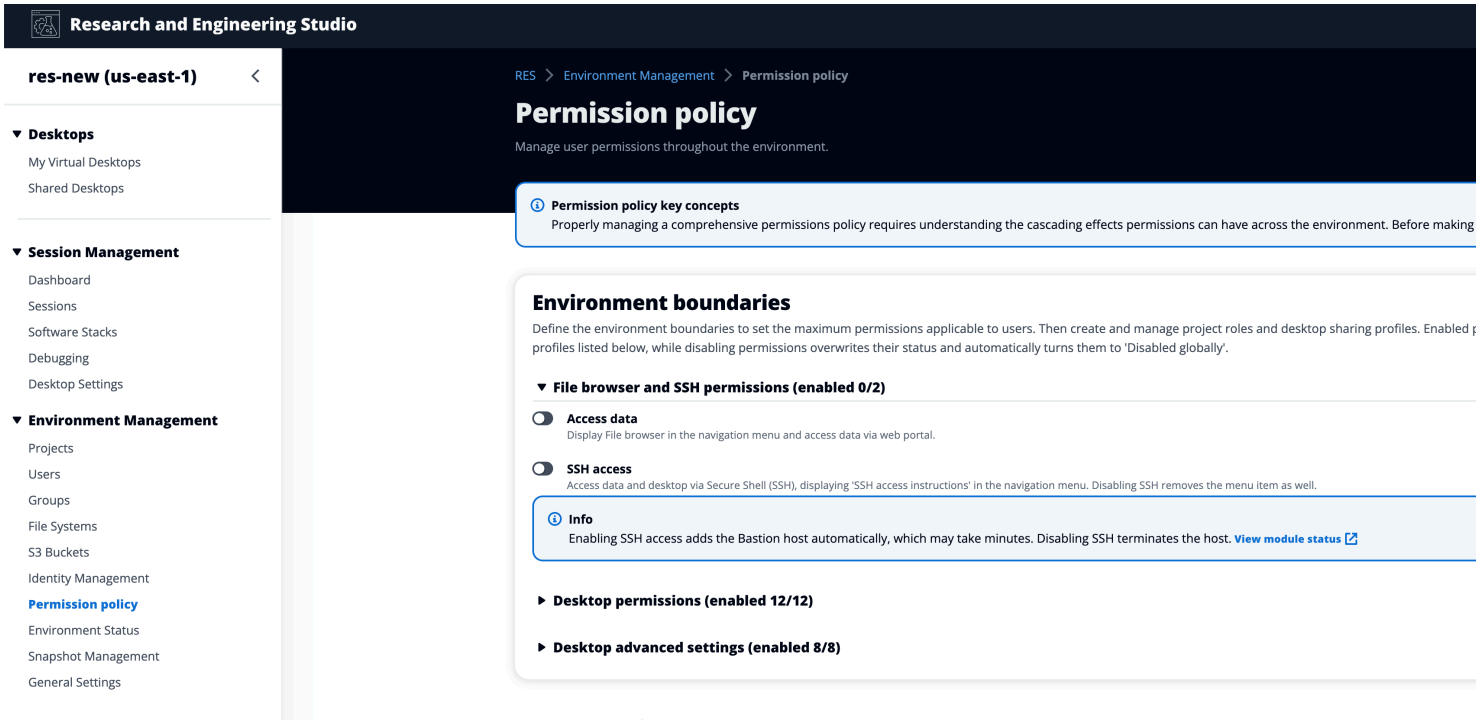
1. Dans la console RES, dans le volet de navigation de gauche, choisissez Environment Management, puis Permission Policy. Sous Limites de l'environnement, sélectionnez le bouton d'accès SSH.



2. Attendez que l'accès SSH soit désactivé.

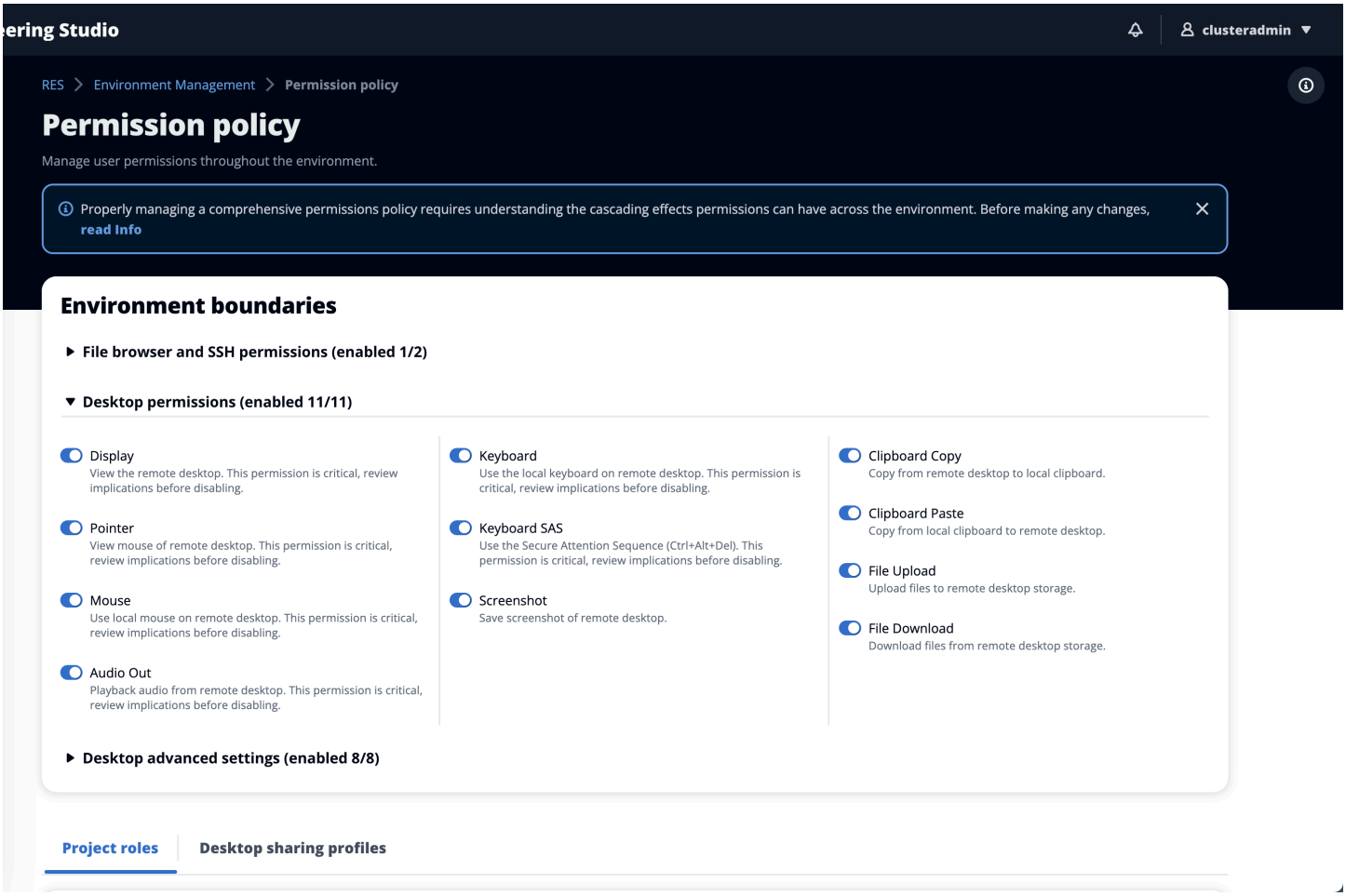


3. Une fois le processus terminé, l'accès SSH est désactivé.



Configuration des autorisations de bureau

Les administrateurs peuvent activer ou désactiver les autorisations de bureau pour gérer globalement les fonctionnalités VDI de tous les propriétaires de sessions. Toutes ces autorisations, ou un sous-ensemble, peuvent être utilisées pour créer des profils de partage de bureau qui déterminent les actions pouvant être effectuées par les utilisateurs avec lesquels un bureau est partagé. Si une autorisation de bureau est désactivée, les autorisations correspondantes seront automatiquement désactivées dans les profils de partage de bureau. Ces autorisations seront étiquetées comme « Désactivées globalement ». Même si l'administrateur réactive cette autorisation de bureau, l'autorisation dans le profil de partage de bureau restera désactivée jusqu'à ce que l'administrateur l'active manuellement.

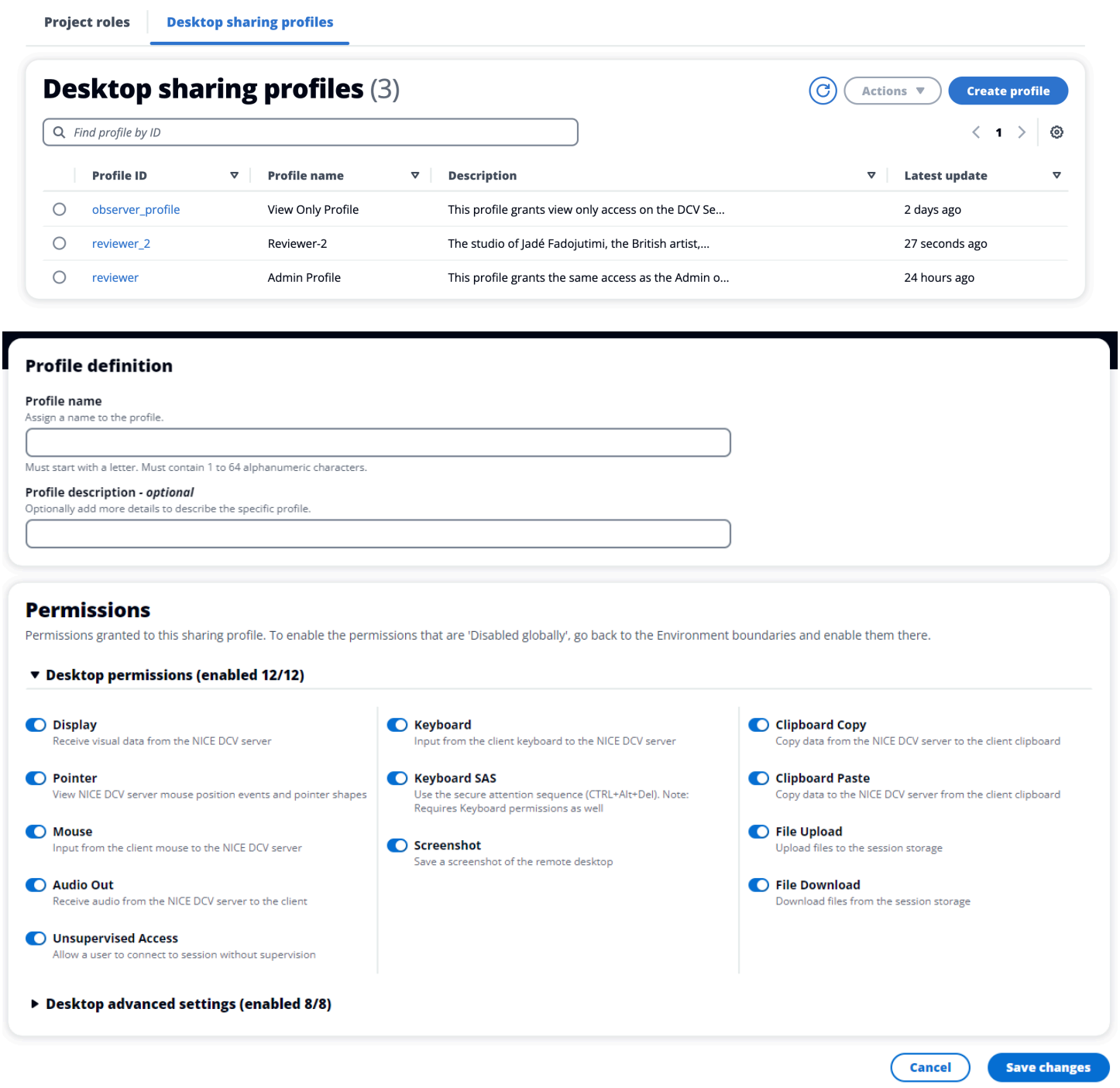


Profils de partage de bureau

Les administrateurs peuvent créer de nouveaux profils et les personnaliser. Ces profils sont accessibles à tous les utilisateurs et sont utilisés lors du partage d'une session avec d'autres utilisateurs. Les autorisations maximales accordées au sein de ces profils ne peuvent pas dépasser les autorisations de bureau autorisées dans le monde entier.

Créer un profil

Les administrateurs peuvent choisir Créer un profil pour créer un nouveau profil. Ils peuvent ensuite saisir un nom de profil, une description du profil, définir les autorisations souhaitées et enregistrer leurs modifications.



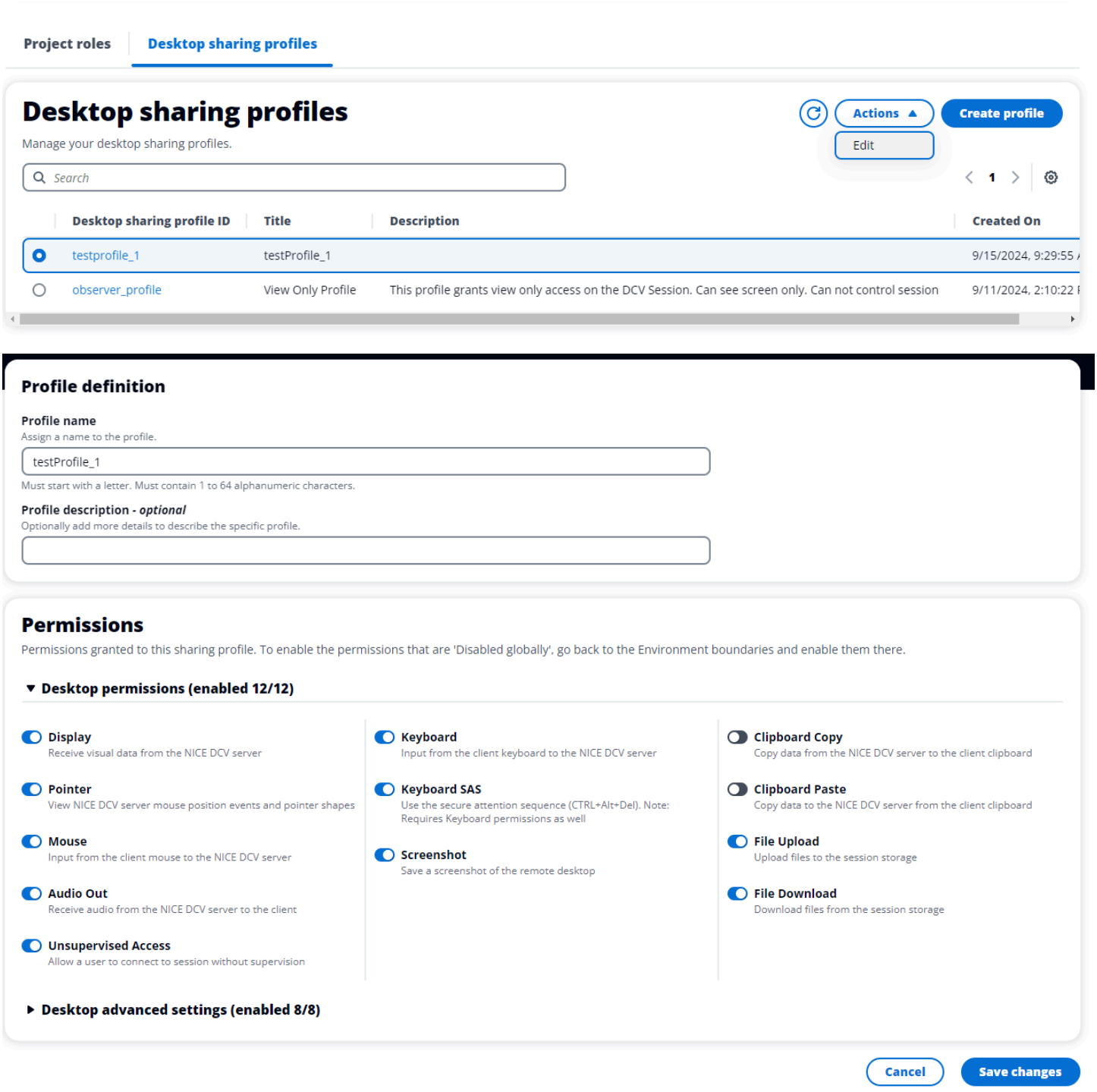
Modifier le profil

Pour modifier un profil :

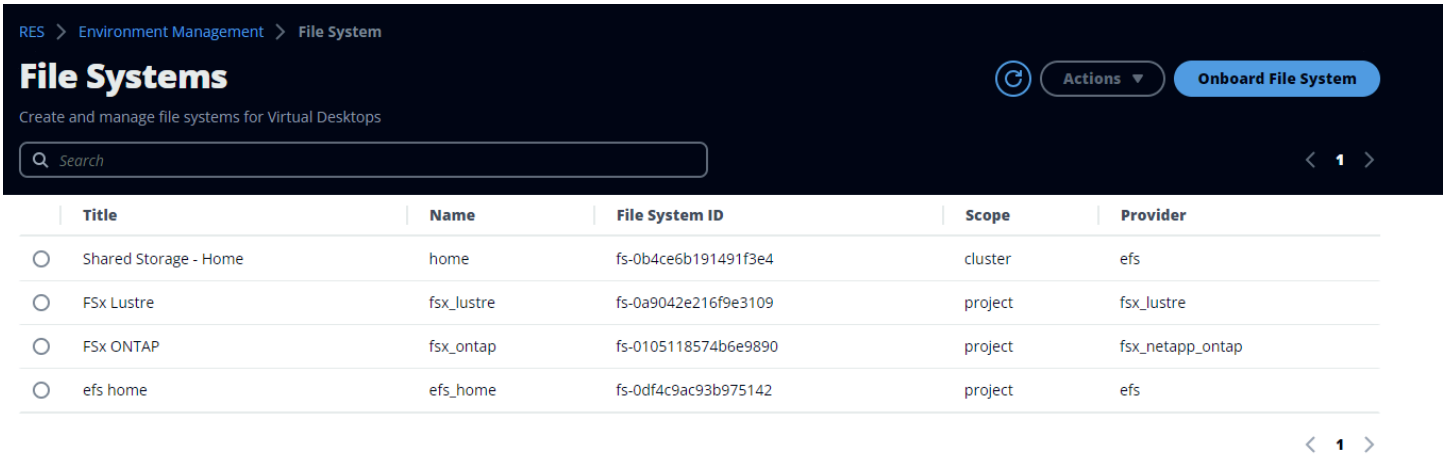
1. Sélectionnez le profil souhaité.
2. Choisissez Actions, puis sélectionnez Modifier pour modifier le profil.

3. Ajustez les autorisations selon vos besoins.
4. Sélectionnez Enregistrer les modifications.

Toute modification apportée au profil sera immédiatement appliquée aux sessions ouvertes en cours.



Systèmes de fichiers



Sur la page Systèmes de fichiers, vous pouvez :

1. Recherchez des systèmes de fichiers.
2. Lorsqu'un système de fichiers est sélectionné, utilisez le menu Actions pour :
   a. Ajoutez le système de fichiers à un projet.
   b. Supprimer le système de fichiers d'un projet
3. Intégrez un nouveau système de fichiers.
4. Lorsqu'un système de fichiers est sélectionné, vous pouvez agrandir le volet en bas de l'écran pour afficher les détails du système de fichiers.

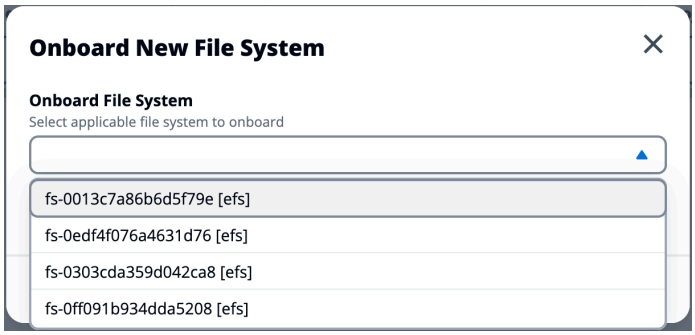
Rubriques

- Intégrer un système de fichiers

Intégrer un système de fichiers

> **Note**
>
> Pour intégrer correctement un système de fichiers, celui-ci doit partager le même VPC et au moins un de vos sous-réseaux RES. Vous devez également vous assurer que le groupe de sécurité est correctement configuré afin d' VDIs avoir accès au contenu du système de fichiers.

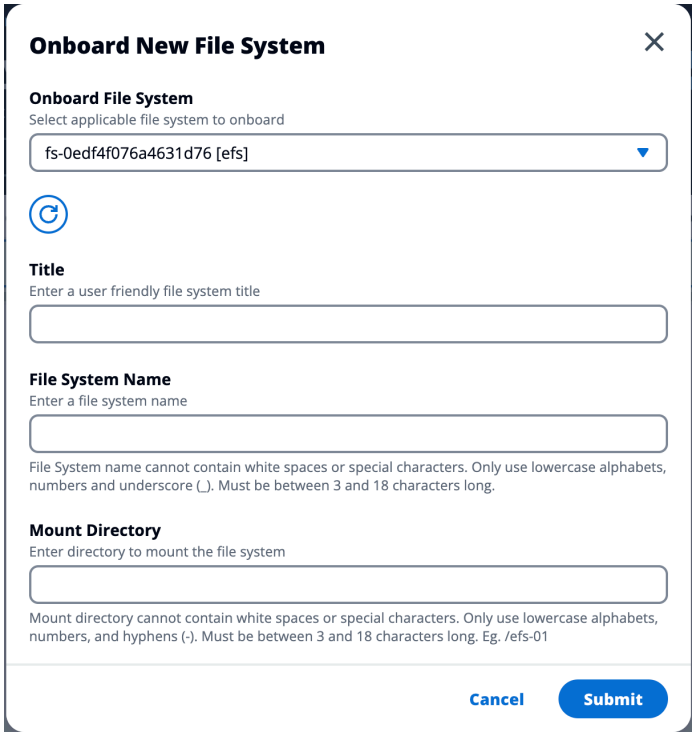
1. Choisissez le système de fichiers intégré.
2. Sélectionnez un système de fichiers dans le menu déroulant. Le modal s'étendra avec des entrées détaillées supplémentaires.



3. Entrez les détails du système de fichiers.

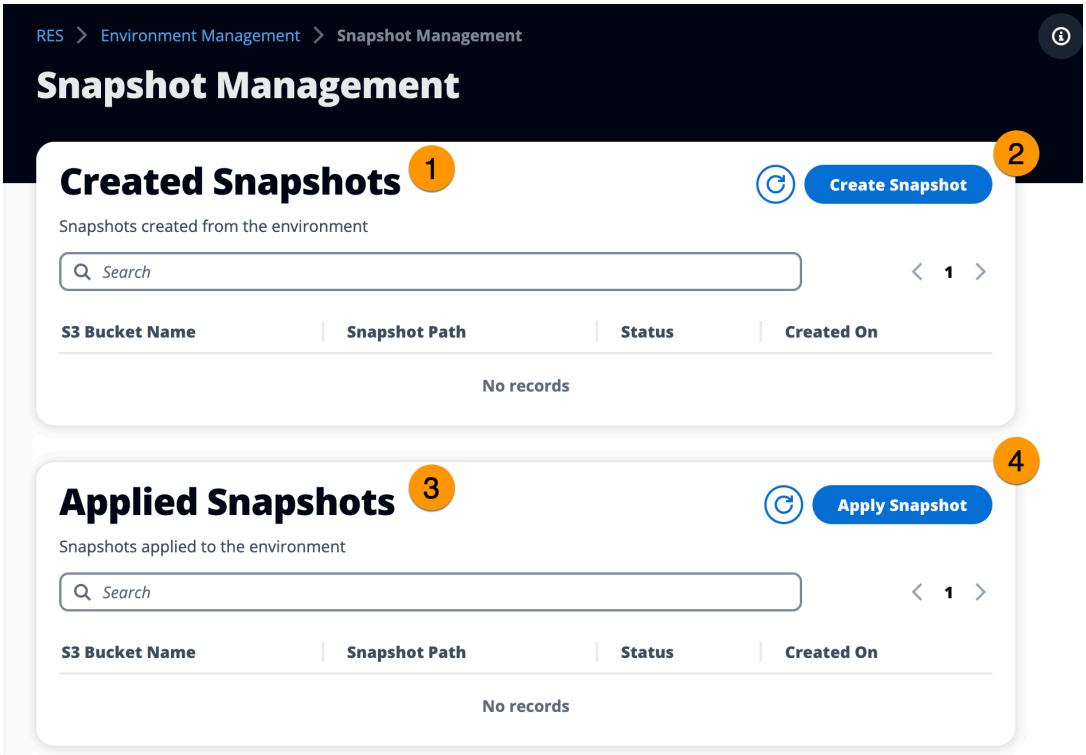
> **Note**
>
> Par défaut, les administrateurs et les propriétaires de projets ont la possibilité de choisir un système de fichiers personnel lors de la création d'un nouveau projet, qui ne peut pas être modifié par la suite.
> Les systèmes de fichiers destinés à être utilisés comme répertoires de base dans les projets doivent être intégrés en définissant leur chemin de répertoire de montage sur. `/home` Cela remplira le système de fichiers intégré dans les options déroulantes du système de fichiers du répertoire de base. Cette fonctionnalité permet de garder les données isolées entre les projets puisque seuls les utilisateurs associés au projet auront accès au système de fichiers via leur VDIs. VDIs montera le système de fichiers au point de montage sélectionné lors de l'intégration d'un système de fichiers.

4. Sélectionnez Soumettre.



Gestion des instantanés

La gestion des snapshots simplifie le processus de sauvegarde et de migration des données entre les environnements, garantissant ainsi cohérence et précision. Avec les instantanés, vous pouvez enregistrer l'état de votre environnement et migrer les données vers un nouvel environnement ayant le même état.



Depuis la page de gestion des snapshots, vous pouvez :

1. Affichez tous les instantanés créés et leur statut.
2. Créez un instantané. Avant de créer un instantané, vous devez créer un bucket avec les autorisations appropriées.
3. Affichez tous les instantanés appliqués et leur état.
4. Appliquez un instantané.

Rubriques

- Créer un instantané
- Appliquer un instantané

Créer un instantané

Avant de créer un instantané, vous devez fournir à un compartiment Amazon S3 les autorisations nécessaires. Pour en savoir plus sur la création d'un compartiment, consultez Créer un compartiment. Nous recommandons d'activer la gestion des versions des compartiments et la journalisation des accès au serveur. Ces paramètres peuvent être activés depuis l'onglet Propriétés du bucket après le provisionnement.

> **Note**
>
> Le cycle de vie de ce compartiment Amazon S3 ne sera pas géré au sein du produit. Vous devrez gérer le cycle de vie du bucket depuis la console.

Pour ajouter des autorisations au bucket, procédez comme suit :

1. Sélectionnez le compartiment que vous avez créé dans la liste des compartiments.
2. Sélectionnez l'onglet Autorisations.
3. Sous Politique de compartiment, choisissez Modifier.
4. Ajoutez la déclaration suivante à la politique du compartiment. Remplacez les valeurs suivantes par les vôtres :

   - *111122223333*-> votre identifiant AWS de compte
   - *{RES_ENVIRONMENT_NAME}*-> le nom de votre environnement RES
   - *us-east-1*-> votre AWS région
   - *amzn-s3-demo-bucket*-> le nom de votre compartiment S3

   > **Important**
   >
   > Certaines chaînes de version limitées sont prises en charge par AWS. Pour de plus amples informations, veuillez consulter https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

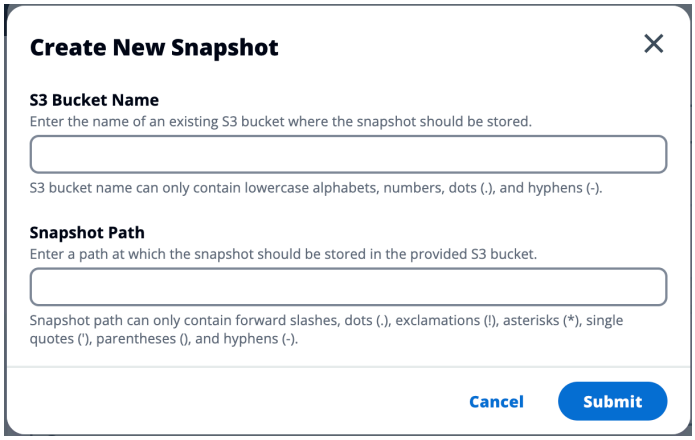
   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-role"
```

```
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Pour créer l'instantané :

1. Choisissez Create Snapshot (Créer un instantané).
2. Entrez le nom du compartiment Amazon S3 que vous avez créé.
3. Entrez le chemin où vous souhaitez que le cliché soit stocké dans le compartiment. Par exemple, **`october2023/23`**.
4. Sélectionnez Soumettre.



5. Après cinq à dix minutes, choisissez Actualiser sur la page Instantanés pour vérifier l'état. Un instantané ne sera pas valide tant que le statut ne passera pas de IN_PROGRESS à COMPLETED.

Appliquer un instantané

Une fois que vous avez créé un instantané d'un environnement, vous pouvez l'appliquer à un nouvel environnement pour faire migrer les données. Vous devrez ajouter une nouvelle politique au compartiment pour permettre à l'environnement de lire l'instantané.

L'application d'un instantané copie des données telles que les autorisations des utilisateurs, les projets, les piles de logiciels, les profils d'autorisation et les systèmes de fichiers avec leurs associations dans un nouvel environnement. Les sessions utilisateur ne seront pas répliquées. Lorsque le cliché est appliqué, il vérifie les informations de base de chaque enregistrement de ressource pour déterminer s'il existe déjà. Pour les enregistrements dupliqués, le snapshot ignore la création de ressources dans le nouvel environnement. Pour les enregistrements similaires, tels que partager un nom ou une clé, mais les autres informations de base sur les ressources varient, il créera un nouvel enregistrement avec un nom et une clé modifiés en utilisant la convention suivante :`RecordName_SnapshotRESVersion_ApplySnapshotID`. `ApplySnapshotID`Il ressemble à un horodatage et identifie chaque tentative d'application d'un instantané.

Au cours de l'application de capture instantanée, la capture instantanée vérifie la disponibilité des ressources. La ressource non disponible pour le nouvel environnement ne sera pas créée. Pour les ressources dotées d'une ressource dépendante, le cliché vérifie la disponibilité de la ressource dépendante. Si la ressource dépendante n'est pas disponible, elle créera la ressource principale sans la ressource dépendante.

Si le nouvel environnement ne fonctionne pas comme prévu ou échoue, vous pouvez consulter les CloudWatch journaux trouvés dans le groupe de journaux `/res-<env-name>/cluster-manager` pour plus de détails. Chaque journal comportera la balise [apply snapshot]. Une fois que vous avez appliqué un instantané, vous pouvez vérifier son statut the section called “Gestion des instantanés” sur la page.

Pour ajouter des autorisations au bucket, procédez comme suit :

1. Sélectionnez le compartiment que vous avez créé dans la liste des compartiments.
2. Sélectionnez l'onglet Autorisations.
3. Sous Politique de compartiment, choisissez Modifier.
4. Ajoutez la déclaration suivante à la politique du compartiment. Remplacez les valeurs suivantes par les vôtres :

   - *111122223333*-> votre identifiant AWS de compte
   - *{RES_ENVIRONMENT_NAME}*-> le nom de votre environnement RES
   - *us-east-1*-> votre AWS région
   - *amzn-s3-demo-bucket*-> le nom de votre compartiment S3

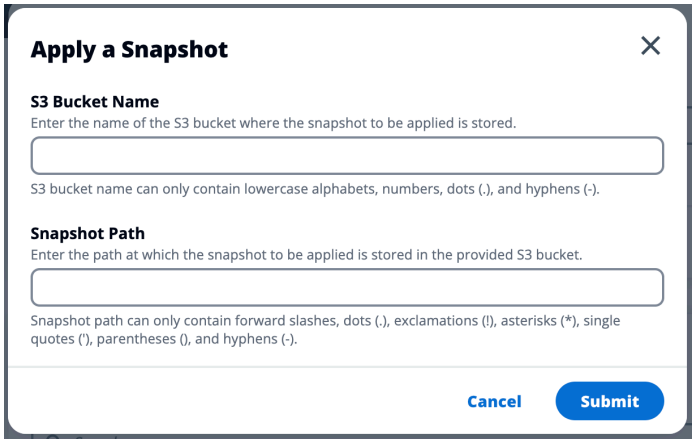
   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-role"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Pour appliquer un instantané :

1. Choisissez Appliquer un instantané.
2. Entrez le nom du compartiment Amazon S3 contenant le snapshot.
3. Entrez le chemin du fichier vers le snapshot dans le compartiment.
4. Sélectionnez Soumettre.



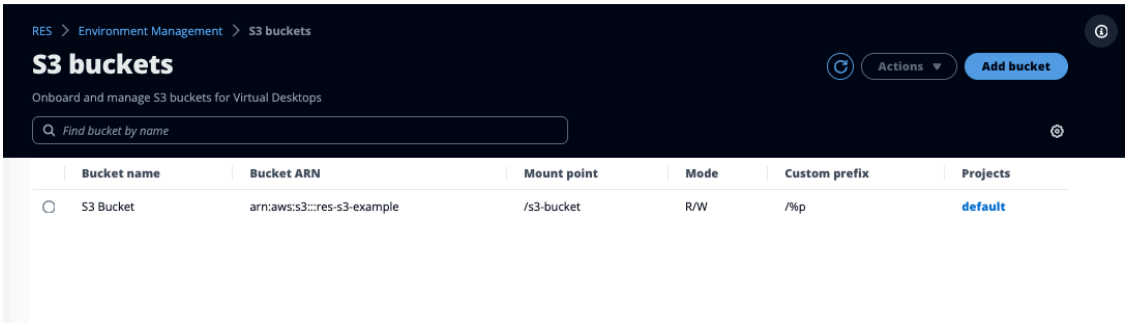
5. Après cinq à dix minutes, choisissez Actualiser sur la page de gestion des snapshots pour vérifier l'état.

Compartiments Amazon S3

Research and Engineering Studio (RES) prend en charge le montage de compartiments Amazon S3 sur des instances VDI (Virtual Desktop Infrastructure) Linux. Les administrateurs RES peuvent intégrer des compartiments S3 à RES, les associer à des projets, modifier leur configuration et supprimer des compartiments dans l'onglet Compartiments S3 sous Gestion de l'environnement.

Le tableau de bord des compartiments S3 fournit une liste des compartiments S3 intégrés mis à votre disposition. Depuis le tableau de bord des compartiments S3, vous pouvez :

1. Utilisez Ajouter un compartiment pour intégrer un compartiment S3 à RES.
2. Sélectionnez un compartiment S3 et utilisez le menu Actions pour :
   - Modifier un bucket
   - Supprimer un seau
3. Utilisez le champ de recherche pour effectuer une recherche par nom de compartiment et trouver des compartiments S3 intégrés.



Les sections suivantes décrivent comment gérer les compartiments Amazon S3 dans vos projets RES.

Rubriques

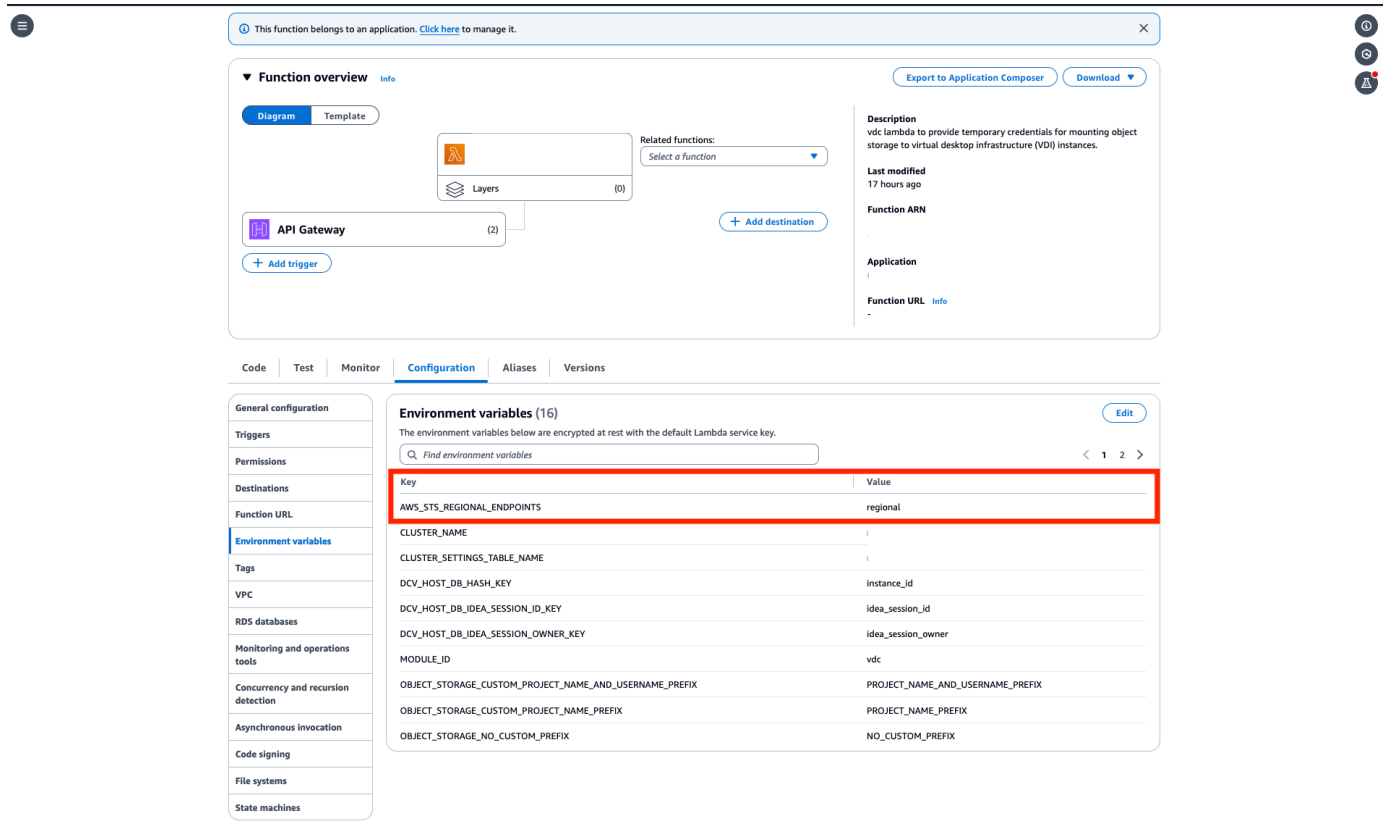
- Conditions requises pour les compartiments Amazon S3 pour les déploiements de VPC isolés
- Ajouter un compartiment Amazon S3
- Modifier un compartiment Amazon S3
- Supprimer un compartiment Amazon S3
- Isolation des données
- Accès au bucket entre comptes
- Empêcher l'exfiltration de données dans un VPC privé

- Résolution des problèmes
- Activant CloudTrail

Conditions requises pour les compartiments Amazon S3 pour les déploiements de VPC isolés

Si vous déployez Research and Engineering Studio dans un VPC isolé, suivez ces étapes pour mettre à jour les paramètres de configuration Lambda après avoir déployé RES dans votre compte. AWS

1. Connectez-vous à la console Lambda du AWS compte sur lequel Research and Engineering Studio est déployé.
2. Recherchez et naviguez jusqu'à la fonction Lambda nommée. `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`
3. Sélectionnez l'onglet Configuration de la fonction.



4. Sur le côté gauche, choisissez Variables d'environnement pour afficher cette section.
5. Choisissez Modifier et ajoutez la nouvelle variable d'environnement suivante à la fonction :

- Clé : `AWS_STS_REGIONAL_ENDPOINTS`
- Valeur : `regional`

6. Choisissez Enregistrer.

Ajouter un compartiment Amazon S3

Pour ajouter un compartiment S3 à votre environnement RES :

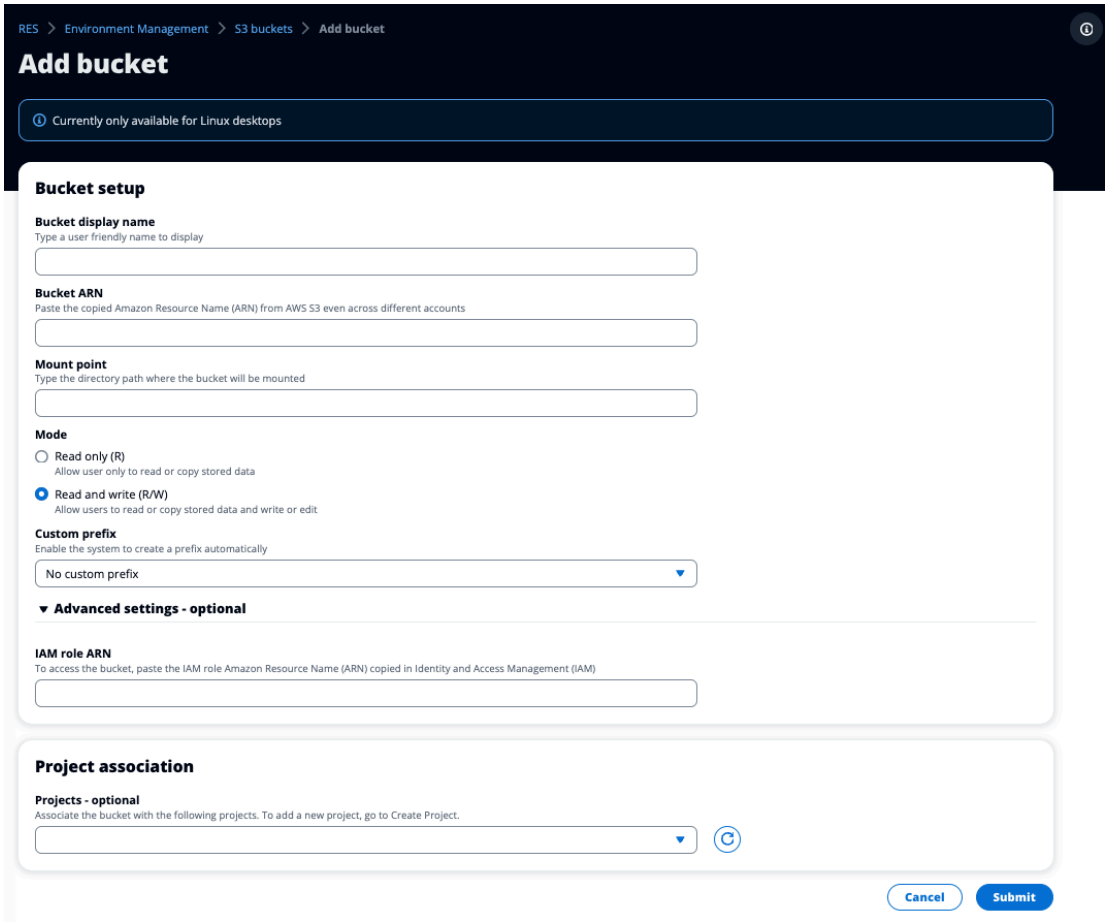
1. Choisissez Add bucket (Ajouter un compartiment).
2. Entrez les détails du bucket tels que le nom du bucket, l'ARN et le point de montage.

> **Important**
>
> - L'ARN du bucket, le point de montage et le mode fournis ne peuvent pas être modifiés après la création.
> - L'ARN du bucket peut contenir un préfixe qui isolera le bucket S3 intégré par rapport à ce préfixe.

3. Sélectionnez le mode dans lequel vous souhaitez embarquer votre bucket.

> **Important**
>
> - Voir Isolation des données pour plus d'informations sur l'isolation des données avec des modes spécifiques.

4. Sous Options avancées, vous pouvez fournir un ARN de rôle IAM pour monter les buckets pour l'accès entre comptes. Suivez les étapes décrites Accès au bucket entre comptes pour créer le rôle IAM requis pour l'accès entre comptes.
5. (Facultatif) Associez le bucket à des projets, qui peuvent être modifiés ultérieurement. Toutefois, un compartiment S3 ne peut pas être monté sur les sessions VDI existantes d'un projet. Seules les sessions lancées une fois que le projet a été associé au bucket monteront le bucket.
6. Sélectionnez Soumettre.



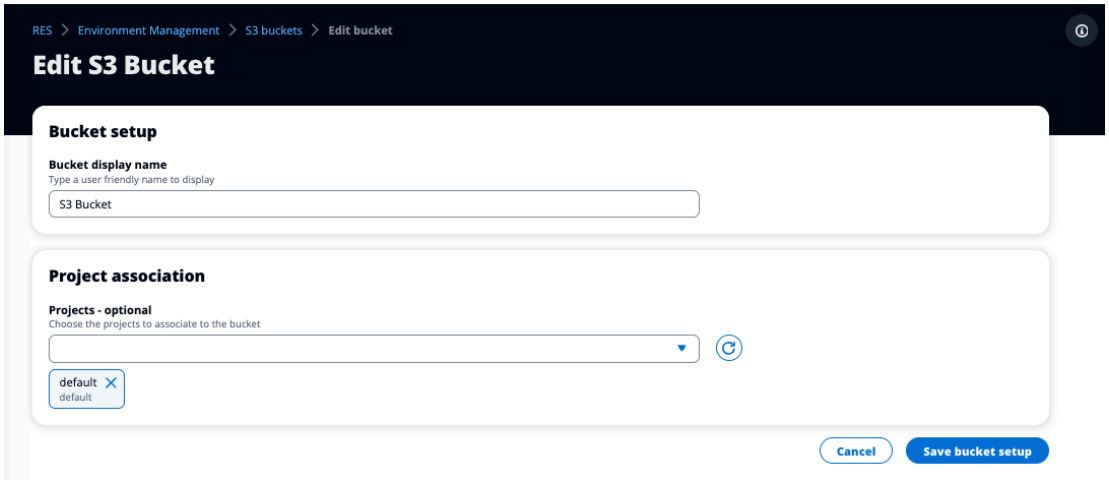
Modifier un compartiment Amazon S3

1. Sélectionnez un compartiment S3 dans la liste des compartiments S3.
2. Dans le menu Actions, sélectionnez Modifier.
3. Entrez vos mises à jour.

> **Important**
>
> - L'association d'un projet à un compartiment S3 ne montera pas le compartiment sur les instances d'infrastructure de bureau virtuel (VDI) existantes de ce projet. Le bucket ne sera monté sur les sessions VDI lancées dans un projet qu'une fois le bucket associé à ce projet.

- La dissociation d'un projet d'un compartiment S3 n'aura aucun impact sur les données contenues dans le compartiment S3, mais les utilisateurs d'ordinateurs de bureau perdront l'accès à ces données.

4. Choisissez Enregistrer la configuration du bucket.



Supprimer un compartiment Amazon S3

1. Sélectionnez un compartiment S3 dans la liste des compartiments S3.
2. Dans le menu Actions, sélectionnez Supprimer.

> **Important**
>
> - Vous devez d'abord supprimer toutes les associations de projets du compartiment.
> - L'opération de suppression n'a aucun impact sur les données du compartiment S3. Il supprime uniquement l'association du compartiment S3 avec RES.
> - La suppression d'un compartiment entraîne la perte de l'accès des sessions VDI existantes au contenu de ce compartiment à l'expiration des informations d'identification de cette session (environ 1 heure).

Isolation des données

Lorsque vous ajoutez un compartiment S3 à RES, vous avez la possibilité d'isoler les données qu'il contient pour des projets et des utilisateurs spécifiques. Sur la page Ajouter un compartiment, vous pouvez sélectionner un mode Read Only (R) ou Read and Write (R/W).

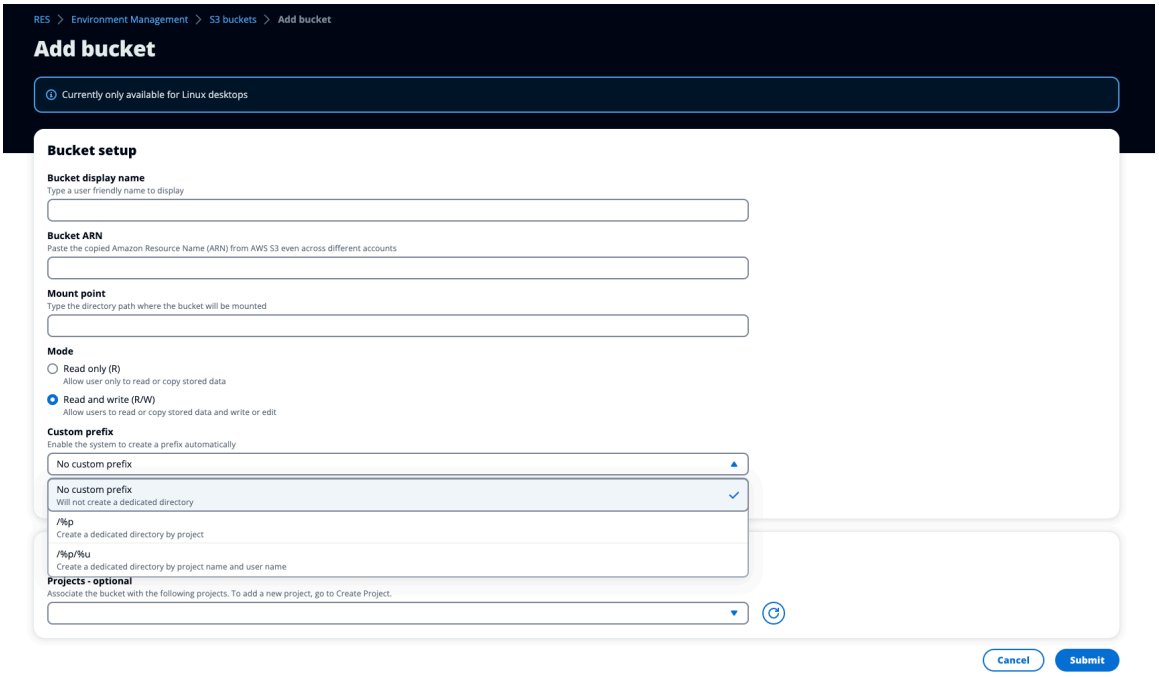
Lecture seule

Si `Read Only (R)` cette option est sélectionnée, l'isolation des données est appliquée en fonction du préfixe de l'ARN du bucket (Amazon Resource Name). Par exemple, si un administrateur ajoute un bucket à RES à l'aide de l'ARN `arn:aws:s3:::`*`bucket-name/example-data/`* et associe ce bucket au projet A et au projet B, les utilisateurs qui lancent VDIs depuis le projet A et le projet B ne peuvent lire que les données situées *`bucket-name`* sous le chemin*`/example-data`*. Ils n'auront pas accès aux données en dehors de ce chemin. Si aucun préfixe n'est ajouté à l'ARN du bucket, l'intégralité du bucket sera mise à la disposition de tous les projets qui lui sont associés.

Lire et écrire

Si `Read and Write (R/W)` cette option est sélectionnée, l'isolation des données est toujours appliquée en fonction du préfixe de l'ARN du bucket, comme décrit ci-dessus. Ce mode comporte des options supplémentaires permettant aux administrateurs de fournir un préfixe basé sur des variables pour le compartiment S3. Lorsque cette option `Read and Write (R/W)` est sélectionnée, une section Préfixe personnalisé devient disponible et propose un menu déroulant avec les options suivantes :

- Aucun préfixe personnalisé
- /%p
- /%p/%u



Aucune isolation personnalisée des données

Lorsque `No custom prefix` le préfixe personnalisé est sélectionné, le bucket est ajouté sans aucune isolation de données personnalisée. Cela permet à tous les projets associés au bucket d'avoir un accès en lecture et en écriture. Par exemple, si un administrateur ajoute un bucket à RES à l'aide de l'ARN `arn:aws:s3:::`*`bucket-name`* avec `No custom prefix` selected et associe ce bucket aux projets A et B, les utilisateurs qui le lancent VDIs depuis le projet A et le projet B auront un accès illimité en lecture et en écriture au bucket.

Isolation des données au niveau du projet

Lorsque `/%p` le préfixe personnalisé est sélectionné, les données du compartiment sont isolées pour chaque projet spécifique qui lui est associé. La `%p` variable représente le code du projet. Par exemple, si un administrateur ajoute un bucket à RES en utilisant l'ARN `arn:aws:s3:::`*`bucket-name`* avec `/%p` selected et un point de montage de*`/bucket`*, et qu'il associe ce bucket aux projets A et B, l'utilisateur A du projet A peut y écrire un fichier*`/bucket`*. L'utilisateur B du projet A peut également voir le fichier dans lequel l'utilisateur A a écrit*`/bucket`*. Toutefois, si l'utilisateur B lance un VDI dans le projet B et y jette un *`/bucket`* œil, il ne verra pas le fichier écrit par l'utilisateur A, car les données sont isolées par projet. Le fichier écrit par l'utilisateur A se trouve dans le compartiment S3 sous le préfixe, `/ProjectA` tandis que l'utilisateur B ne peut y accéder que `/ProjectB` s'il utilise le fichier VDIs depuis le projet B.

Isolation des données au niveau du projet et de l'utilisateur

Lorsque le préfixe personnalisé **/%p/%u** est sélectionné, les données du compartiment sont isolées pour chaque projet spécifique et pour chaque utilisateur associé à ce projet. La %p variable représente le code du projet et %u le nom d'utilisateur. Par exemple, un administrateur ajoute un bucket à RES en utilisant l'ARN `arn:aws:s3:::`*`bucket-name`* dont le point de montage est /%p/%u sélectionné et le point de montage est égal à*`/bucket`*. Ce compartiment est associé au projet A et au projet B. L'utilisateur A du projet A peut y écrire un fichier*`/bucket`*. Contrairement au scénario précédent avec uniquement %p l'isolation, l'utilisateur B ne verra pas dans ce cas le fichier écrit par l'utilisateur A dans le projet A*`/bucket`*, car les données sont isolées à la fois par le projet et par l'utilisateur. Le fichier écrit par l'utilisateur A se trouve dans le compartiment S3 sous le préfixe, `/ProjectA/UserA` tandis que l'utilisateur B ne peut y accéder que `/ProjectA/UserB` s'il l'utilise VDIs dans le projet A.

Accès au bucket entre comptes

RES est capable de monter des buckets à partir d'autres AWS comptes, à condition que ces buckets disposent des autorisations appropriées. Dans le scénario suivant, un environnement RES du compte A souhaite monter un compartiment S3 dans le compte B.

Étape 1 : Créez un rôle IAM dans le compte dans lequel RES est déployé (ce rôle sera appelé compte A) :

1. Connectez-vous à la console AWS de gestion du compte RES qui doit accéder au compartiment S3 (compte A).
2. Ouvrez la console IAM :
   a. Accédez au tableau de bord IAM.
   b. Dans le panneau de navigation, choisissez Politiques.
3. Créez une politique :
   a. Choisissez Create Policy (Créer une politique).
   b. Sélectionnez l'onglet JSON.
   c. Collez la politique JSON suivante (*`amzn-s3-demo-bucket`*remplacez-la par le nom du compartiment S3 situé dans le compte B) :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

d. Choisissez Suivant.

4. Passez en revue et créez la politique :

   a. Donnez un nom à la politique (par exemple, AccessPolicy « S3 »).

   b. Ajoutez une description facultative pour expliquer l'objectif de la politique.

   c. Passez en revue la politique et choisissez Créer une politique.

5. Ouvrez la console IAM :

   a. Accédez au tableau de bord IAM.

   b. Dans le panneau de navigation, choisissez Rôles.

6. Créez un rôle :

   a. Choisissez Créer un rôle.

   b. Choisissez Politique de confiance personnalisée comme type d'entité de confiance.

c. Collez la politique JSON suivante (*111122223333*remplacez-la par l'ID de compte réel du compte A, *ENVIRONMENT_NAME* par le nom de l'environnement du déploiement de RES et *us-east-1* par la AWS région dans laquelle RES est déployé) :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/<ENVIRONMENT_NAME>-vdc-custom-
credential-broker-lambda-role"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. Choisissez Suivant.

7. Joindre des politiques d'autorisation :

a. Recherchez et sélectionnez la politique que vous avez créée précédemment.

b. Choisissez Suivant.

8. Marquez, révisez et créez le rôle :

a. Entrez un nom de rôle (par exemple, AccessRole « S3 »).

b. À l'étape 3, choisissez Ajouter une étiquette, puis entrez la clé et la valeur suivantes :

- Clé : `res:Resource`
- Valeur : `s3-bucket-iam-role`

c. Passez en revue le rôle et choisissez Créer un rôle.

9. Utilisez le rôle IAM dans RES :

a. Copiez l'ARN du rôle IAM que vous avez créé.

b. Connectez-vous à la console RES.

c. Dans le volet de navigation de gauche, choisissez S3 Bucket.

d. Choisissez Ajouter un compartiment et remplissez le formulaire avec l'ARN du compartiment S3 multi-comptes.

e. Choisissez le menu déroulant Paramètres avancés - facultatif.

f. Entrez l'ARN du rôle dans le champ ARN du rôle IAM.

g. Choisissez Ajouter un compartiment.

Étape 2 : Modifier la politique de compartiment dans le compte B

1. Connectez-vous à la console AWS de gestion du compte B.
2. Ouvrez la console S3 :

   a. Accédez au tableau de bord S3.

   b. Sélectionnez le bucket auquel vous souhaitez accorder l'accès.
3. Modifiez la politique relative aux compartiments :

   a. Sélectionnez l'onglet Permissions, puis choisissez Bucket policy.

   b. Ajoutez la politique suivante pour accorder au rôle IAM depuis le compte A l'accès au compartiment (remplacez-le *111122223333* par l'ID de compte réel du compte A et *amzn-s3-demo-bucket* par le nom du compartiment S3) :

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

c. Choisissez Enregistrer.

Empêcher l'exfiltration de données dans un VPC privé

Pour empêcher les utilisateurs d'exfiltrer les données des compartiments S3 sécurisés vers leurs propres compartiments S3 de leur compte, vous pouvez associer un point de terminaison VPC pour sécuriser votre VPC privé. Les étapes suivantes montrent comment créer un point de terminaison VPC pour le service S3 qui prend en charge l'accès aux compartiments S3 au sein de votre compte, ainsi qu'à tout compte supplémentaire doté de compartiments multicomptes.

1. Ouvrez la console Amazon VPC :
   a. Connectez-vous à la console AWS de gestion.
   b. Ouvrez la console Amazon VPC à l'adresse. https://console.aws.amazon.com/vpc/
2. Créez un point de terminaison VPC pour S3 :
   a. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
   b. Choisissez Créer un point de terminaison.
   c. Pour Catégorie de service, assurez-vous que l'option services AWS est sélectionnée.
   d. Dans le champ Nom du service, entrez `com.amazonaws.<region>.s3` (remplacez `<region>` par votre AWS région) ou recherchez « S3 ».
   e. Sélectionnez le service S3 dans la liste.
3. Configurer les paramètres du point de terminaison :
   a. Pour le VPC, sélectionnez le VPC dans lequel vous souhaitez créer le point de terminaison.
   b. Pour les sous-réseaux, sélectionnez les deux sous-réseaux privés utilisés pour les sous-réseaux VDI lors du déploiement.
   c. Pour Activer le nom DNS, assurez-vous que l'option est cochée. Cela permet de résoudre le nom d'hôte DNS privé sur les interfaces réseau des terminaux.

4. Configurez la politique pour restreindre l'accès :

   a. Sous Politique, sélectionnez Personnaliser.

   b. Dans l'éditeur de règles, entrez une politique qui restreint l'accès aux ressources de votre compte ou d'un compte spécifique. Voici un exemple de politique (remplacez-le *amzn-s3-demo-bucket* par le nom de votre compartiment S3 *111122223333* et *444455556666* par le AWS compte approprié IDs auquel vous souhaitez avoir accès) :

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",
                        "444455556666"
                    ]
                }
            }
        }
    ]
}
```

5. Créez le point de terminaison :

   a. Vérifiez vos paramètres.

   b. Choisissez Créer un point de terminaison.

6. Vérifiez le point de terminaison :

   a. Une fois le point de terminaison créé, accédez à la section Points de terminaison de la console VPC.

b. Sélectionnez le point de terminaison nouvellement créé.

c. Vérifiez que l'état est disponible.

En suivant ces étapes, vous créez un point de terminaison VPC qui autorise un accès S3 limité aux ressources de votre compte ou à un ID de compte spécifié.

Résolution des problèmes

Comment vérifier si un bucket ne parvient pas à être monté sur un VDI

Si un bucket ne parvient pas à être monté sur un VDI, vous pouvez vérifier les erreurs à certains endroits. Suivez les étapes ci-dessous.

1. Vérifiez les journaux VDI :

   a. Connectez-vous à la console AWS de gestion.

   b. Ouvrez la console EC2 et accédez à Instances.

   c. Sélectionnez l'instance VDI que vous avez lancée.

   d. Connectez-vous au VDI via le gestionnaire de session.

   e. Exécutez les commandes suivantes :

   ```
   sudo su
   cd ~/bootstrap/logs
   ```

   Vous trouverez ici les journaux de bootstrap. Les détails de toute défaillance figureront dans le `configure.log.{time}` fichier.

   Consultez également le `/etc/message` journal pour plus de détails.

2. Vérifiez les journaux CloudWatch Lambda de Custom Credential Broker :

   a. Connectez-vous à la console AWS de gestion.

   b. Ouvrez la CloudWatch console et accédez à Log groups.

   c. Recherchez le groupe de journaux`/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.

   d. Examinez le premier groupe de journaux disponible et repérez les éventuelles erreurs dans les journaux. Ces journaux contiendront des détails concernant les problèmes potentiels liés

à la fourniture d'informations d'identification personnalisées temporaires pour le montage de compartiments S3.

3. Vérifiez les CloudWatch journaux personnalisés de Credential Broker API Gateway :

   a. Connectez-vous à la console AWS de gestion.

   b. Ouvrez la CloudWatch console et accédez à Log groups.

   c. Recherchez le groupe de journaux`<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`.

   d. Examinez le premier groupe de journaux disponible et repérez les éventuelles erreurs dans les journaux. Ces journaux contiendront des détails concernant toutes les demandes et réponses adressées à l'API Gateway concernant les informations d'identification personnalisées nécessaires au montage des compartiments S3.

Comment modifier la configuration du rôle IAM d'un bucket après l'intégration

1. Connectez-vous à la console AWS DynamoDB.
2. Sélectionnez le tableau :

   a. Dans le volet de navigation de gauche, choisissez Tables.

   b. Recherchez et sélectionnez`<stack-name>.cluster-settings`.

3. Scannez le tableau :

   a. Sélectionnez Explorer les éléments de table.

   b. Assurez-vous que Scan est sélectionné.

4. Ajoutez un filtre :

   a. Choisissez Filtres pour ouvrir la section de saisie des filtres.

   b. Réglez le filtre pour qu'il corresponde à votre clé-

      - Attribut : Entrez la clé.
      - État : Sélectionnez Commence par.
      - Valeur : entrez « `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` remplacement `<filesystem_id>` » par la valeur du système de fichiers à modifier.

5. Exécutez le scan :

Choisissez Exécuter pour exécuter le scan avec le filtre.

6. Vérifiez la valeur :

   Si l'entrée existe, assurez-vous que la valeur est correctement définie avec le bon ARN du rôle IAM.

   Si l'entrée n'existe pas :

   a. Choisissez Créer un élément.
   b. Entrez les détails de l'article :

      - Pour l'attribut clé, entrez`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
      - Ajoutez le bon ARN du rôle IAM.

   c. Choisissez Enregistrer pour ajouter l'article.

7. Redémarrez les instances VDI :

   Redémarrez l'instance pour vous assurer VDIs que les ARN affectés par le rôle IAM incorrect sont à nouveau montés.

Activant CloudTrail

Pour l'activer CloudTrail dans votre compte à l'aide de la CloudTrail console, suivez les instructions fournies dans la section Création d'un historique avec la CloudTrail console dans le guide de AWS CloudTrail l'utilisateur. CloudTrail enregistrera l'accès aux compartiments S3 en enregistrant le rôle IAM qui y a accédé. Cela peut être lié à un ID d'instance, qui est lié à un projet ou à un utilisateur.

Utiliser le produit

Cette section fournit des conseils aux utilisateurs sur l'utilisation de bureaux virtuels pour collaborer avec d'autres utilisateurs.

Rubriques

Accès SSH

Pour utiliser SSH pour accéder à l'hôte du bastion, procédez comme suit :

1. Dans le menu RES, choisissez SSH access.
2. Suivez les instructions à l'écran pour utiliser SSH ou PuTTY pour y accéder.

Bureaux virtuels

Le module d'interface de bureau virtuel (VDI) permet aux utilisateurs de créer et de gérer des bureaux virtuels Windows ou Linux sur. AWS Les utilisateurs peuvent lancer des instances Amazon EC2 avec leurs outils et applications préférés préinstallés et configurés.

Systèmes d'exploitation pris en charge

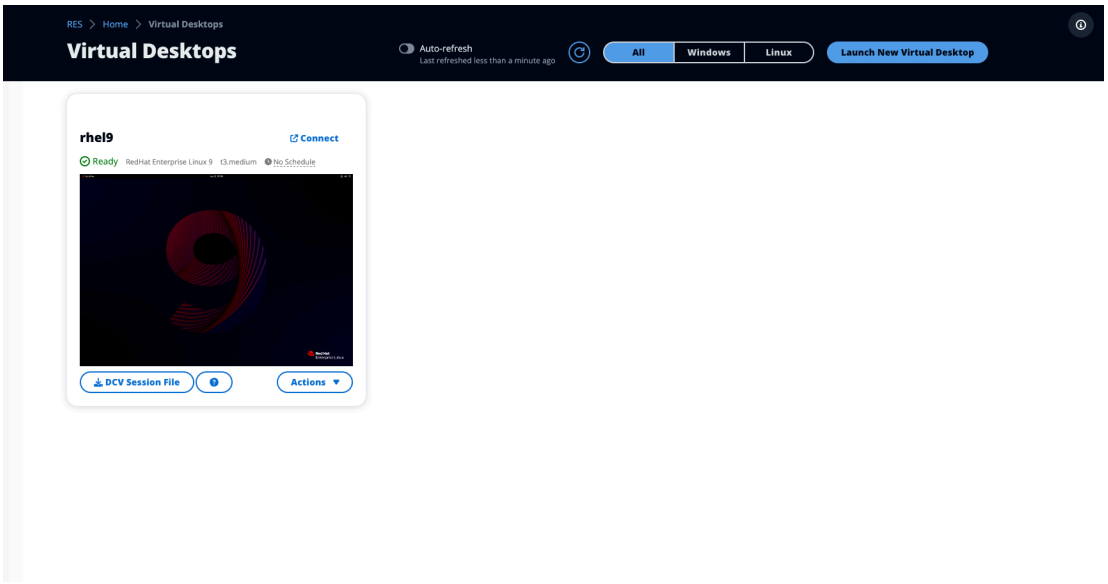
RES prend actuellement en charge le lancement de bureaux virtuels à l'aide des systèmes d'exploitation suivants :

- Amazon Linux 2 (x86 et ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL 8 (x86) et 9 (x86)
- Windows Server 2019, 2022 (x86)
- Windows 10, 11 (x86)

Rubriques

Lancer un nouvel ordinateur de bureau

1. Dans le menu, choisissez My Virtual Desktops.
2. Choisissez Lancer un nouveau bureau virtuel.



3. Entrez les informations relatives à votre nouvel ordinateur de bureau.
4. Sélectionnez Soumettre.

Une nouvelle carte contenant les informations de votre bureau apparaît instantanément, et votre bureau sera prêt à être utilisé dans les 10 à 15 minutes. Le temps de démarrage dépend de l'image sélectionnée. RES détecte les instances de GPU et installe les pilotes appropriés.

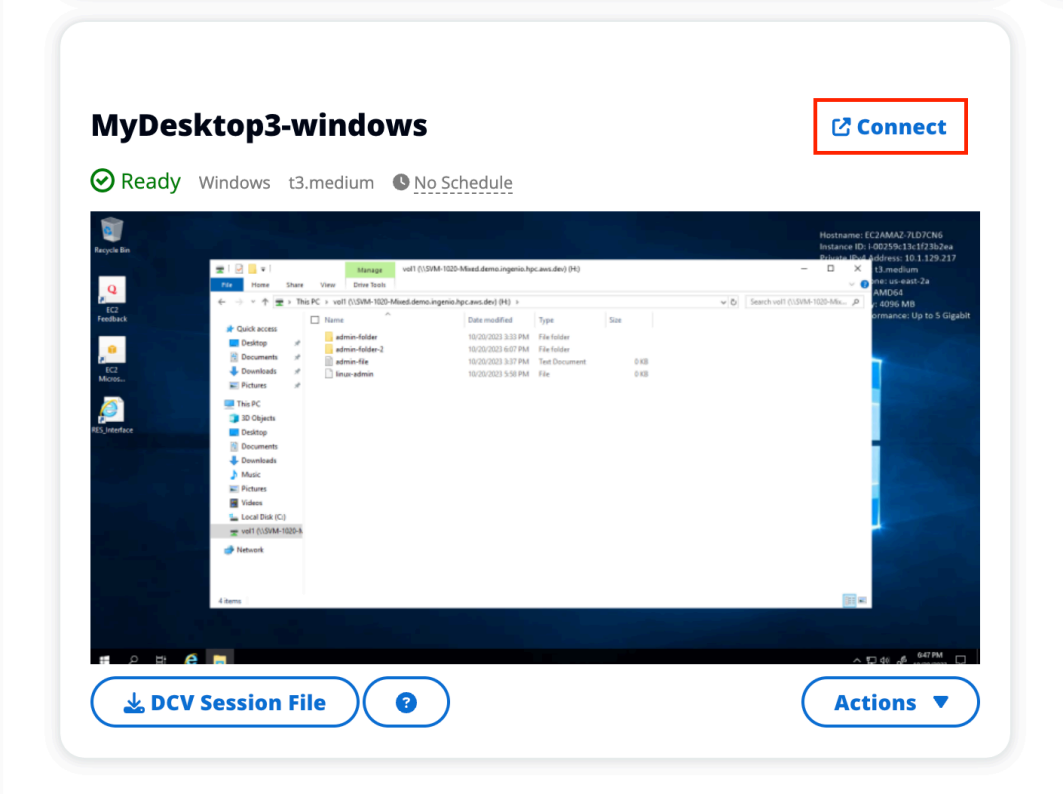
Accédez à votre bureau

Pour accéder à un bureau virtuel, choisissez la carte correspondante et connectez-vous via le Web ou un client DCV.

Web connection

L'accès à votre bureau via le navigateur Web est la méthode de connexion la plus simple.

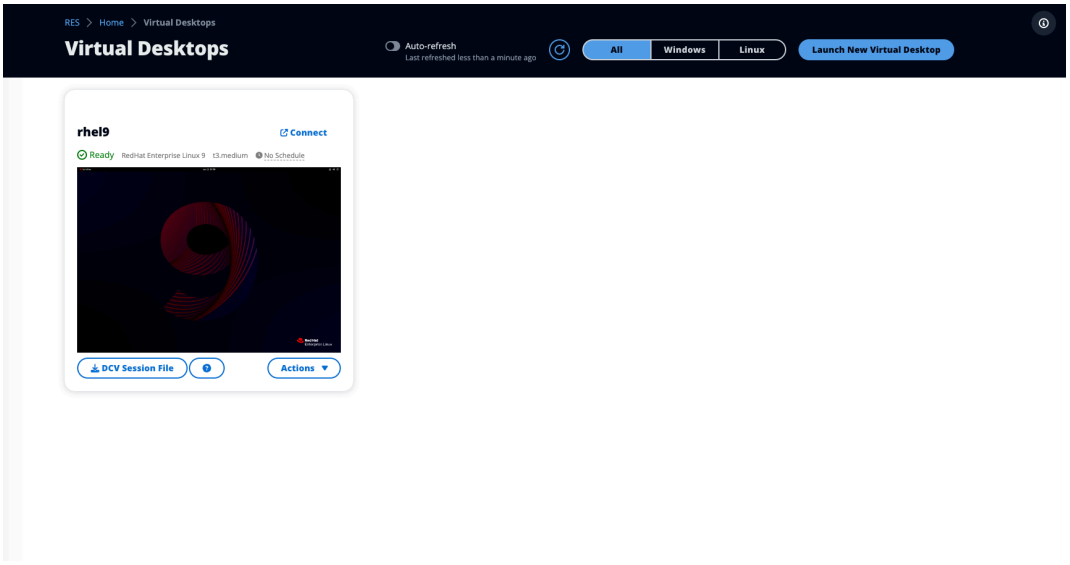
- Choisissez Connect ou choisissez la miniature pour accéder à votre bureau directement via votre navigateur.



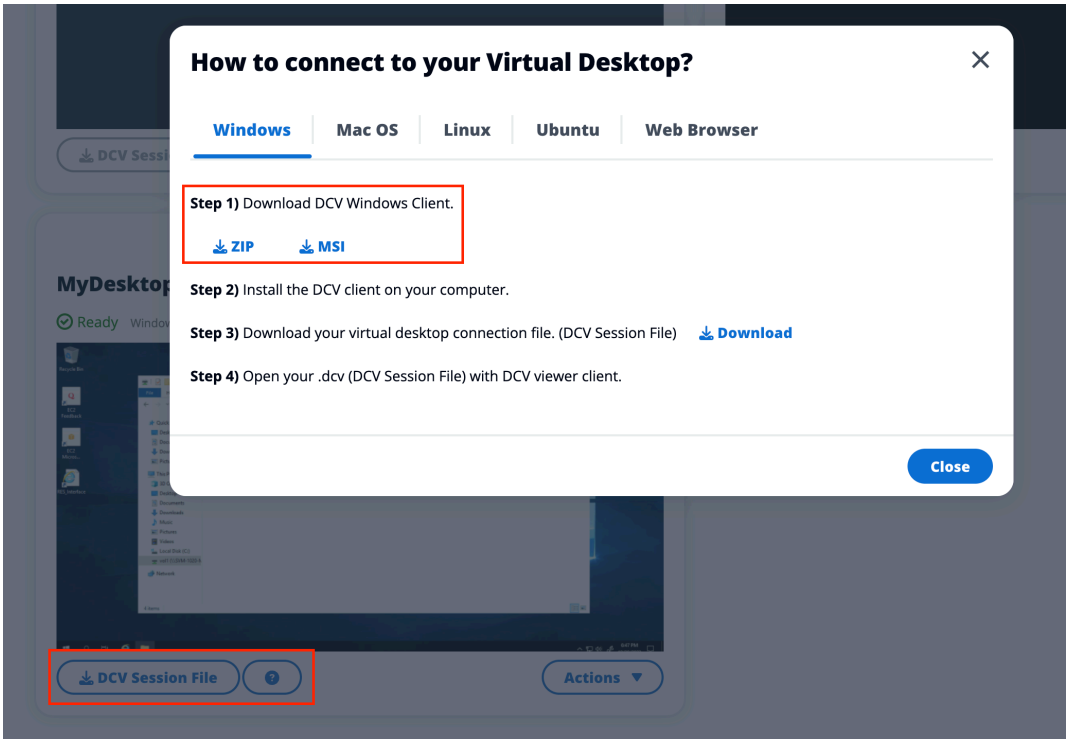
DCV connection

L'accès à votre bureau par le biais d'un client DCV offre les meilleures performances. Pour y accéder via DCV :

1. Choisissez Fichier de session DCV pour télécharger le `.dcv` fichier. Vous aurez besoin d'un client DCV installé sur votre système.



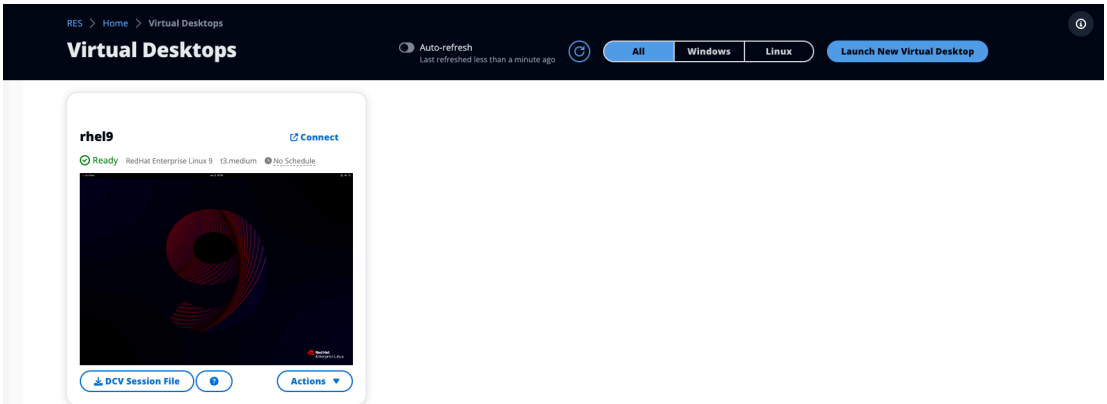
2. Pour les instructions d'installation, choisissez le ? icône.



Contrôlez l'état de votre bureau

Pour contrôler l'état de votre ordinateur de bureau :

1. Choisissez Actions.



2. Choisissez Virtual Desktop State. Vous avez le choix entre quatre états :

   - Arrêter

     Une session arrêtée ne subira aucune perte de données, et vous pouvez redémarrer une session arrêtée à tout moment.
   - Redémarrer

     Redémarre la session en cours.
   - Résilier

     Met définitivement fin à une session. La fin d'une session peut entraîner une perte de données si vous utilisez un stockage éphémère. Vous devez sauvegarder vos données sur le système de fichiers RES avant de terminer.
   - Hiberner

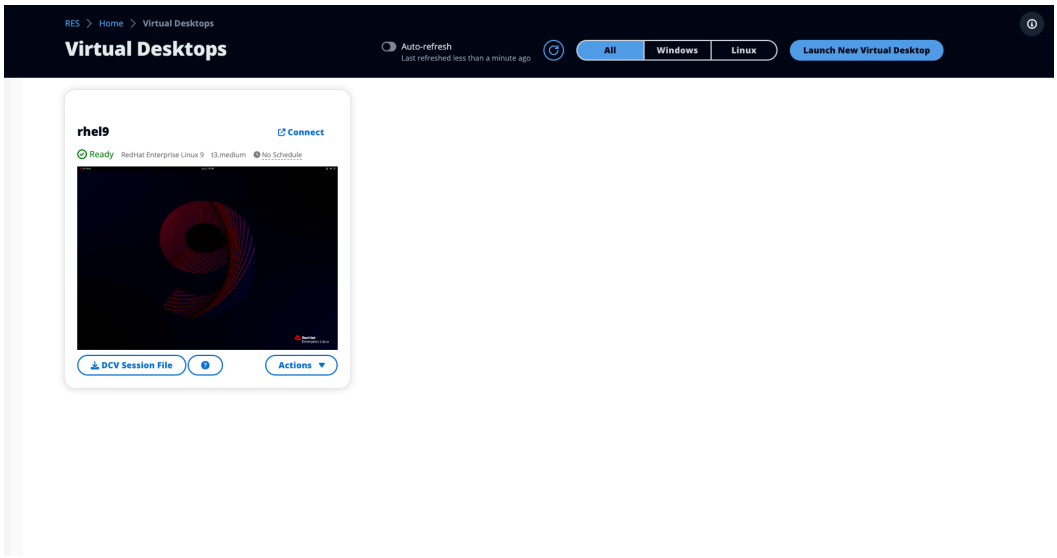
     L'état de votre bureau sera enregistré en mémoire. Lorsque vous redémarrez le bureau, vos applications reprennent, mais les connexions à distance risquent d'être perdues. Toutes les instances ne prennent pas en charge l'hibernation, et l'option n'est disponible que si elle a été activée lors de la création de l'instance. Pour vérifier si votre instance prend en charge cet état, consultez la section Conditions préalables à l'hibernation.

Modifier un bureau virtuel

Vous pouvez mettre à jour le matériel de votre bureau virtuel ou modifier le nom de session.

1. Avant de modifier la taille de l'instance, vous devez arrêter la session :

   a. Choisissez Actions.



   b. Choisissez Virtual Desktop State.

   c. Choisissez Arrêter.

> **Note**
>
> Vous ne pouvez pas mettre à jour la taille du bureau pour les sessions en veille prolongée.

2. Une fois que vous avez confirmé que le bureau s'est arrêté, choisissez Actions, puis choisissez Mettre à jour la session.
3. Modifiez le nom de la session ou choisissez la taille de bureau que vous souhaitez.
4. Sélectionnez Soumettre.
5. Une fois vos instances mises à jour, redémarrez votre bureau :

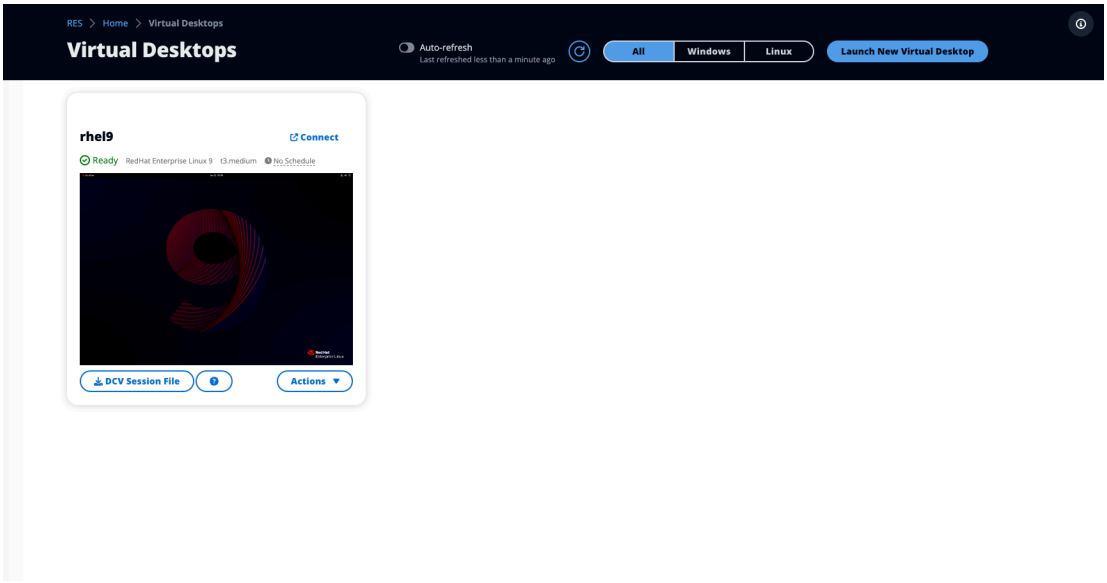
   a. Choisissez Actions.

   b. Choisissez Virtual Desktop State.

   c. Sélectionnez Démarrer.

Récupérer les informations de session

1. Choisissez Actions.



2. Choisissez Afficher les informations.

Planifier des bureaux virtuels

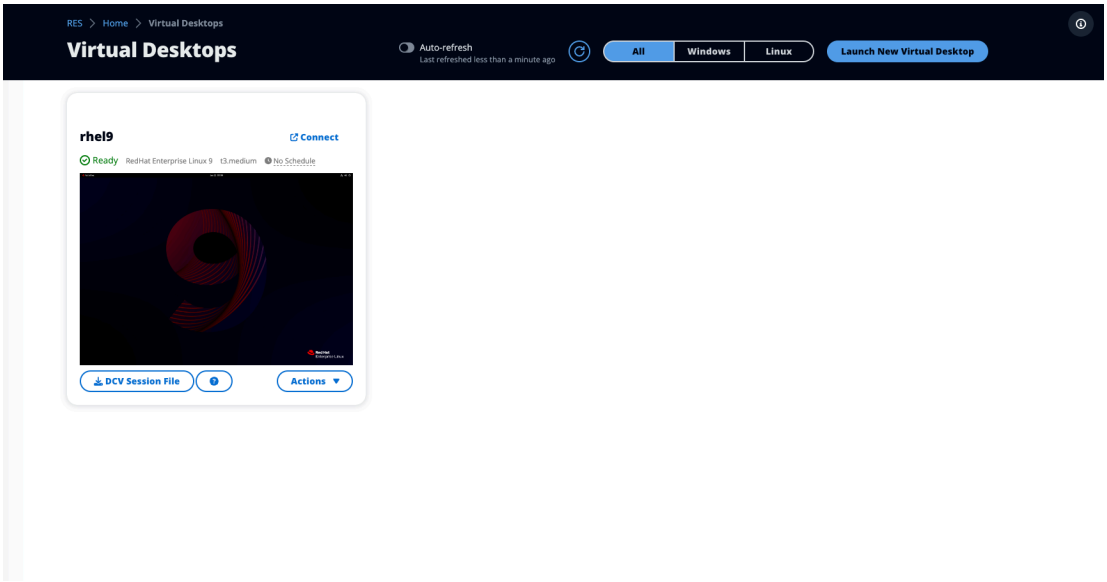
Par défaut, les bureaux virtuels sont programmés pour s'arrêter automatiquement les samedis et dimanches. Les plannings des postes de travail individuels peuvent être ajustés à l'aide des fenêtres de planification accessibles depuis le menu Actions des bureaux individuels, comme indiqué dans la section suivante. Pour en savoir plus, Définition de plannings par défaut pour l'ensemble de l'environnement consultez cette section. Les ordinateurs de bureau peuvent également s'arrêter en cas d'inactivité afin de réduire les coûts. Consultez Arrêt automatique de l'interface de bureau virtuel pour en savoir plus sur VDI Autostop.

Rubriques

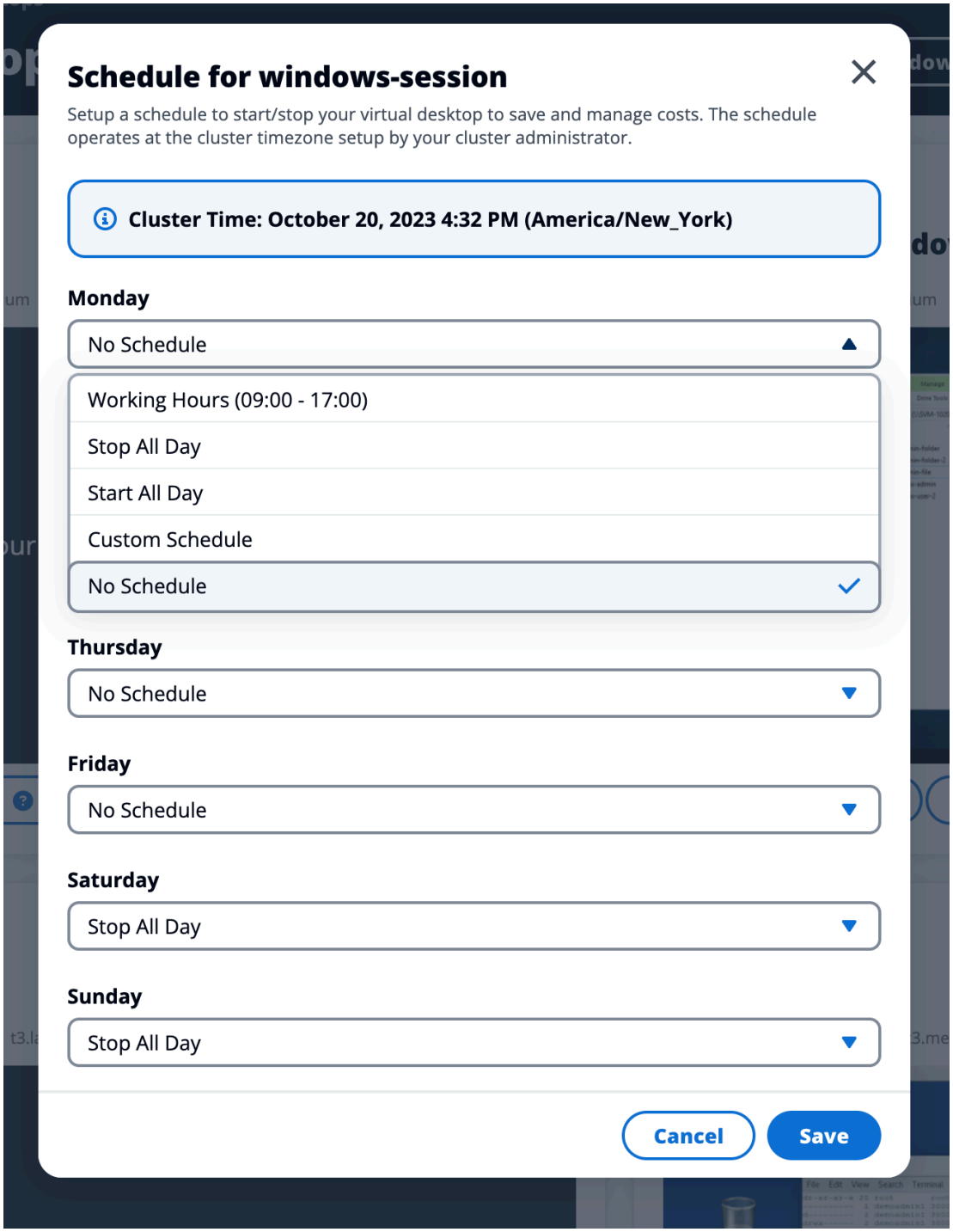
- Configuration de plannings de bureau individuels
- Définition de plannings par défaut pour l'ensemble de l'environnement

Configuration de plannings de bureau individuels

1. Choisissez Actions.



2. Sélectionnez Programme.
3. Définissez votre emploi du temps pour chaque jour.
4. Choisissez Enregistrer.



Définition de plannings par défaut pour l'ensemble de l'environnement

La planification par défaut peut être mise à jour dans DynamoDB :

1. Recherchez le tableau des paramètres du cluster de votre environnement :`<env-name>.cluster-settings`.

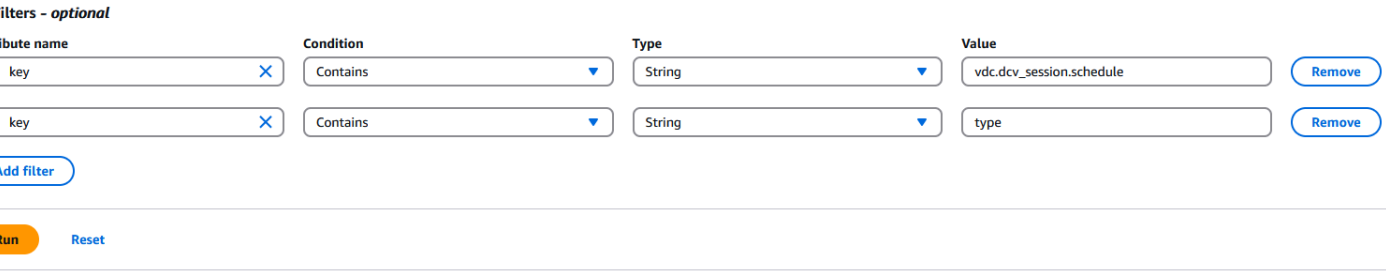
2. Sélectionnez Explorer les articles.
3. Sous Filtres, entrez les deux filtres suivants :

   Filtre 1

   - Nom de l'attribut = **`key`**
   - État = **`Contains`**
   - Type = **`String`**
   - Valeur = **`vdc.dcv_session.schedule`**

   Filtre 2

   - Nom de l'attribut = **`key`**
   - État = **`Contains`**
   - Type = **`String`**
   - Valeur = **`type`**



   Cela affichera sept entrées représentant les types de calendrier par défaut pour chaque jour du formulaire`vdc.dcv_session.schedule.<day>.type`. Les valeurs valides sont :

   - `NO_SCHEDULE`
   - `STOP_ALL_DAY`
   - `START_ALL_DAY`
   - `WORKING_HOURS`
   - `CUSTOM_SCHEDULE`
4. S'il `CUSTOM_SCHEDULE` est défini, vous devez fournir les heures de début et de fin personnalisées. Pour ce faire, utilisez le filtre suivant dans le tableau des paramètres du cluster :

- Nom de l'attribut = **`key`**
- État = **`Contains`**
- Type = **`String`**
- Valeur = **`vdc.dcv_session.schedule`**

5. Recherchez l'article au format `vdc.dcv_session.schedule.<day>.start_up_time` et `vdc.dcv_session.schedule.<day>.shut_down_time` pour les jours respectifs pour lesquels vous souhaitez définir votre calendrier personnalisé. À l'intérieur de l'élément, supprimez l'entrée Null et remplacez-la par une entrée String comme suit :

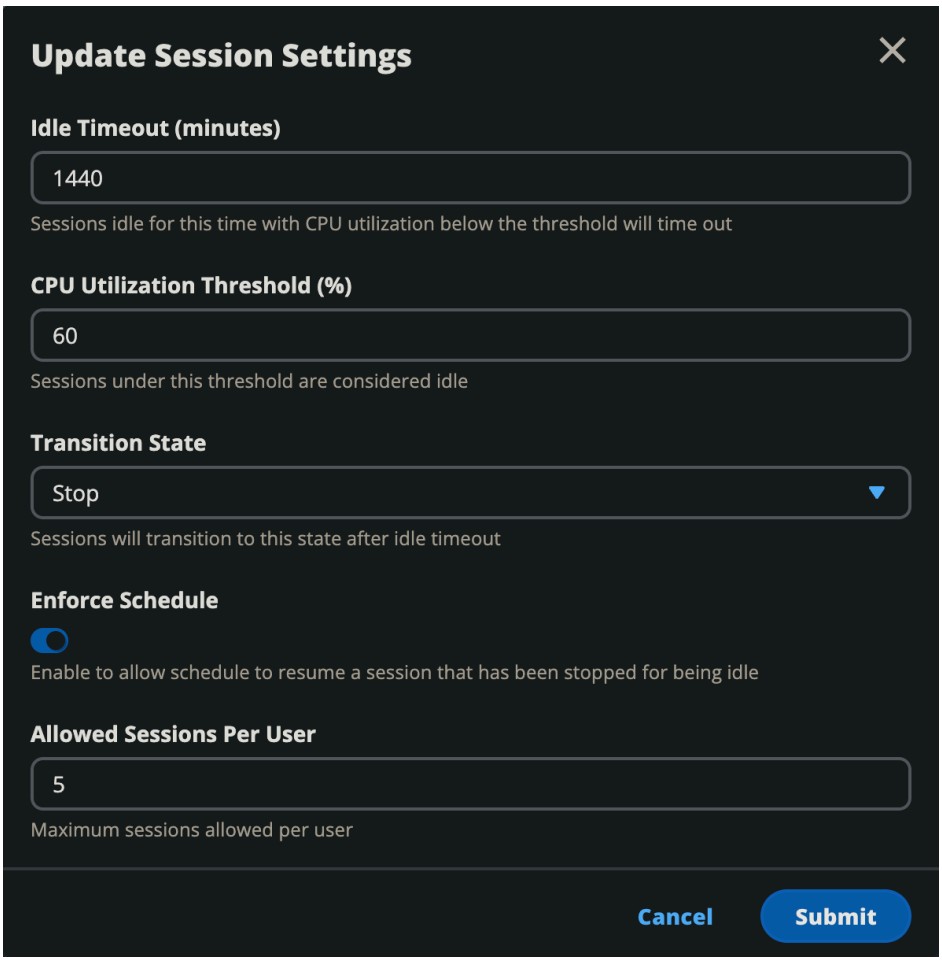
   - Nom de l'attribut = **`value`**
   - Valeur = ***`<The time>`***
   - Type = **`String`**

   La valeur horaire doit être formatée au format XX:XX à l'aide d'une horloge de 24 heures. Par exemple, 9 h 00 serait 9 h 00 tandis que 17 h serait 17 h 00. L'heure saisie correspond toujours à l'heure locale de la AWS région dans laquelle l'environnement RES est déployé.

Arrêt automatique de l'interface de bureau virtuel

Les administrateurs peuvent configurer les paramètres pour autoriser l'arrêt ou VDIs la fin de l'inactivité. Il existe 4 paramètres configurables :

1. Délai d'inactivité : les sessions inactives pendant cette période avec une utilisation du processeur inférieure au seuil expireront.
2. Seuil d'utilisation du processeur : les sessions sans interaction et inférieures à ce seuil sont considérées comme inactives. Si ce paramètre est défini sur 0, les sessions ne seront jamais considérées comme inactives.
3. État de transition : après expiration du délai d'inactivité, les sessions passeront à cet état (arrêtées ou terminées).
4. Appliquer le calendrier : si cette option est sélectionnée, une session arrêtée pour cause d'inactivité peut être reprise selon son calendrier quotidien.

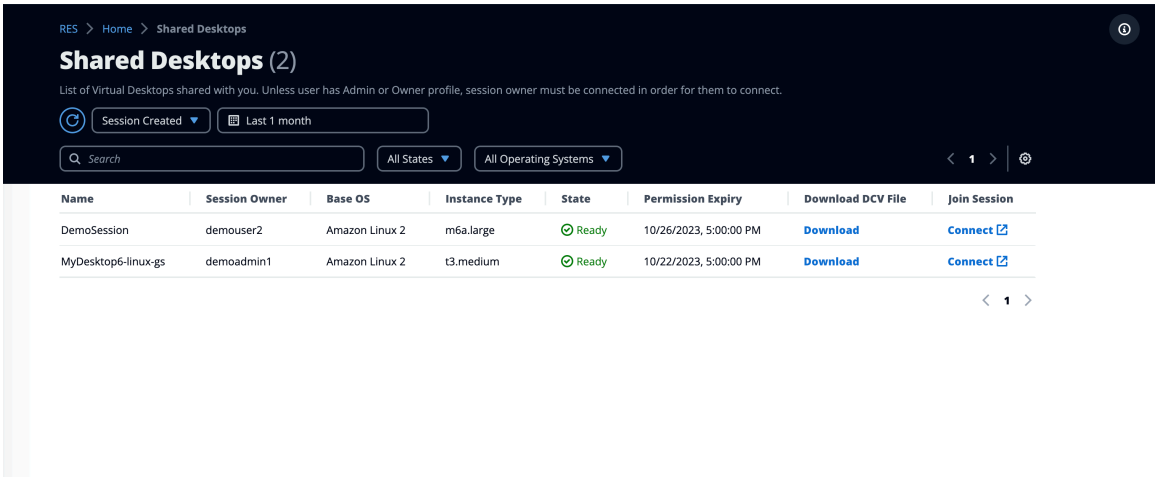


Ces paramètres sont présents sur la page Paramètres du bureau sous l'onglet Serveur. Une fois que vous avez mis à jour les paramètres en fonction de vos besoins, cliquez sur Soumettre pour enregistrer les paramètres. Les nouvelles sessions utiliseront les paramètres mis à jour, mais notez que les sessions existantes utiliseront toujours les paramètres qu'elles avaient lors de leur lancement.

Une fois le délai expiré, les sessions se termineront ou passeront à l'`STOPPED_IDLE`état en fonction de leur configuration. Les utilisateurs auront la possibilité de démarrer `STOPPED_IDLE` des sessions depuis l'interface utilisateur.

Bureaux partagés

Sur les bureaux partagés, vous pouvez voir les bureaux qui ont été partagés avec vous. Pour se connecter à un poste de travail, le propriétaire de la session doit également être connecté, sauf si vous êtes administrateur ou propriétaire.



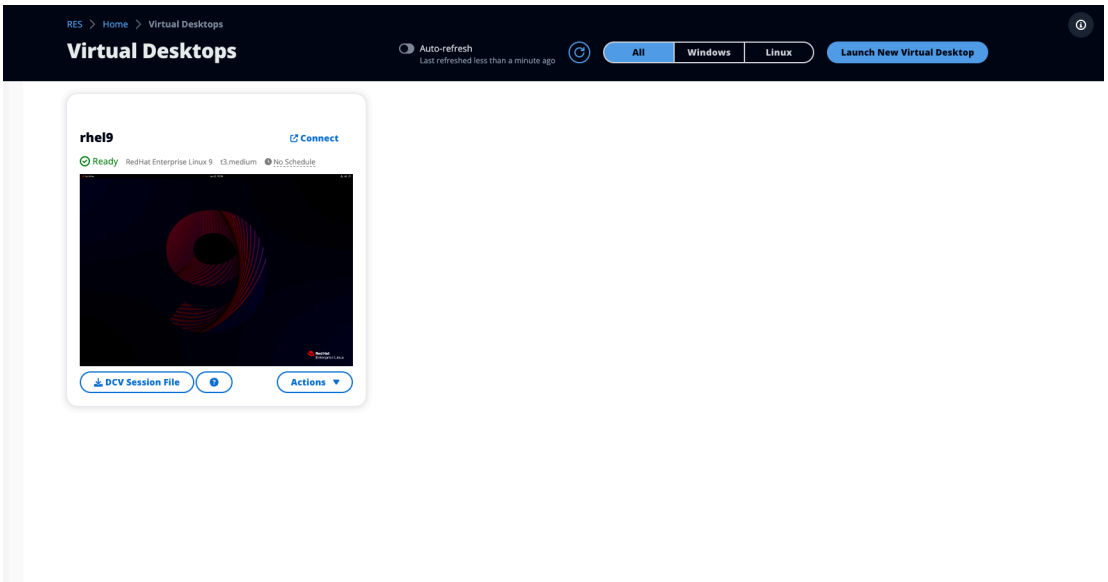
Lorsque vous partagez une session, vous pouvez configurer les autorisations pour vos collaborateurs. Par exemple, vous pouvez accorder un accès en lecture seule à un coéquipier avec lequel vous collaborez.

Rubriques

- Partage d'un ordinateur
- Accédez à un bureau partagé

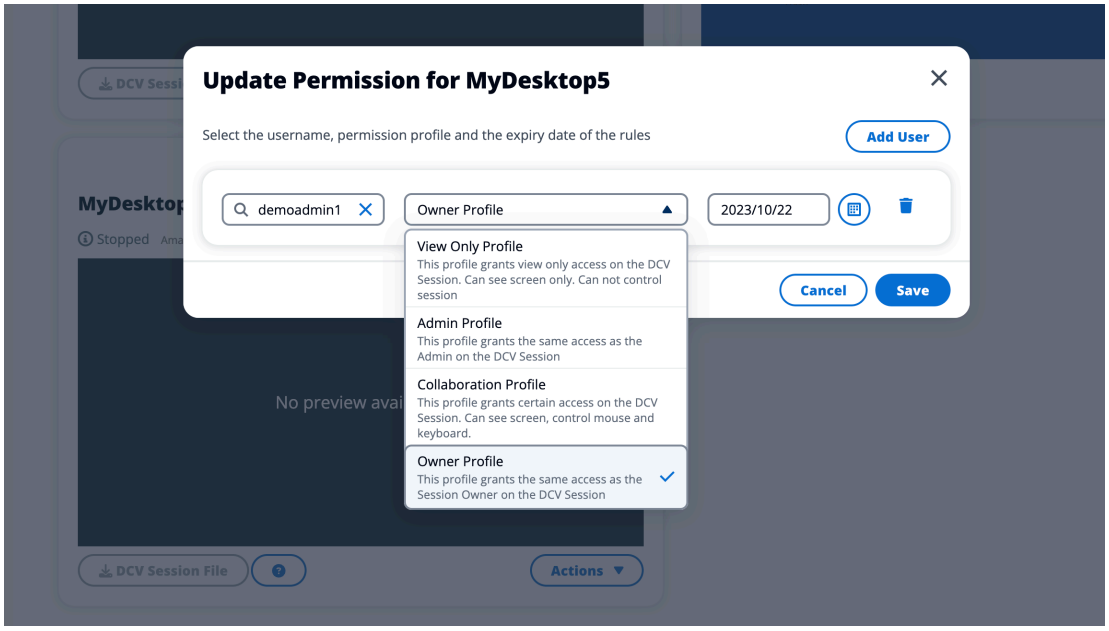
Partage d'un ordinateur

1. Dans votre session de bureau, choisissez Actions.



2. Sélectionnez Autorisations de session.

3. Sélectionnez l'utilisateur et le niveau d'autorisation. Vous pouvez également définir une date d'expiration.
4. Choisissez Enregistrer.



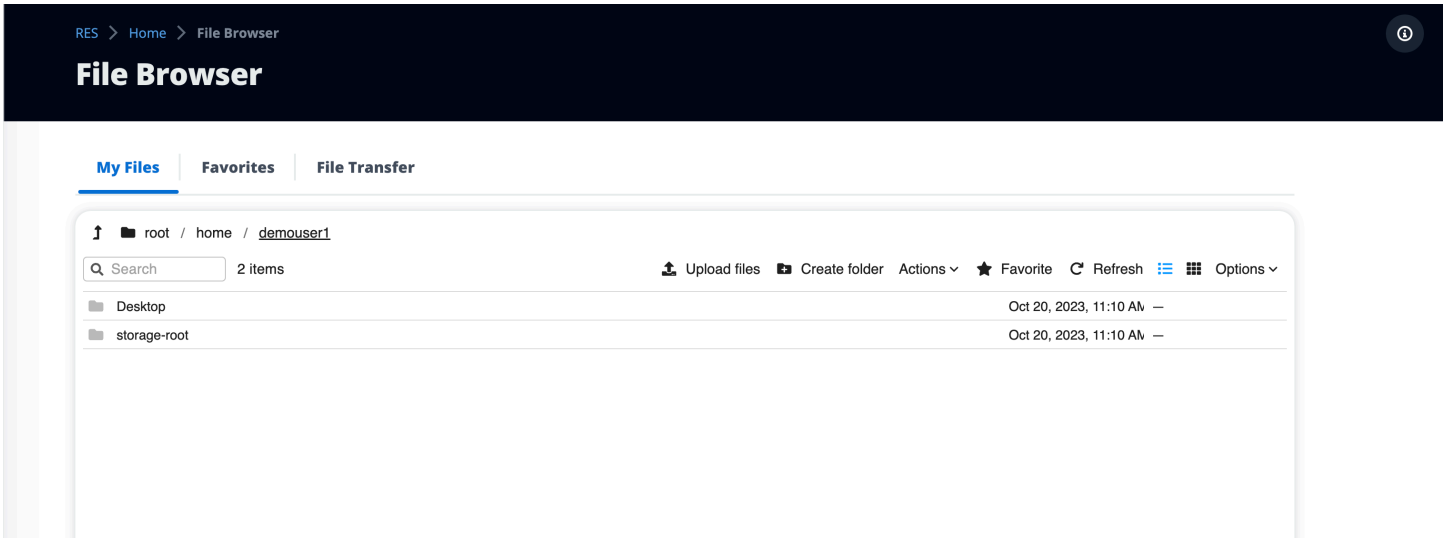
Pour plus d'informations sur les autorisations, consultezthe section called “Stratégie d'autorisation”.

Accédez à un bureau partagé

Dans Bureaux partagés, vous pouvez afficher les bureaux partagés avec vous et vous connecter à une instance. Vous pouvez vous inscrire par navigateur Web ou par DCV. Pour vous connecter, suivez les instructions indiquées dansAccédez à votre bureau.

Navigateur de fichiers

Le navigateur de fichiers vous permet d'accéder au système de fichiers EFS partagé global via le portail Web. Vous pouvez gérer tous les fichiers disponibles auxquels vous êtes autorisé à accéder sur le système de fichiers sous-jacent. Il s'agit du même système de fichiers que celui partagé par vos bureaux virtuels Linux. La mise à jour de fichiers sur votre bureau virtuel est identique à la mise à jour d'un fichier via le terminal ou un navigateur de fichiers basé sur le Web.

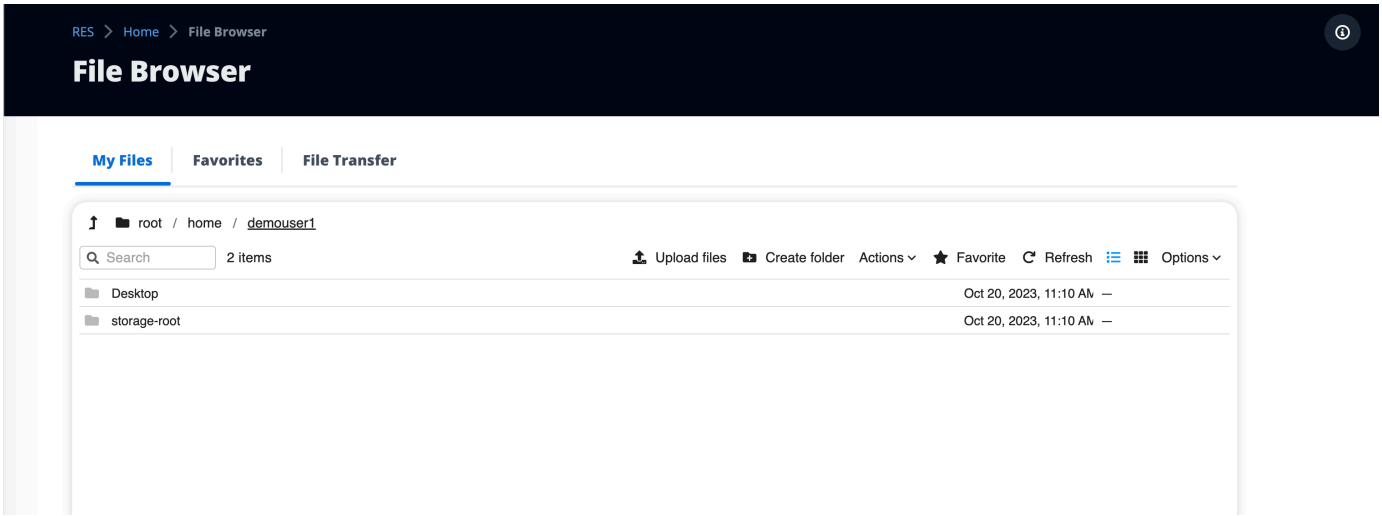


Rubriques

- Téléversez un ou plusieurs fichiers
- Supprimer un ou plusieurs fichiers
- Gérer les favoris
- Modifier des fichiers
- Transférer des fichiers

Téléversez un ou plusieurs fichiers

1. Choisissez Charger des fichiers.

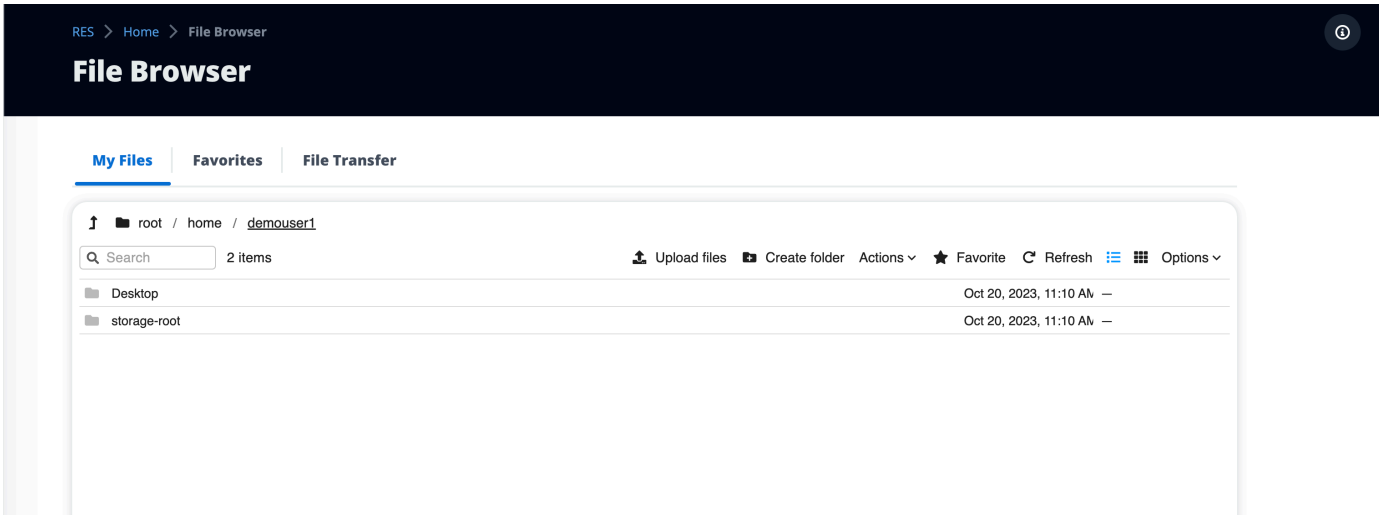


2. Déposez des fichiers ou recherchez les fichiers à télécharger.

3. Choisissez Upload (n) files.

Supprimer un ou plusieurs fichiers

1. Sélectionnez le ou les fichiers que vous souhaitez supprimer.



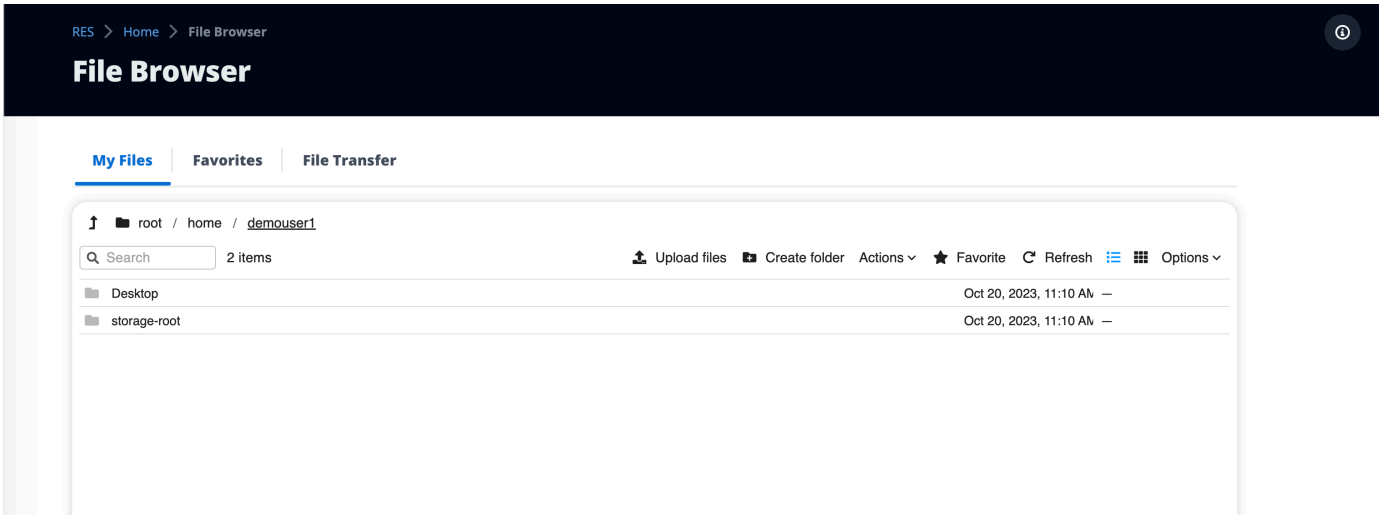
2. Choisissez Actions.
3. Sélectionnez Supprimer les fichiers.

Vous pouvez également cliquer avec le bouton droit sur un fichier ou un dossier et sélectionner Supprimer les fichiers.

Gérer les favoris

Pour épingler des fichiers et des dossiers importants, vous pouvez les ajouter aux favoris.

1. Sélectionnez un fichier ou un dossier.



2. Choisissez Favori.

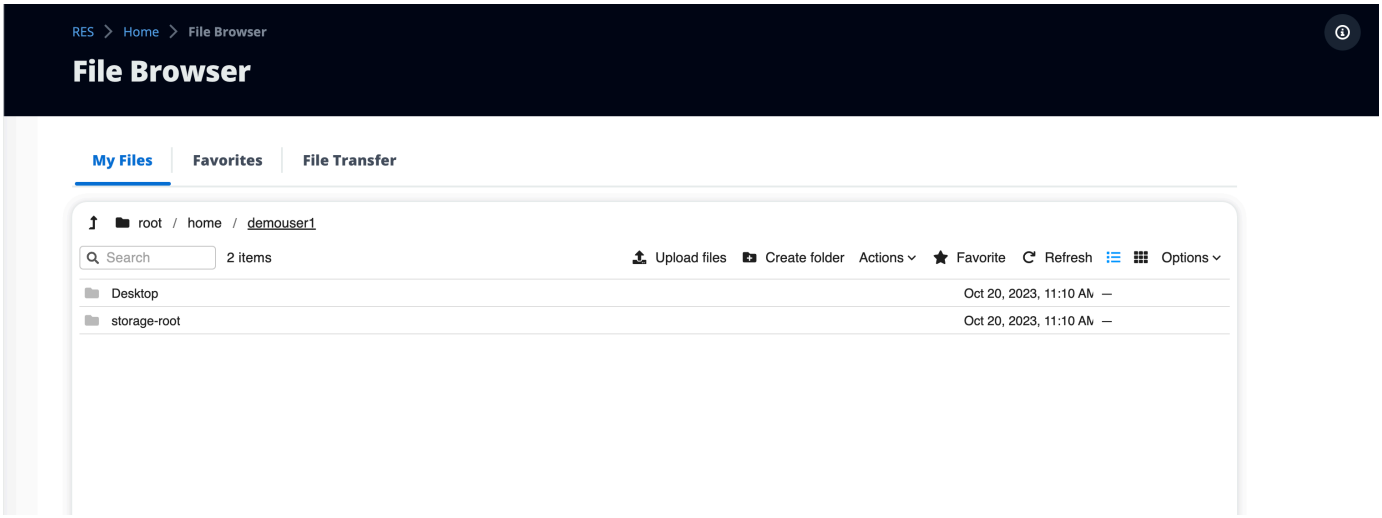
Vous pouvez également cliquer avec le bouton droit sur un fichier ou un dossier et sélectionner Favoris.

> **Note**
>
> Les favoris sont enregistrés dans le navigateur local. Si vous changez de navigateur ou si vous videz le cache, vous devrez réépingler vos favoris.

Modifier des fichiers

Vous pouvez modifier le contenu des fichiers texte dans le portail Web.

1. Sélectionnez le fichier que vous souhaitez mettre à jour. Un modal s'ouvre avec le contenu du fichier.

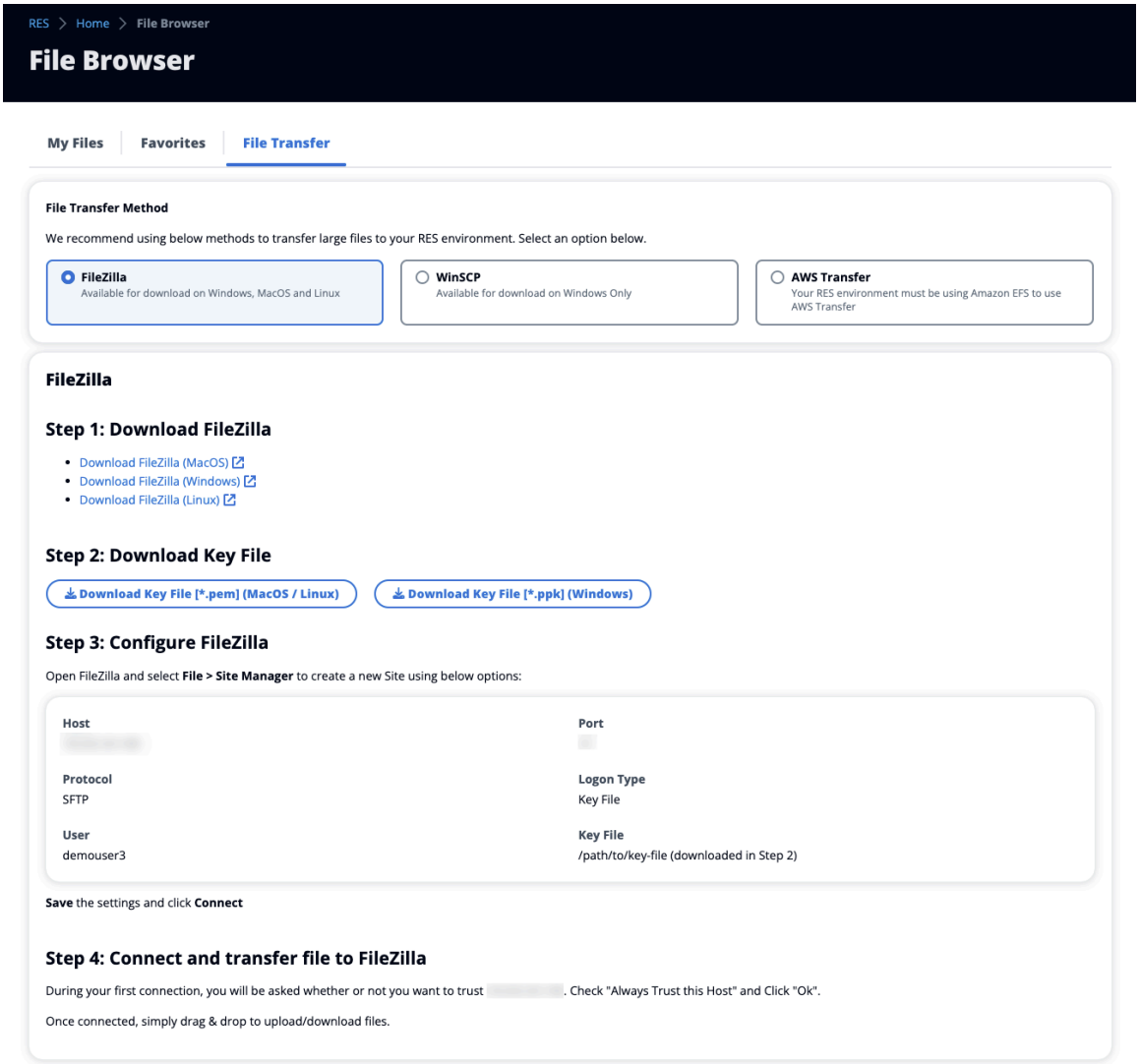


2. Effectuez vos mises à jour et choisissez Enregistrer.

Transférer des fichiers

Utilisez le transfert de fichiers pour utiliser des applications de transfert de fichiers externes pour transférer des fichiers. Vous pouvez sélectionner l'une des applications suivantes et suivre les instructions affichées à l'écran pour transférer des fichiers.

- FileZilla (Windows, macOS, Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)


RES > Home > File Browser
File Browser
My Files
Favorites
File Transfer
File Transfer Method
We recommend using below methods to transfer large files to your RES environment. Select an option below.
FileZilla
Available for download on Windows, MacOS and Linux
WinSCP
Available for download on Windows Only
AWS Transfer
Your RES environment must be using Amazon EFS to use AWS Transfer
FileZilla
Step 1: Download FileZilla
Download FileZilla (MacOS)
Download FileZilla (Windows)
Download FileZilla (Linux)
Step 2: Download Key File
Download Key File [*.pem] (MacOS / Linux)
Download Key File [*.ppk] (Windows)
Step 3: Configure FileZilla
Open FileZilla and select File > Site Manager to create a new Site using below options:
Host
Port
Protocol
SFTP
Logon Type
Key File
User
demouser3
Key File
/path/to/key-file (downloaded in Step 2)
Save the settings and click Connect
Step 4: Connect and transfer file to FileZilla
During your first connection, you will be asked whether or not you want to trust . Check "Always Trust this Host" and Click "Ok".
Once connected, simply drag & drop to upload/download files.

Résolution des problèmes

Cette section contient des informations sur la façon de surveiller le système et de résoudre les problèmes spécifiques susceptibles de survenir.

Rubriques

Contenu détaillé :

- (2024.04.02 et versions antérieures) La clé privée pour accéder à l'hôte Bastion n'est pas valide

Débogage et surveillance généraux

Cette section contient des informations sur l'endroit où les informations peuvent être trouvées dans RES.

- Sources d'informations utiles sur les journaux et les événements
  - Où trouver les variables d'environnement
  - Fichiers journaux sur les instances Amazon EC2 de l'environnement
  - CloudFormation Piles
  - Défaillances du système dues à un problème et reflétées par l'activité du groupe Amazon EC2 Auto Scaling
- Apparence typique de la console Amazon EC2
  - Hôtes d'infrastructure
  - Hôtes d'infrastructure et bureaux virtuels
  - Hôtes en état de terminaison
  - Commandes utiles liées à Active Directory (AD) à titre de référence
- Débogage de Windows DCV
- Rechercher des informations sur la version d'Amazon DCV

Sources d'informations utiles sur les journaux et les événements

Diverses sources d'informations conservées peuvent être référencées à des fins de dépannage et de surveillance.

Où trouver les variables d'environnement

Par défaut, vous pouvez trouver des variables d'environnement, telles que le nom d'utilisateur du propriétaire de la session, aux emplacements suivants :

- Linux : `/etc/environment`
- Windows: `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\environment_variables.json`

Fichiers journaux sur les instances Amazon EC2 de l'environnement

Les fichiers journaux existent sur les instances Amazon EC2 utilisées par RES. Le gestionnaire de session SSM peut être utilisé pour ouvrir une session sur l'instance afin d'examiner ces fichiers.

Sur les instances d'infrastructure telles que le gestionnaire de clusters et le contrôleur vdc, les journaux d'applications et autres se trouvent aux emplacements suivants.

- /opt/idea/app/logs/application.journal
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

Sur un bureau virtuel Linux, les fichiers suivants contiennent des fichiers journaux utiles

- /var/log/dcv/
- /root/bootstrap/logs/userdata.journal
- /var/log/messages

Sur Windows, les journaux des instances de bureau virtuel se trouvent à l'adresse

- PS C : \ ProgramData \ n ice \ dcv \ log
- PS C : \ ProgramData \ n nice \ DCVSession ManagerAgent \ log

Sous Windows, la journalisation de certaines applications se trouve à l'adresse suivante :

- PS C:\Program Files \ NICE \ DCV \ Server \ bin

Sous Windows, les fichiers du certificat DCV NICE se trouvent dans :

- C:\Windows\System32\config\systemprofile \ AppData \ Local \ NICE \ dcv \

Groupes Amazon CloudWatch Log

Amazon EC2 et les ressources de AWS Lambda calcul consignent les informations dans Amazon CloudWatch Log Groups. Les entrées du journal qu'ils contiennent peuvent fournir des informations utiles pour résoudre des problèmes potentiels ou pour obtenir des informations générales.

Ces groupes sont nommés comme suit :

- `/aws/lambda/<envname>-/ - lambda related`
- `/<envname>/`
  - `cluster-manager/ - main infrastructure host`
  - `vdc/ - virtual desktop related`
    - `dcv-broker/ - desktop related`
    - `dcv-connection-gateway/ - desktop related`
    - `controller/ - main desktop controller host`
    - `dcv-session/ - desktop session related`

Lorsque vous examinez des groupes de journaux, il peut être utile de les filtrer à l'aide de chaînes majuscules et minuscules telles que les suivantes. Cela ne produira que les messages contenant les chaînes notées.

```
?"ERROR" ?"error"
```

Une autre méthode de surveillance des problèmes consiste à créer des CloudWatch tableaux de bord Amazon contenant des widgets affichant les données qui vous intéressent.

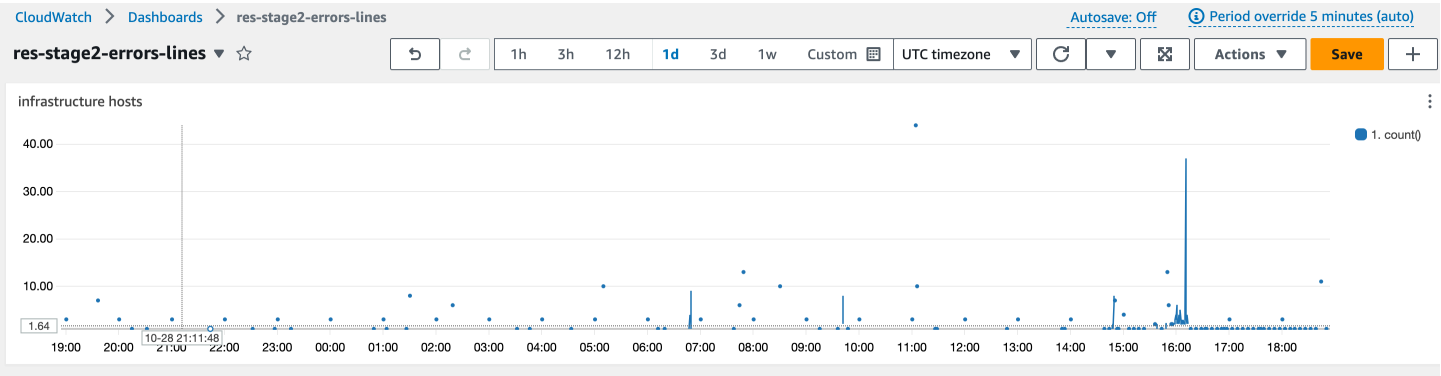
Un exemple consiste à créer un widget qui compte l'occurrence des chaînes error et ERROR et à les représenter graphiquement sous forme de lignes. Cette méthode permet de détecter plus facilement l'apparition de problèmes ou de tendances potentiels indiquant qu'un changement de modèle s'est produit.

Voici un exemple de cela pour les hôtes d'infrastructure. Pour l'utiliser, concaténez les lignes de requête et remplacez les `<region>` attributs `<envname>` et par les valeurs appropriées.

```
{
    "widgets": [
        {
            "type": "log",
```

```
            "x": 0,
            "y": 0,
            "width": 24,
            "height": 6,
            "properties": {
                "query": "SOURCE '/<envname>/vdc/controller' |
                    SOURCE '/<envname>/cluster-manager' |
                    SOURCE '/<envname>/vdc/dcv-broker' |
                   SOURCE '/<envname>/vdc/dcv-connection-gateway' |
                    fields @timestamp, @message, @logStream, @log\n|
                    filter @message like /(?i)(error|ERROR)/\n|
                    sort @timestamp desc|
                    stats count() by bin(30s)",
                "region": "<region>",
                "title": "infrastructure hosts",
                "view": "timeSeries",
                "stacked": false
            }
        }
    ]
}
```

Un exemple de tableau de bord peut apparaître comme suit :



CloudFormation Piles

Les CloudFormation piles créées lors de la création de l'environnement contiennent des informations sur les ressources, les événements et les sorties associées à la configuration de l'environnement.

Pour chacune des piles, l'onglet Événements, ressources et sorties peut être consulté pour obtenir des informations sur les piles.

piles RES :

- <envname>-sangle
- <envname>-grappe
- <envname>-métriques
- <envname>- service d'annuaire
- <envname>-fournisseur d'identité
- <envname>-stockage partagé
- <envname>-gestionnaire de clusters
- <envname>-vdc
- <envname>-bastion-hôte

Suite d'environnements de démonstration (si vous déployez un environnement de démonstration et que vous ne disposez pas de ces ressources externes, vous pouvez utiliser des recettes de calcul à AWS haute performance pour générer des ressources pour un environnement de démonstration.)

- <envname>
- <envname>-Réseautage
- <envname>- DirectoryService
- <envname>-Rangement
- <envname>- WindowsManagementHost

Défaillances du système dues à un problème et reflétées par l'activité du groupe Amazon EC2 Auto Scaling

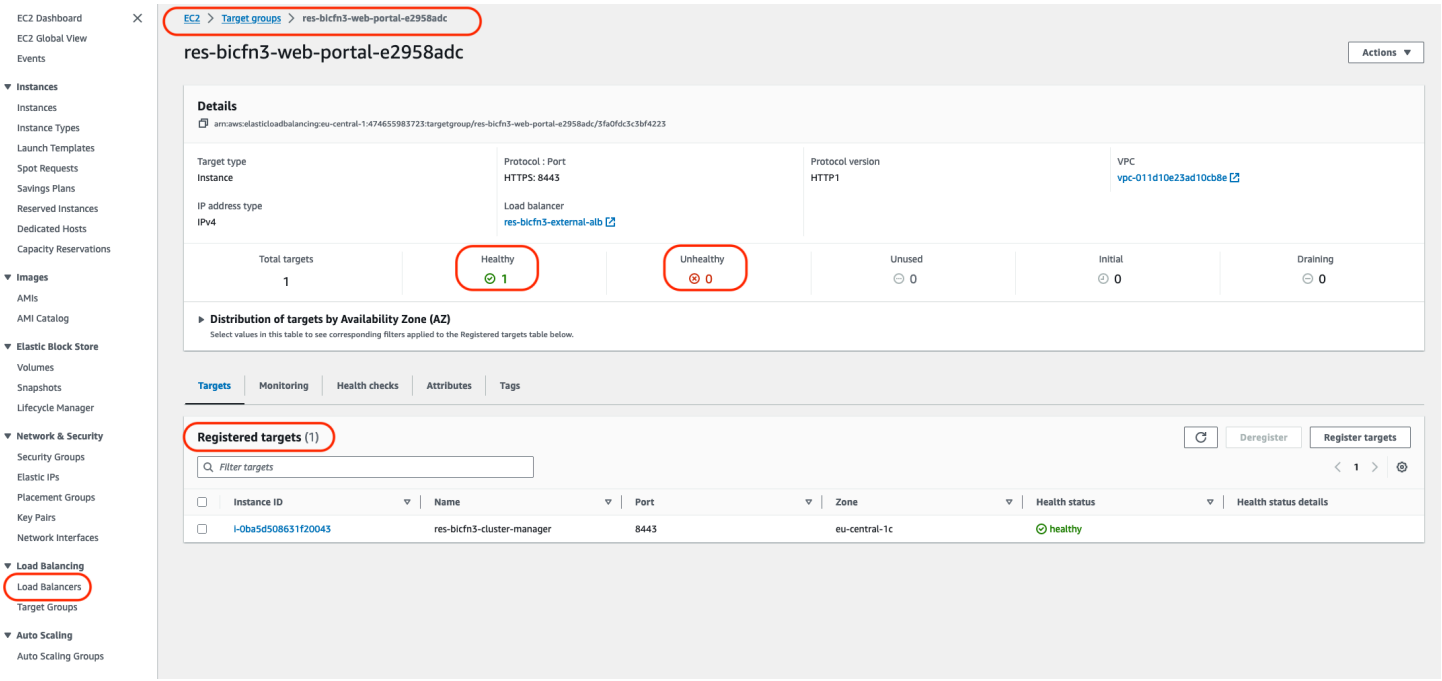
Si le RES UIs indique des erreurs de serveur, cela peut être dû à un logiciel d'application ou à un autre problème.

Chacun des groupes d'autoscaling (ASG) d'instance Amazon EC2 de l'infrastructure contient un onglet Activité qui peut être utile pour détecter l'activité de dimensionnement des instances. Si les pages de l'interface utilisateur indiquent des erreurs ou ne sont pas accessibles, vérifiez la présence de plusieurs instances résiliées sur la console Amazon EC2 et consultez l'onglet Auto Scaling Group Activity pour trouver l'ASG correspondant afin de déterminer si les instances Amazon EC2 sont cycliques.

Dans ce cas, utilisez le groupe de CloudWatch journaux Amazon associé à l'instance afin de déterminer si des erreurs susceptibles d'indiquer la cause du problème sont enregistrées. Il peut

également être possible d'utiliser la console de session SSM pour ouvrir une session sur une instance en cours d'exécution de ce type et examiner les fichiers journaux de l'instance afin d'en déterminer la cause avant que l'instance ne soit marquée comme défectueuse et interrompue par l'ASG.

La console ASG peut afficher une activité similaire à celle qui suit si ce problème se produit.

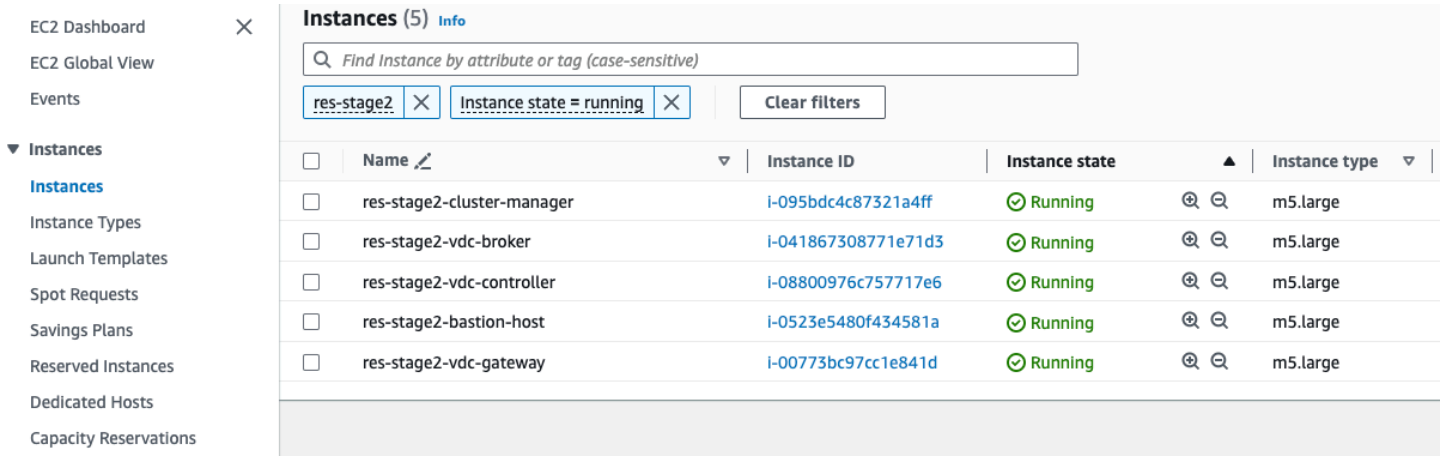


Apparence typique de la console Amazon EC2

Cette section contient des captures d'écran du système fonctionnant dans différents états.

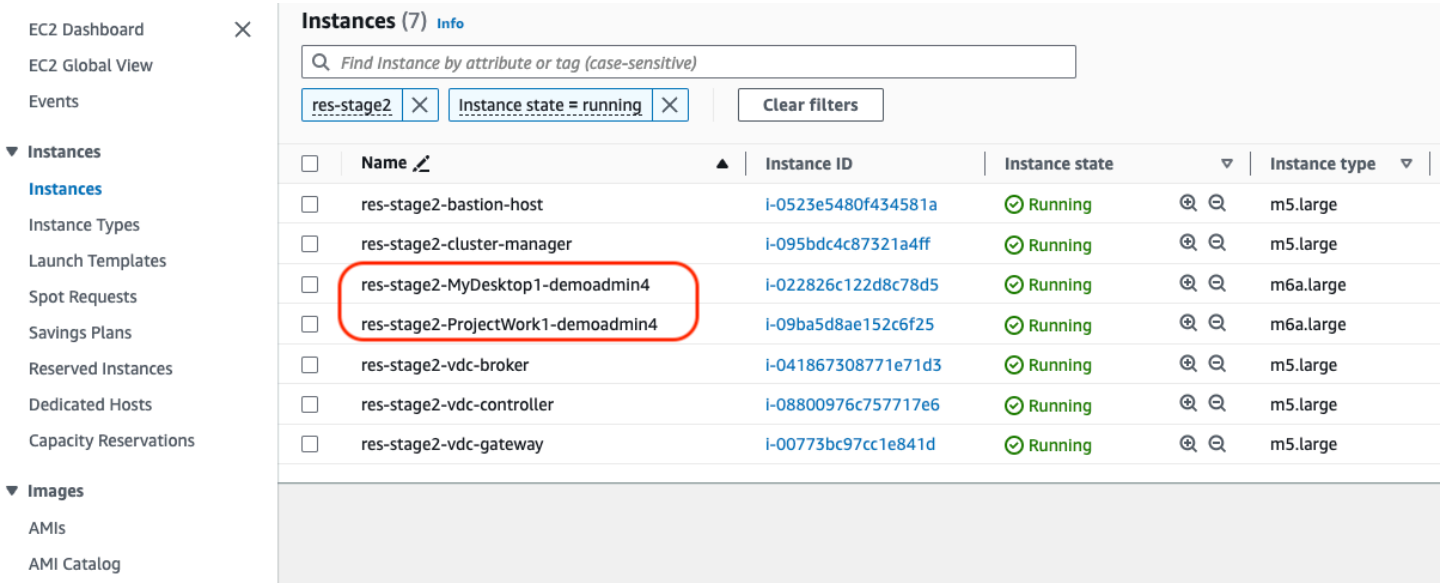
Hôtes d'infrastructure

Lorsqu'aucun bureau n'est en cours d'exécution, la console Amazon EC2 ressemble généralement à ce qui suit. Les instances présentées sont les hôtes de l'infrastructure RES Amazon EC2. Le préfixe d'un nom d'instance est le nom de l'environnement RES.



Hôtes d'infrastructure et bureaux virtuels

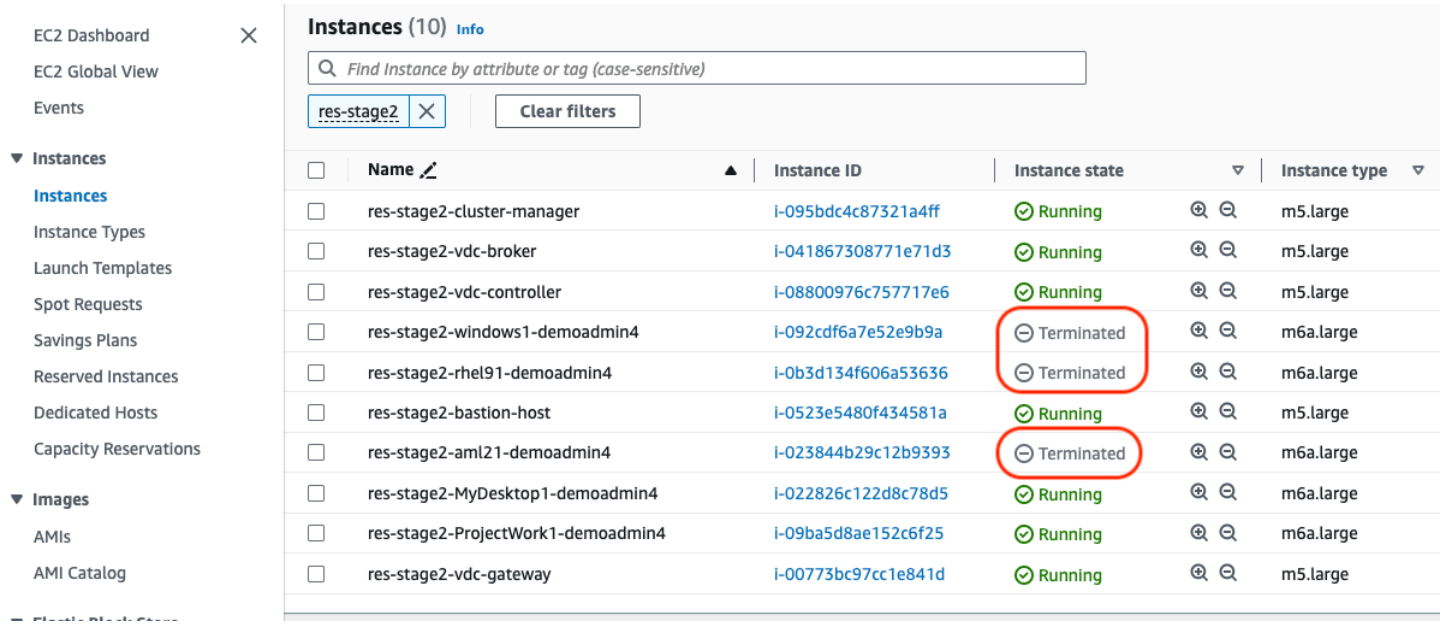
Dans la console Amazon EC2, lorsque des bureaux virtuels sont en cours d'exécution, ils ressemblent à ce qui suit. Dans ce cas, les bureaux virtuels sont indiqués en rouge. Le suffixe du nom de l'instance est l'utilisateur qui a créé le poste de travail. Le nom au centre est le nom de session défini au moment du lancement. Il s'agit soit du « MyDesktop » par défaut, soit du nom défini par l'utilisateur.



Hôtes en état de terminaison

Lorsque la console Amazon EC2 affiche des instances résiliées, il s'agit généralement d'hôtes de bureau qui ont été résiliés. Si la console inclut des hôtes d'infrastructure en état d'arrêt, en particulier s'il en existe plusieurs du même type, cela peut indiquer qu'un problème système est en cours.

L'image suivante montre les instances de bureau qui ont été mises hors service.



Commandes utiles liées à Active Directory (AD) à titre de référence

Vous trouverez ci-dessous des exemples de commandes liées au protocole LDAP qui peuvent être saisies sur les hôtes d'infrastructure pour afficher les informations relatives à la configuration AD. Le domaine et les autres paramètres utilisés doivent refléter ceux saisis au moment de la création de l'environnement.

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>
```

Débogage de Windows DCV

Sur un poste de travail Windows, vous pouvez répertorier la session qui lui est associée à l'aide de ce qui suit :

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe'list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
 name:windows1)
```

Rechercher des informations sur la version d'Amazon DCV

Amazon DCV est utilisé pour les sessions de bureau virtuel. AWS Amazon CV. Les exemples suivants montrent comment déterminer la version du logiciel DCV installée.

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

Amazon DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe' version

Amazon DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Problème RunBooks

La section suivante décrit les problèmes susceptibles de survenir, explique comment les détecter et propose des suggestions pour les résoudre.

- Problèmes d'installation
  - Je souhaite configurer des domaines personnalisés après avoir installé RES
  - CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»
  - Notification par e-mail non reçue après la création CloudFormation réussie des piles
  - Instances en cycle ou contrôleur VDC en état d'échec

Problèmes d'installation

Rubriques

.....

Je souhaite configurer des domaines personnalisés après avoir installé RES

> **Note**
>
> Conditions préalables : Vous devez stocker le certificat et PrivateKey son contenu dans un secret Secrets Manager avant d'effectuer ces étapes.

Ajouter des certificats au client Web

1. Mettez à jour le certificat attaché à l'écouteur de l'équilibreur de charge external-alb :
   a. Accédez à l'équilibreur de charge externe RES dans la AWS console sous EC2 > Équilibrage de charge > Équilibreurs de charge.
   b. Recherchez l'équilibreur de charge qui respecte la convention `<env-name>-external-alb` de dénomination.
   c. Vérifiez les écouteurs connectés à l'équilibreur de charge.

d. Mettez à jour l'écouteur auquel un SSL/TLS certificat par défaut est attaché avec les détails du nouveau certificat.

e. Enregistrez vos modifications.

2. Dans le tableau des paramètres du cluster :

a. Trouvez la table des paramètres du cluster dans DynamoDB -> Tables ->. *<env-name>*`.cluster-settings`

b. Accédez à Explorer les éléments et filtrez par attribut : nom « clé », type « chaîne », condition « contient » et valeur « external_alb ».

c. Réglé `cluster.load_balancers.external_alb.certificates.provided` sur True.

d. Mettez à jour la valeur `decluster.load_balancers.external_alb.certificates.custom_dns_name`. Il s'agit du nom de domaine personnalisé pour l'interface utilisateur Web.

e. Mettez à jour la valeur `decluster.load_balancers.external_alb.certificates.acm_certificate_arn`. Il s'agit de l'Amazon Resource Name (ARN) du certificat correspondant stocké dans Amazon Certificate Manager (ACM).

3. Mettez à jour l'enregistrement de sous-domaine Route53 correspondant que vous avez créé pour votre client Web afin qu'il pointe vers le nom DNS de l'équilibreur de charge alb externe. `<env-name>-external-alb`

4. Si l'authentification unique est déjà configurée dans l'environnement, reconfigurez l'authentification unique avec les mêmes entrées que celles que vous avez utilisées initialement depuis le bouton Gestion de l'environnement > Gestion des identités > Authentification unique > État > Modifier du portail Web RES.

Ajoutez des certificats au VDIs

1. Accordez à l'application RES l'autorisation d'effectuer une GetSecret opération sur le secret en ajoutant les balises suivantes au secret :

- `res:EnvironmentName` : *<env-name>*
- `res:ModuleName` : `virtual-desktop-controller`

2. Dans le tableau des paramètres du cluster :

a. Trouvez la table des paramètres du cluster dans DynamoDB -> Tables ->. *<env-name>*`.cluster-settings`

b. Accédez à Explorer les éléments et filtrez par attribut : nom « clé », type « chaîne », condition « contient » et valeur « dcv_connection_gateway ».

c. Réglé `vdc.dcv_connection_gateway.certificate.provided` sur True.

d. Mettez à jour la valeur `devdc.dcv_connection_gateway.certificate.custom_dns_name`. Il s'agit du nom de domaine personnalisé pour l'accès VDI.

e. Mettez à jour la valeur `devdc.dcv_connection_gateway.certificate.certificate_secret_arn`. Il s'agit de l'ARN du secret qui contient le contenu du certificat.

f. Mettez à jour la valeur `devdc.dcv_connection_gateway.certificate.private_key_secret_arn`. Il s'agit de l'ARN du secret qui contient le contenu de la clé privée.

3. Mettez à jour le modèle de lancement utilisé pour l'instance de passerelle :

a. Ouvrez le groupe Auto Scaling dans la AWS console sous EC2 > Auto Scaling > Auto Scaling Groups.

b. Sélectionnez le groupe de mise à l'échelle automatique de la passerelle qui correspond à l'environnement RES. Le nom suit la convention de dénomination*<env-name>*`-vdc-gateway-asg`.

c. Recherchez et ouvrez le modèle de lancement dans la section des détails.

d. Sous Détails > Actions > choisissez Modifier le modèle (Créer une nouvelle version).

e. Faites défiler l'écran vers le bas jusqu'à Détails avancés.

f. Faites défiler l'écran jusqu'en bas, jusqu'à Données utilisateur.

g. Recherchez les mots `CERTIFICATE_SECRET_ARN` et`PRIVATE_KEY_SECRET_ARN`. Mettez à jour ces valeurs avec les ARNs informations fournies aux secrets qui contiennent le contenu du certificat (voir étape 2.c) et de la clé privée (voir étape 2.d).

h. Assurez-vous que le groupe Auto Scaling est configuré pour utiliser la version récemment créée du modèle de lancement (depuis la page du groupe Auto Scaling).

4. Mettez à jour l'enregistrement de sous-domaine Route53 correspondant que vous avez créé pour vos bureaux virtuels afin qu'il pointe vers le nom DNS de l'équilibreur de charge nlb externe :. *<env-name>*`-external-nlb`

5. Mettez fin à l'instance dcv-gateway existante : `<env-name>-vdc-gateway` et attendez qu'une nouvelle instance démarre.

.....

CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»

Pour identifier le problème, examinez le groupe de CloudWatch journaux Amazon nommé`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. S'il existe plusieurs groupes de journaux portant le même nom, examinez le premier disponible. Un message d'erreur dans les journaux fournira plus d'informations sur le problème.

> **Note**
>
> Vérifiez que les valeurs des paramètres ne comportent pas d'espaces.

.....

Notification par e-mail non reçue après la création CloudFormation réussie des piles

Si aucune invitation par e-mail n'a été reçue après la création réussie des CloudFormation piles, vérifiez les points suivants :

1. Vérifiez que le paramètre d'adresse e-mail a été correctement saisi.

   Si l'adresse e-mail est incorrecte ou n'est pas accessible, supprimez et redéployez l'environnement Research and Engineering Studio.
2. Consultez la console Amazon EC2 pour trouver des preuves de l'existence d'instances cycliques.

   Si certaines instances Amazon EC2 avec le `<envname>` préfixe apparaissent comme terminées puis sont remplacées par une nouvelle instance, il se peut qu'il y ait un problème avec le réseau ou la configuration d'Active Directory.
3. Si vous avez déployé les recettes AWS High Performance Compute pour créer vos ressources externes, vérifiez que le VPC, les sous-réseaux privés et publics et les autres paramètres sélectionnés ont été créés par la pile.

Si l'un des paramètres est incorrect, vous devrez peut-être supprimer et redéployer l'environnement RES. Pour de plus amples informations, veuillez consulter Désinstallez le produit.

4. Si vous avez déployé le produit avec vos propres ressources externes, vérifiez que le réseau et Active Directory correspondent à la configuration attendue.

   Il est essentiel de confirmer que les instances d'infrastructure ont bien rejoint Active Directory. Essayez les étapes ci-dessous the section called "Instances en cycle ou contrôleur VDC en état d'échec" pour résoudre le problème.

.....

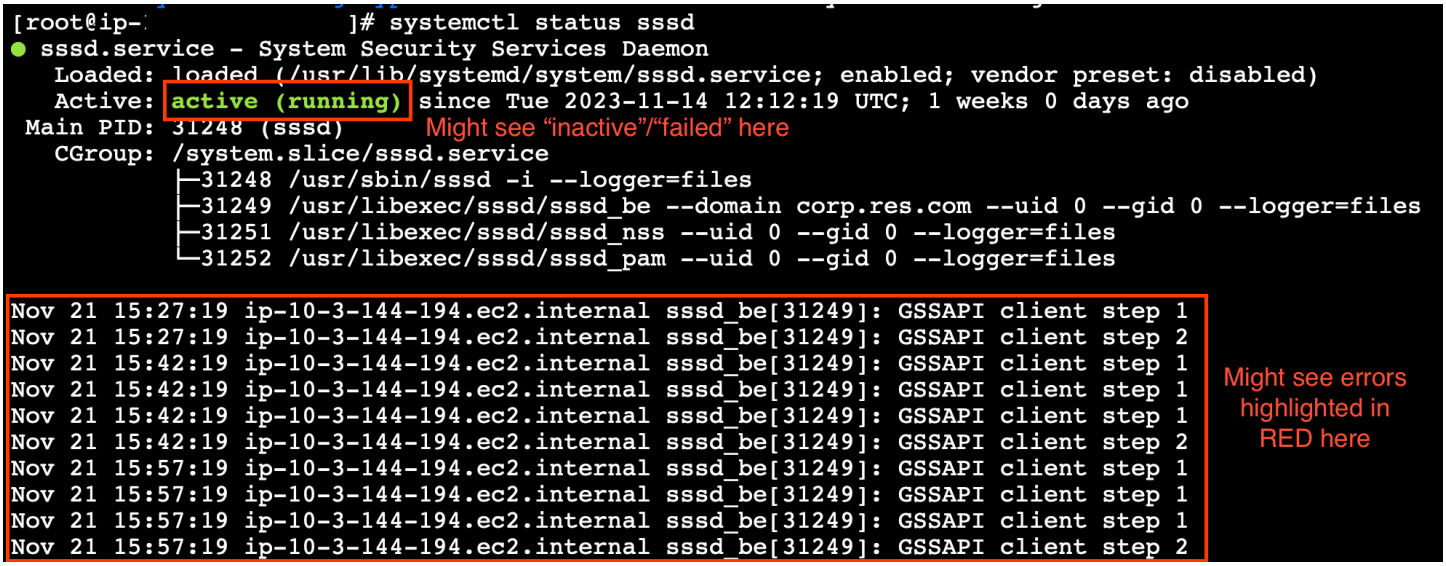
Instances en cycle ou contrôleur VDC en état d'échec

La cause la plus probable de ce problème est l'incapacité des ressources à se connecter ou à rejoindre Active Directory.

Pour vérifier le problème, procédez comme suit :

1. À partir de la ligne de commande, démarrez une session avec SSM sur l'instance en cours d'exécution du vdc-controller.
2. Exécutez `sudo su -`.
3. Exécutez `systemctl status sssd`.

Si le statut est inactif, en échec ou si des erreurs apparaissent dans les journaux, cela signifie que l'instance n'a pas pu rejoindre Active Directory.



Journal des erreurs SSM

Pour résoudre le problème, procédez comme suit :

- À partir de la même instance de ligne de commande, exécutez `cat /root/bootstrap/logs/userdata.log` pour examiner les journaux.

Le problème peut avoir l'une des trois causes profondes possibles.

Cause première 1 : informations de connexion LDAP saisies incorrectes

Passez en revue les journaux. Si le message suivant se répète plusieurs fois, cela signifie que l'instance n'a pas pu rejoindre Active Directory.

```
+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))
```

1. Vérifiez que les valeurs des paramètres suivants ont été saisies correctement lors de la création de la pile RES.

   - directoryservice.ldap_connection_uri
   - directoryservice.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - directoryservice.name

2. Mettez à jour les valeurs incorrectes dans la table DynamoDB. La table se trouve dans la console DynamoDB sous Tables. Le nom de la table doit être*<stack name>*`.cluster-settings`.
3. Après avoir mis à jour la table, supprimez le gestionnaire de clusters et le contrôleur vdc qui exécutent actuellement les instances de l'environnement. Le dimensionnement automatique démarrera de nouvelles instances en utilisant les dernières valeurs de la table DynamoDB.

Cause première 2 : ServiceAccount nom d'utilisateur saisi incorrect

Si les journaux sont renvoyés`Insufficient permissions to modify computer account`, le ServiceAccount nom saisi lors de la création de la pile est peut-être incorrect.

1. Depuis la AWS console, ouvrez Secrets Manager.
2. Recherchez `directoryserviceServiceAccountUsername`. Le secret devrait être*<stack name>*`-directoryservice-ServiceAccountUsername`.
3. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis Texte en clair.
4. Si la valeur a été mise à jour, supprimez les instances de cluster-manager et vdc-controller en cours d'exécution de l'environnement. Auto Scaling démarrera de nouvelles instances en utilisant la dernière valeur de Secrets Manager.

Cause première 3 : ServiceAccount mot de passe saisi incorrect

Si les journaux s'affichent`Invalid credentials`, le ServiceAccount mot de passe saisi lors de la création de la pile est peut-être incorrect.

1. Depuis la AWS console, ouvrez Secrets Manager.
2. Recherchez `directoryserviceServiceAccountPassword`. Le secret devrait être`<stack name>-directoryservice-ServiceAccountPassword`.
3. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis Texte en clair.
4. Si vous avez oublié le mot de passe ou si vous n'êtes pas certain que le mot de passe saisi est correct, vous pouvez le réinitialiser dans Active Directory et Secrets Manager.

    a. Pour réinitialiser le mot de passe dans AWS Managed Microsoft AD :

        i. Ouvrez la AWS console et accédez à Directory Service.

        ii. Sélectionnez l'ID de répertoire pour votre répertoire RES, puis choisissez Actions.

        iii. Sélectionnez Réinitialiser le mot de passe utilisateur.

        iv. Entrez le ServiceAccount nom d'utilisateur.

        v. Entrez un nouveau mot de passe, puis choisissez Réinitialiser le mot de passe.

    b. Pour réinitialiser le mot de passe dans Secrets Manager, procédez comme suit :

        i. Ouvrez la AWS console et accédez à Secrets Manager.

        ii. Recherchez `directoryserviceServiceAccountPassword`. Le secret devrait être`<stack name>-directoryservice-ServiceAccountPassword`.

        iii. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis choisissez Texte en clair.

        iv. Choisissez Modifier.

        v. Définissez un nouveau mot de passe pour l' ServiceAccount utilisateur et choisissez Enregistrer.

5. Si vous avez mis à jour la valeur, supprimez les instances de cluster-manager et vdc-controller en cours d'exécution de l'environnement. La mise à l'échelle automatique démarrera les nouvelles instances en utilisant la dernière valeur.

.....

La CloudFormation pile d'environnements ne parvient pas à être supprimée en raison d'une erreur d'objet dépendant

Si la suppression de la *<env-name>*-vdc CloudFormation pile échoue en raison d'une erreur d'objet dépendant telle que lavdcdcvhostsecuritygroup, cela peut être dû à une instance Amazon EC2 lancée dans un sous-réseau ou un groupe de sécurité créé par RES à l'aide de la console. AWS

Pour résoudre le problème, recherchez et mettez fin à toutes les instances Amazon EC2 lancées de cette manière. Vous pouvez ensuite reprendre la suppression de l'environnement.

.....

Erreur rencontrée pour le paramètre de bloc CIDR lors de la création de l'environnement

Lors de la création d'un environnement, une erreur apparaît pour le paramètre de bloc CIDR avec un statut de réponse de [FAILED].

Exemple d'erreur :

```
Failed to update cluster prefix list:
        An error occurred (InvalidParameterValue) when calling the
 ModifyManagedPrefixList operation:
        The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
 in the following form: 10.0.0.0/16.
```

Pour résoudre le problème, le format attendu est x.x.x.0/24 ou x.x.x.0/32.

.....

CloudFormation échec de création de pile lors de la création de l'environnement

La création d'un environnement implique une série d'opérations de création de ressources. Dans certaines régions, un problème de capacité peut survenir et entraîner l'échec de la création d'une CloudFormation pile.

Dans ce cas, supprimez l'environnement et réessayez de le créer. Vous pouvez également réessayer la création dans une autre région.

.....

La création d'une pile de ressources externes (démo) échoue avec AdDomainAdminNode CREATE_FAILED

Si la création de la pile d'environnement de démonstration échoue avec l'erreur suivante, cela peut être dû au fait que l'application de correctifs Amazon EC2 s'est produite de manière inattendue lors du provisionnement après le lancement de l'instance.

```
AdDomainAdminNode CREATE_FAILED  Failed to receive 1 resource signal(s) within the
 specified duration
```

Pour déterminer la cause de l'échec, procédez comme suit :

1. Dans le gestionnaire d'état SSM, vérifiez si les correctifs sont configurés et s'ils sont configurés pour toutes les instances.
2. Dans l'historique RunCommand/Automation d'exécution du SSM, vérifiez si l'exécution d'un document SSM lié aux correctifs coïncide avec le lancement d'une instance.
3. Dans les fichiers journaux des instances Amazon EC2 de l'environnement, consultez la journalisation des instances locales pour déterminer si l'instance a redémarré pendant le provisionnement.

Si le problème est dû à l'application de correctifs, retardez l'application des correctifs pour les instances RES au moins 15 minutes après le lancement.

.....

Problèmes liés à la gestion des identités

La plupart des problèmes liés à l'authentification unique (SSO) et à la gestion des identités sont dus à une mauvaise configuration. Pour plus d'informations sur la configuration de votre configuration SSO, voir :

- the section called “Configuration du SSO avec IAM Identity Center”
- the section called “Configuration de votre fournisseur d'identité pour le SSO”

Pour résoudre d'autres problèmes liés à la gestion des identités, consultez les rubriques de résolution des problèmes suivantes :

Rubriques

- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources
- Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion
- Erreur « Utilisateur introuvable » lors de la tentative de connexion
- Utilisateur ajouté dans Active Directory, mais absent de RES
- Utilisateur non disponible lors de la création d'une session
- Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters

.....

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à exécuter l'PassRole action iam :, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à RES.

Certains AWS services vous permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé marymajor essaie d'utiliser la console pour effectuer une action dans RES. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'effectuer l'PassRole action iam :. Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

.....

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir comment fournir un accès à vos ressources sur les AWS comptes que vous possédez, consultez la section Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les rôles IAM diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

.....

Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion

Ce problème se produit lorsque votre intégration SSO est mal configurée. Pour déterminer le problème, consultez les journaux de l'instance du contrôleur et vérifiez que les paramètres de configuration ne contiennent pas d'erreurs.

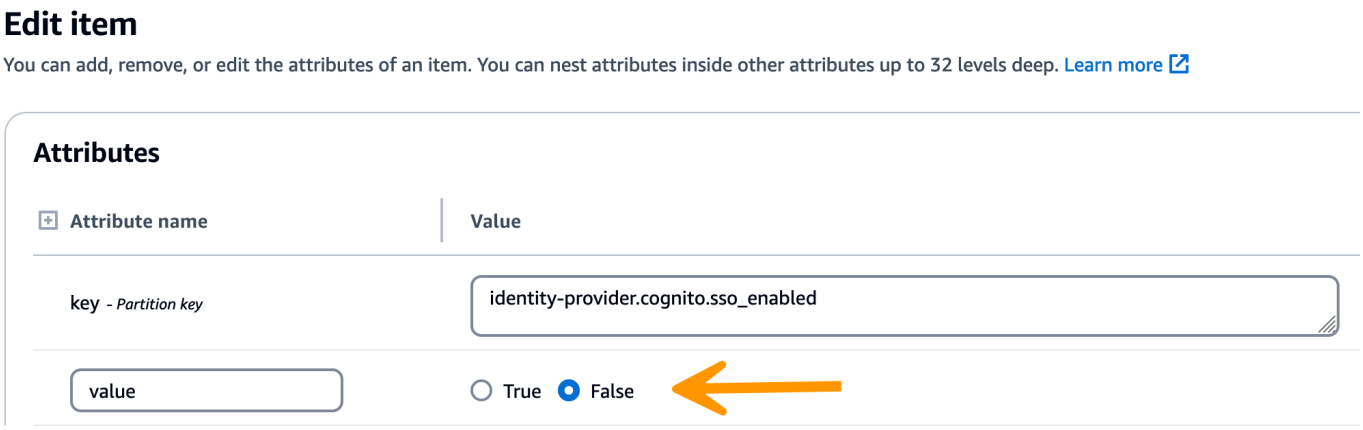
Pour consulter les journaux :

1. Ouvrez la CloudWatch console.
2. Dans Groupes de journaux, recherchez le groupe nommé/*<environment-name>*/cluster-manager.

3. Ouvrez le groupe de journaux pour rechercher d'éventuelles erreurs dans les flux de journaux.

Pour vérifier les paramètres de configuration :

1. Ouvrez la console DynamoDB
2. Dans Tables, recherchez la table nommée`<environment-name>.cluster-settings`.
3. Ouvrez le tableau et choisissez Explorer les éléments du tableau.
4. Développez la section des filtres et entrez les variables suivantes :
   - Nom de l'attribut — clé
   - État — contient
   - Valeur — SSO
5. Cliquez sur Exécuter.
6. Dans la chaîne renvoyée, vérifiez que les valeurs de configuration SSO sont correctes. S'ils sont incorrects, remplacez la valeur de la clé sso_enabled par False.



7. Retournez à l'interface utilisateur RES pour reconfigurer le SSO.

.....

Erreur « Utilisateur introuvable » lors de la tentative de connexion

Si un utilisateur reçoit le message d'erreur « Utilisateur introuvable » lorsqu'il essaie de se connecter à l'interface RES, alors que l'utilisateur est présent dans Active Directory :

- Si l'utilisateur n'est pas présent dans RES et que vous l'avez récemment ajouté à AD
  - Il est possible que l'utilisateur ne soit pas encore synchronisé avec RES. RES se synchronise toutes les heures, vous devrez donc peut-être attendre et vérifier que l'utilisateur a été ajouté après la prochaine synchronisation. Pour synchroniser immédiatement, suivez les étapes décrites dansUtilisateur ajouté dans Active Directory, mais absent de RES.
- Si l'utilisateur est présent dans RES :
  1. Assurez-vous que le mappage des attributs est correctement configuré. Pour de plus amples informations, veuillez consulter Configuration de votre fournisseur d'identité pour l'authentification unique (SSO).
  2. Assurez-vous que l'objet et l'e-mail SAML correspondent tous deux à l'adresse e-mail de l'utilisateur.

.....

Utilisateur ajouté dans Active Directory, mais absent de RES

> **Note**
>
> Cette section s'applique à RES 2024.10 et versions antérieures. Pour RES 2024.12 et versions ultérieures, voir. Comment exécuter manuellement la synchronisation (versions 2024.12 et 2024.12.01) Pour RES 2025.03 et versions ultérieures, voir. Comment démarrer ou arrêter manuellement la synchronisation (versions 2025.03 et ultérieures)

Si vous avez ajouté un utilisateur à Active Directory mais qu'il est absent de RES, la synchronisation AD doit être déclenchée. La synchronisation AD est effectuée toutes les heures par une fonction Lambda qui importe des entrées AD dans l'environnement RES. Parfois, il y a un délai avant l'exécution du prochain processus de synchronisation après l'ajout de nouveaux utilisateurs ou groupes. Vous pouvez lancer la synchronisation manuellement depuis le service Amazon Simple Queue.

Lancez le processus de synchronisation manuellement :

1. Ouvrez la console Amazon SQS.
2. Dans Files d'attente, sélectionnez`<environment-name>-cluster-manager-tasks.fifo`.
3. Choisissez Envoyer et recevoir des messages.

4. Dans le champ Corps du message, entrez :

   `{ "name": "adsync.sync-from-ad", "payload": {} }`

5. Pour l'ID du groupe de messages, entrez : **`adsync.sync-from-ad`**
6. Pour l'ID de déduplication des messages, entrez une chaîne alphanumérique aléatoire. Cette entrée doit être différente de tous les appels effectués au cours des cinq minutes précédentes, sinon la demande sera ignorée.

.....

Utilisateur non disponible lors de la création d'une session

Si vous êtes un administrateur qui crée une session, mais que vous constatez qu'un utilisateur figurant dans Active Directory n'est pas disponible lors de la création d'une session, il se peut que l'utilisateur doive se connecter pour la première fois. Les sessions ne peuvent être créées que pour les utilisateurs actifs. Les utilisateurs actifs doivent se connecter à l'environnement au moins une fois.

.....

Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11,
 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

Si vous recevez cette erreur dans le journal du CloudWatch gestionnaire de clusters, la recherche LDAP a peut-être renvoyé trop d'enregistrements utilisateur. Pour résoudre ce problème, augmentez la limite de résultats de recherche LDAP de votre fournisseur de services Internet.

.....

Stockage

Rubriques

- J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI
- J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI
- Je ne parviens pas à read/write le faire à partir d'hôtes VDI

- J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine

.....

J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI

Les systèmes de fichiers doivent être dans l'état « Disponible » avant de pouvoir être montés par des hôtes VDI. Suivez les étapes ci-dessous pour vérifier que le système de fichiers est dans l'état requis.

Amazon EFS

1. Accédez à la console Amazon EFS.
2. Vérifiez que l'état du système de fichiers est disponible.
3. Si l'état du système de fichiers n'est pas disponible, attendez avant de lancer les hôtes VDI.

Amazon FSx ONTAP

1. Accédez à la FSx console Amazon.
2. Vérifiez que le statut est disponible.
3. Si le statut n'est pas disponible, attendez avant de lancer les hôtes VDI.

.....

J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI

Les systèmes de fichiers intégrés à RES doivent avoir les règles de groupe de sécurité requises configurées pour permettre aux hôtes VDI de monter les systèmes de fichiers. Ces systèmes de fichiers étant créés en externe à RES, RES ne gère pas les règles de groupe de sécurité associées.

Le groupe de sécurité associé aux systèmes de fichiers intégrés doit autoriser le trafic entrant suivant :

- Trafic NFS (port : 2049) depuis les hôtes Linux VDC
- Trafic SMB (port : 445) depuis les hôtes Windows VDC

.....

Je ne parviens pas à read/write le faire à partir d'hôtes VDI

ONTAP prend en charge les styles de sécurité UNIX, NTFS et MIXED pour les volumes. Les styles de sécurité déterminent le type d'autorisations qu'ONTAP utilise pour contrôler l'accès aux données et le type de client qui peut modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole d'ONTAP. ONTAP utilise toutefois des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Exemples de cas d'utilisation relatifs à la gestion des autorisations

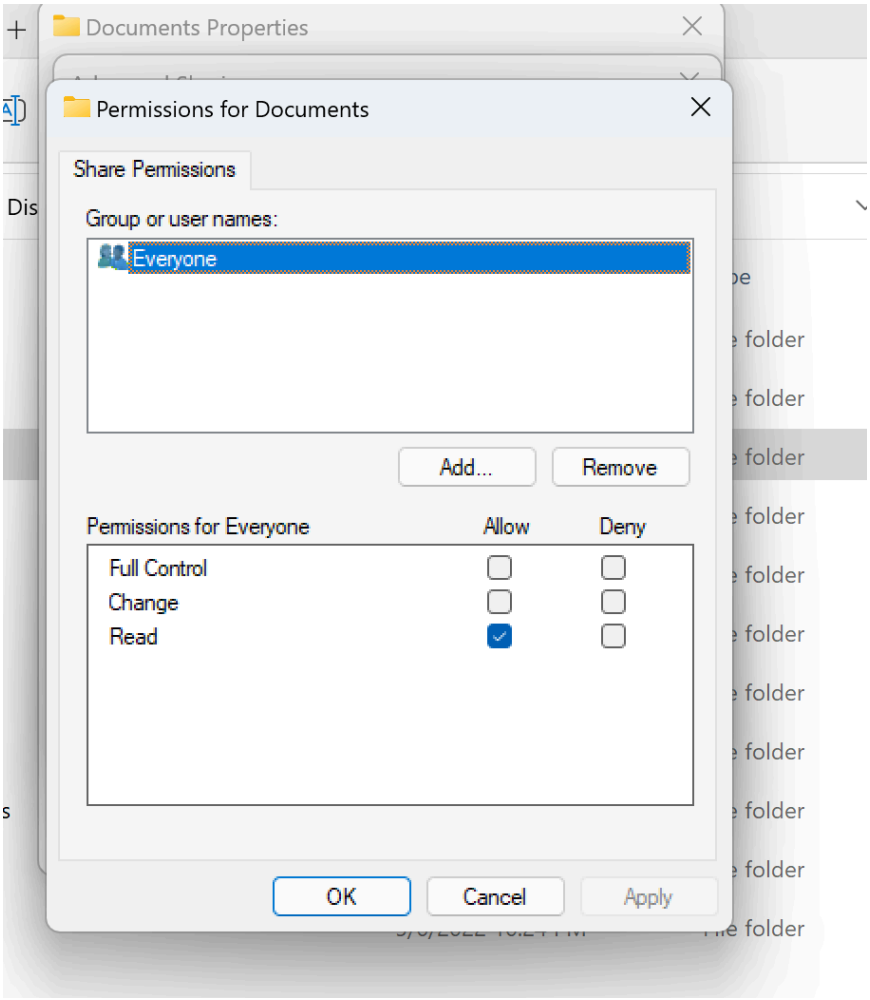
Utilisation d'un volume de style UNIX avec des charges de travail Linux

Les autorisations peuvent être configurées par le sudoer pour les autres utilisateurs. Par exemple, ce qui suit accorderait à tous les membres des read/write autorisations `<group-ID>` complètes sur le `/<project-name>` répertoire :

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

Utilisation d'un volume de style NTFS avec des charges de travail Linux et Windows

Les autorisations de partage peuvent être configurées à l'aide des propriétés de partage d'un dossier spécifique. Par exemple, pour un utilisateur `user_01` et un dossier`myfolder`, vous pouvez définir des autorisations de `Full ControlChange`, ou `Read` pour `Allow` ou `Deny` :



Si le volume doit être utilisé à la fois par des clients Linux et Windows, nous devons configurer un mappage de noms sur la SVM qui associera tout nom d'utilisateur Linux au même nom d'utilisateur au format de nom de domaine NetBIOS de domaine \ nom d'utilisateur. Cela est nécessaire pour traduire entre les utilisateurs de Linux et de Windows. Pour référence, voir Activation des charges de travail multiprotocoles avec Amazon FSx pour NetApp ONTAP.

.....

J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine

Actuellement, lorsque vous créez Amazon FSx pour NetApp ONTAP à partir de la console RES, le système de fichiers est provisionné mais il ne rejoint pas le domaine. Pour associer la SVM du système de fichiers ONTAP créée à votre domaine, consultez Joindre SVMs à un Microsoft Active Directory et suivez les étapes indiquées sur la console Amazon FSx . Assurez-vous que les autorisations requises sont déléguées au compte Amazon FSx Service dans AD. Une fois que la

SVM a rejoint le domaine avec succès, allez dans Résumé de la SVM > Points de terminaison > Nom DNS SMB et copiez le nom DNS car vous en aurez besoin ultérieurement.

Une fois qu'elle est jointe au domaine, modifiez la clé de configuration DNS SMB dans le tableau DynamoDB des paramètres du cluster :

1. Accédez à la console Amazon DynamoDB.
2. Choisissez Tables, puis choisissez`<stack-name>-cluster-settings`.
3. Sous Explorer les éléments du tableau, développez les filtres et entrez le filtre suivant :
   - Nom de l'attribut - clé
   - État : égal à
   - Valeur - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. Sélectionnez l'article renvoyé, puis Actions, Modifier l'article.
5. Mettez à jour la valeur avec le nom DNS SMB que vous avez copié précédemment.
6. Choisissez Enregistrer et fermer.

En outre, assurez-vous que le groupe de sécurité associé au système de fichiers autorise le trafic conformément aux recommandations de la section Contrôle d'accès au système de fichiers avec Amazon VPC. Les nouveaux hôtes VDI utilisant le système de fichiers pourront désormais monter la SVM et le système de fichiers joints au domaine.

Vous pouvez également intégrer un système de fichiers existant déjà joint à votre domaine à l'aide de la fonctionnalité RES Onboard File System. Dans Gestion de l'environnement, choisissez Systèmes de fichiers, Système de fichiers intégré.

.....

Instantanés

Rubriques

- Un instantané a le statut Echoué
- Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.

.....

Un instantané a le statut Echoué

Sur la page RES Snapshots, si un instantané a le statut Echec, vous pouvez en déterminer la cause en accédant au groupe de CloudWatch journaux Amazon du gestionnaire de clusters au moment où l'erreur s'est produite.

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
  asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
  creating the snapshot: An error occurred (TableNotFoundException)
  when calling the UpdateContinuousBackups operation:
  Table not found: res-demo.accounts.sequence-config
```

.....

Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.

Si un instantané pris à partir d'un environnement précédent ne s'applique pas dans un nouvel environnement, consultez les CloudWatch journaux du gestionnaire de clusters pour identifier le problème. Si le problème indique que les tables requises ne peuvent pas être importées, vérifiez que l'instantané est dans un état valide.

1. Téléchargez le fichier metadata.json et vérifiez que le ExportStatus statut des différentes tables est COMPLETED. Assurez-vous que le `ExportManifest` champ est défini dans les différentes tables. Si les champs ci-dessus ne sont pas définis, l'état de l'instantané n'est pas valide et ne peut pas être utilisé avec la fonctionnalité d'application d'un instantané.
2. Après avoir lancé la création d'un instantané, assurez-vous que le statut de l'instantané passe à COMPLETED dans RES. Le processus de création d'un instantané prend de 5 à 10 minutes. Rechargez ou revisitez la page de gestion des instantanés pour vous assurer que le cliché a été créé avec succès. Cela garantira que l'instantané créé est dans un état valide.

.....

Infrastructures

Rubriques

- Groupes cibles d'équilibreur de charge dépourvus d'instances saines

.....

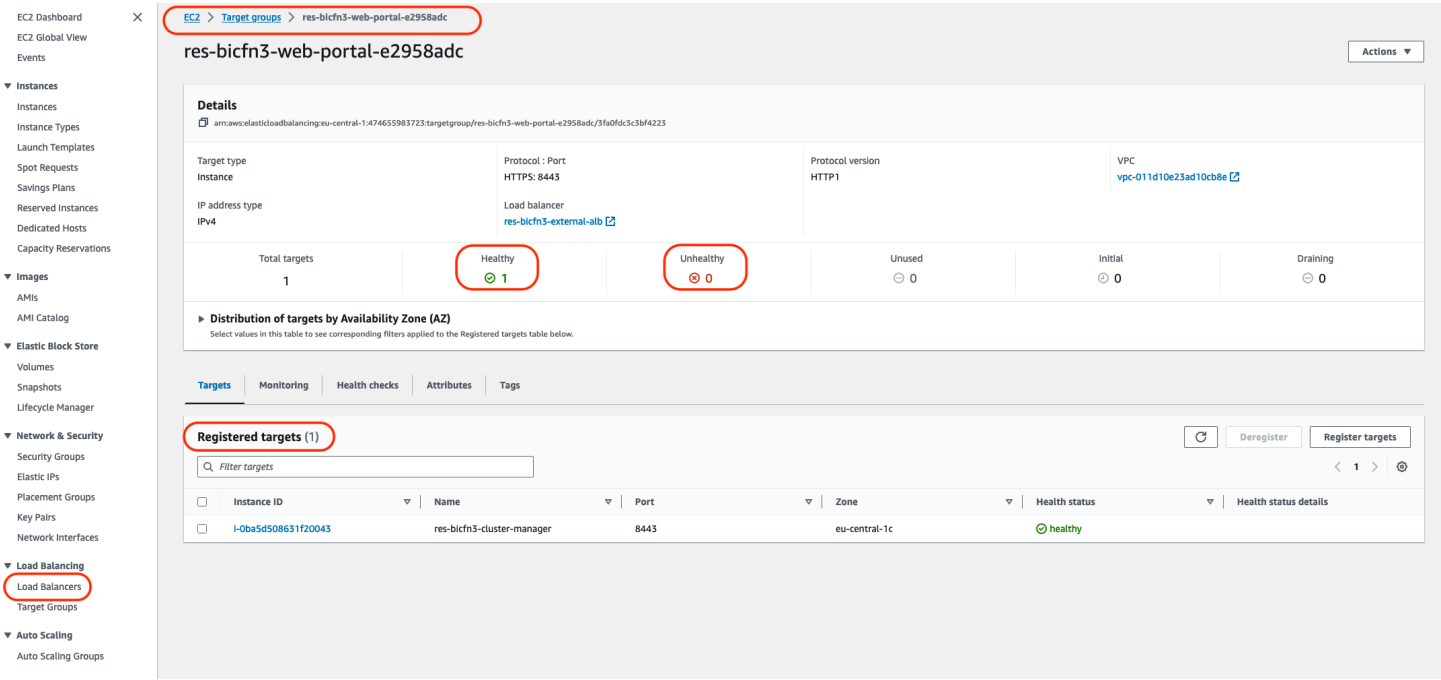
Groupes cibles d'équilibreur de charge dépourvus d'instances saines

Si des problèmes tels que des messages d'erreur du serveur apparaissent dans l'interface utilisateur ou si les sessions de bureau ne peuvent pas se connecter, cela peut indiquer un problème dans l'infrastructure des instances Amazon EC2.

Les méthodes permettant de déterminer la source du problème consistent à vérifier d'abord la console Amazon EC2 pour détecter toute instance Amazon EC2 qui semble se terminer à plusieurs reprises et être remplacée par de nouvelles instances. Si tel est le cas, la vérification des CloudWatch journaux Amazon peut en déterminer la cause.

Une autre méthode consiste à vérifier les équilibreurs de charge du système. Le fait que les équilibreurs de charge trouvés sur la console Amazon EC2 n'affichent aucune instance saine enregistrée indique qu'il peut y avoir des problèmes système.

Voici un exemple d'apparence normale :



Si l'entrée Healthy est 0, cela indique qu'aucune instance Amazon EC2 n'est disponible pour traiter les demandes.

Si l'entrée Unhealthy n'est pas égale à 0, cela indique qu'une instance Amazon EC2 est peut-être en cours de cycle. Cela peut être dû au fait que le logiciel d'application installé ne passe pas les tests de santé.

Si les entrées saines et malsaines sont toutes deux égales à 0, cela indique une erreur de configuration potentielle du réseau. Par exemple, les sous-réseaux public et privé peuvent ne pas avoir de correspondance AZs. Dans ce cas, un texte supplémentaire peut apparaître sur la console indiquant que l'état du réseau existe.

.....

Lancement de bureaux virtuels

Rubriques

.....

Le compte de connexion pour Windows Virtual Desktop est défini sur Administrateur

Si vous parvenez à lancer un bureau virtuel Windows sur le portail Web RES mais que son compte de connexion est défini sur Administrateur lorsque vous vous connectez, votre Windows VDI n'a peut-être pas rejoint Active Directory avec succès.

Pour vérifier, connectez-vous à l'instance Windows depuis la console Amazon EC2 et consultez les journaux de démarrage ci-dessous. `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\` Un message d'erreur commençant par `[Join AD] authorization failed:` indique que l'instance n'a pas réussi à rejoindre l'AD. Vérifiez que le gestionnaire de clusters se connecte CloudWatch sous le nom du groupe de journaux *`<res-environment-name>`*`/cluster-manager` pour plus de détails sur l'échec :

- `Insufficient permissions to modify computer account`
  - Cette erreur indique que votre compte de service ne dispose pas des autorisations appropriées pour ajouter des ordinateurs à l'AD. Consultez la Configuration d'un compte de service pour

Microsoft Active Directory section pour connaître les autorisations requises par le compte de service.

- `Invalid Credentials`
  - Les informations d'identification de votre compte de service dans AD ont expiré ou vous avez fourni des informations d'identification incorrectes. Pour vérifier ou mettre à jour les informations d'identification de votre compte de service, accédez au secret qui stocke le mot de passe dans la console Secrets Manager. Assurez-vous que l'ARN de ce secret est correct dans le champ ARN secret des informations d'identification du compte de service sous Domaine Active Directory sur la page de gestion des identités de votre environnement RES.

.....

Le certificat expire lors de l'utilisation d'une ressource externe CertificateRenewalNode

Si vous avez déployé la recette des ressources externes et que vous rencontrez une erreur indiquant `"The connection has been closed. Transport error"` que vous vous connectez à Linux VDIs, la cause la plus probable est un certificat expiré qui n'est pas automatiquement actualisé en raison d'un chemin d'installation de pip incorrect sous Linux. Les certificats expirent au bout de 3 mois.

Le groupe de CloudWatch log Amazon *<envname>*`/vdc/dcv-connection-gateway` peut enregistrer l'erreur de tentative de connexion avec des messages similaires aux suivants :

```
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Error in connection task: TLS handshake error:
 received fatal alert: CertificateUnknown | redacted:/res-demo/vdc/dcv-connection-
gateway | dcv-connection-gateway_10.3.146.195 |
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Certificate error: AlertReceived(CertificateUnknown)
 | redacted:/res-demo/vdc/dcv-connection-gateway | dcv-connection-gateway_10.3.146.195
 |
```

Pour résoudre le problème :

1. Dans votre AWS compte, accédez à EC2. Si une instance est nommée`*-CertificateRenewalNode-*`, mettez-la hors service.

2. Accédez à Lambda. Vous devriez voir une fonction Lambda nommée`*-CertificateRenewalLambda-*`. Vérifiez que le code Lambda contient quelque chose de similaire à ce qui suit :

```
export HOME=/tmp/home
mkdir -p $HOME

cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
python3 ./get-pip.py
pip3 install boto3
eval $(python3 -c "from botocore.credentials import
 InstanceMetadataProvider, InstanceMetadataFetcher; provider =
 InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
 num_attempts=2)); c = provider.load().get_frozen_credentials();
 print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
 AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
 AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
git clone https://github.com/Neilpang/acme.sh.git
cd acme.sh
```

3. Trouvez le dernier modèle de pile de certificats de ressources externes ici. Trouvez le code Lambda dans le modèle : Ressources → Propriétés CertificateRenewalLambda→ Code. Vous trouverez peut-être quelque chose de similaire à ce qui suit :

```
sudo yum install -y wget
export HOME=/tmp/home
mkdir -p $HOME
cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
mkdir -p pip
python3 ./get-pip.py --target $PWD/pip
$PWD/pip/bin/pip3 install boto3
eval $(python3 -c "from botocore.credentials import
 InstanceMetadataProvider, InstanceMetadataFetcher; provider =
 InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
 num_attempts=2)); c = provider.load().get_frozen_credentials();
 print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
```

```
 AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
 AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
VERSION=3.1.0
wget https://github.com/acmesh-official/acme.sh/archive/refs/tags/$VERSION.tar.gz -
O acme-$VERSION.tar.gz
tar -xvf acme-$VERSION.tar.gz
cd acme.sh-$VERSION
```

4. Remplacez la section de l'étape 2 de la fonction `*-CertificateRenewalLambda-*` Lambda par le code de l'étape 3. Sélectionnez Déployer et attendez que le changement de code prenne effet.
5. Pour déclencher manuellement la fonction Lambda, accédez à l'onglet Test, puis sélectionnez Test. Aucune saisie supplémentaire n'est requise. Cela devrait créer une instance de certificat EC2 qui met à jour le certificat et PrivateKey les secrets dans Secret Manager.
6. Mettez fin à l'instance dcv-gateway existante : `<env-name>-vdc-gateway` et attendez que le groupe auto scaling en déploie automatiquement une nouvelle.

.....

Un bureau virtuel qui fonctionnait auparavant n'est plus en mesure de se connecter correctement

Si une connexion de bureau se ferme ou si vous ne pouvez plus vous y connecter, le problème peut être dû à la défaillance de l'instance Amazon EC2 sous-jacente ou à la résiliation ou à l'arrêt de l'instance Amazon EC2 en dehors de l'environnement RES. L'état de l'interface utilisateur d'administration peut continuer à indiquer qu'il est prêt, mais les tentatives de connexion échouent.

La console Amazon EC2 doit être utilisée pour déterminer si l'instance a été résiliée ou arrêtée. En cas d'arrêt, essayez de le redémarrer. Si l'état est résilié, un autre bureau devra être créé. Toutes les données stockées dans le répertoire personnel de l'utilisateur doivent toujours être disponibles au démarrage de la nouvelle instance.

Si l'instance qui a échoué précédemment apparaît toujours dans l'interface utilisateur d'administration, il peut être nécessaire de la fermer à l'aide de l'interface utilisateur d'administration.

.....

Je ne peux lancer que 5 bureaux virtuels

La limite par défaut du nombre de bureaux virtuels qu'un utilisateur peut lancer est de 5. Cela peut être modifié par un administrateur à l'aide de l'interface utilisateur d'administration comme suit :

- Accédez aux paramètres du bureau.
- Sélectionnez l'onglet Général.
- Sélectionnez l'icône d'édition située à droite des sessions autorisées par défaut par utilisateur et par projet et remplacez la valeur par la nouvelle valeur souhaitée.
- Sélectionnez Soumettre.
- Actualisez la page pour confirmer que le nouveau paramètre est en place.

.....

Les tentatives de connexion Windows pour ordinateur de bureau échouent avec le message « La connexion a été fermée ». Erreur de transport »

Si une connexion de bureau Windows échoue avec le message d'erreur « La connexion a été fermée » s'affiche dans l'interface utilisateur. « Erreur de transport », la cause peut être due à un problème dans le logiciel du serveur DCV lié à la création de certificats sur l'instance Windows.

Le groupe de CloudWatch log Amazon `<envname>/vdc/dcv-connection-gateway` peut enregistrer l'erreur de tentative de connexion avec des messages similaires aux suivants :

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]

Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
```

```
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

Dans ce cas, une solution peut être d'utiliser le gestionnaire de session SSM pour ouvrir une connexion à l'instance Windows et supprimer les 2 fichiers relatifs aux certificats suivants :

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

Les fichiers doivent être automatiquement recréés et une tentative de connexion ultérieure peut être couronnée de succès.

Si cette méthode résout le problème et si les nouveaux lancements de postes de travail Windows produisent la même erreur, utilisez la fonction Create Software Stack pour créer une nouvelle pile logicielle Windows de l'instance fixe avec les fichiers de certificat régénérés. Cela peut produire une pile logicielle Windows qui peut être utilisée pour des lancements et des connexions réussis.

.....

VDIs bloqué dans l'état de provisionnement

Si le lancement d'un poste de travail reste en état de provisionnement dans l'interface utilisateur d'administration, cela peut être dû à plusieurs raisons.

Pour en déterminer la cause, examinez les fichiers journaux de l'instance de bureau et recherchez les erreurs susceptibles d'être à l'origine du problème. Ce document contient une liste de fichiers journaux et de groupes de CloudWatch journaux Amazon contenant des informations pertinentes dans la section intitulée Sources d'informations utiles sur les journaux et les événements.

Les causes potentielles de ce problème sont les suivantes.

- L'identifiant AMI utilisé a été enregistré en tant que pile logicielle mais n'est pas pris en charge par RES.

Le script de provisionnement bootstrap n'a pas pu se terminer car l'Amazon Machine Image (AMI) ne dispose pas de la configuration attendue ou de l'outillage requis. Les fichiers journaux de l'instance, par exemple `/root/bootstrap/logs/` sur une instance Linux, peuvent contenir des informations utiles à ce sujet. AMIs les identifiants extraits du AWS Marketplace peuvent ne pas fonctionner pour les instances de bureau RES. Ils doivent être testés pour confirmer s'ils sont pris en charge.

- Les scripts de données utilisateur ne sont pas exécutés lorsque l'instance de bureau virtuel Windows est lancée à partir d'une AMI personnalisée.

  Par défaut, les scripts de données utilisateur s'exécutent une seule fois lors du lancement d'une instance Amazon EC2. Si vous créez une AMI à partir d'une instance de bureau virtuel existante, puis que vous enregistrez une pile logicielle auprès de l'AMI et que vous essayez de lancer un autre bureau virtuel avec cette pile logicielle, les scripts de données utilisateur ne s'exécuteront pas sur la nouvelle instance de bureau virtuel.

  Pour résoudre le problème, ouvrez une fenêtre de PowerShell commande en tant qu'administrateur sur l'instance de bureau virtuel d'origine que vous avez utilisée pour créer l'AMI, puis exécutez la commande suivante :

  ```
  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
  ```

  Créez ensuite une nouvelle AMI à partir de l'instance. Vous pouvez utiliser la nouvelle AMI pour enregistrer des piles de logiciels et lancer de nouveaux bureaux virtuels par la suite. Notez que vous pouvez également exécuter la même commande sur l'instance qui reste dans l'état de provisionnement et redémarrer l'instance pour corriger la session de bureau virtuel, mais vous rencontrerez à nouveau le même problème lors du lancement d'un autre bureau virtuel à partir de l'AMI mal configurée.

.....

VDIs passer à l'état d'erreur après le lancement

Problème possible 1 : le système de fichiers personnel possède un répertoire pour l'utilisateur avec différentes autorisations POSIX.

C'est peut-être le problème que vous rencontrez si les scénarios suivants sont vrais :

1. La version RES déployée est 2024.01 ou supérieure.

2. Lors du déploiement de la pile RES, l'attribut for `EnableLdapIDMapping` a été défini sur`True`.
3. Le système de fichiers home spécifié lors du déploiement de la pile RES était utilisé dans une version antérieure à RES 2024.01 ou dans un environnement précédent avec `EnableLdapIDMapping` une valeur définie sur. `False`

Étapes de résolution : supprimez les répertoires utilisateur du système de fichiers.

1. SSM vers l'hôte du gestionnaire de clusters.
2. `cd /home`.
3. `ls`- doit répertorier les répertoires dont les noms de répertoire correspondent aux noms d'utilisateur, tels que`admin1`,`admin2`.. et ainsi de suite.
4. Supprimez les répertoires,`sudo rm -r 'dir_name'`. Ne supprimez pas les répertoires ssm-user et ec2-user.
5. Si les utilisateurs sont déjà synchronisés avec le nouvel environnement, supprimez ceux de l'utilisateur de la table DDB de l'utilisateur (sauf clusteradmin).
6. Lancez la synchronisation AD : `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` exécutez-la dans le gestionnaire de clusters Amazon EC2.
7. Redémarrez l'instance VDI dans l'`Error`état indiqué sur la page Web RES. Vérifiez que le VDI passe à l'`Ready`état en 20 minutes environ.

.....

Composant de bureau virtuel

Rubriques

- L'instance Amazon EC2 s'affiche à plusieurs reprises comme terminée dans la console
- L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API
- Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter
- Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init < > le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » (où le compte est un nom d'utilisateur)

- Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »
- Problèmes liés aux options DHCP avec la configuration external/customer AD
- Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

.....

L'instance Amazon EC2 s'affiche à plusieurs reprises comme terminée dans la console

Si une instance d'infrastructure apparaît à plusieurs reprises comme étant terminée dans la console Amazon EC2, la cause peut être liée à sa configuration et dépendre du type d'instance d'infrastructure. Les méthodes suivantes permettent d'en déterminer la cause.

Si l'instance vdc-controller affiche des états de terminaison répétés dans la console Amazon EC2, cela peut être dû à une balise secrète incorrecte. Les secrets conservés par RES comportent des balises utilisées dans le cadre des politiques de contrôle d'accès IAM associées aux instances Amazon EC2 de l'infrastructure. Si le contrôleur vdc fonctionne en cycle et que l'erreur suivante apparaît dans le groupe de CloudWatch journaux, cela peut être dû au fait qu'un secret n'a pas été correctement étiqueté. Notez que le secret doit être marqué comme suit :

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

Le message du CloudWatch journal Amazon correspondant à cette erreur s'affichera comme suit :

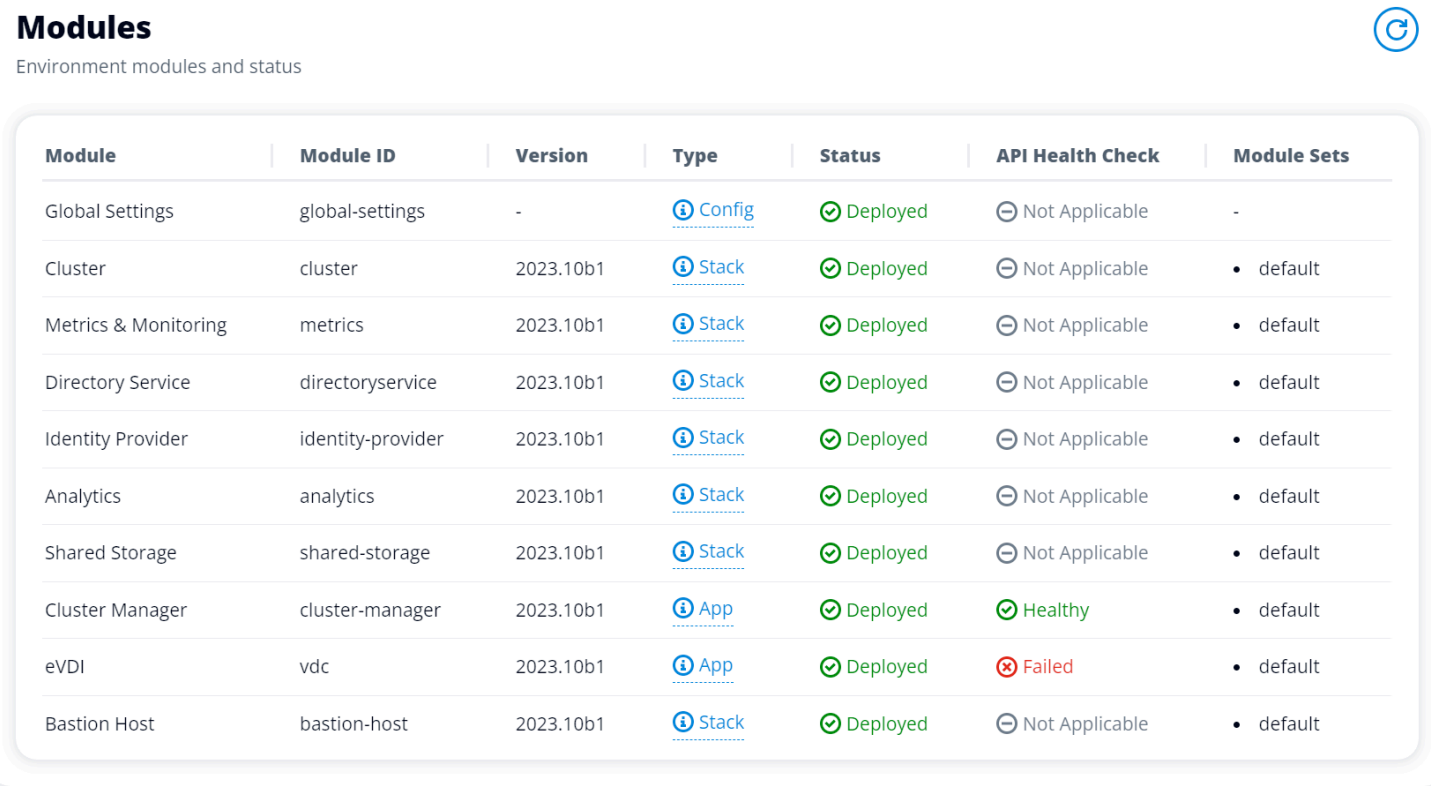
```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Vérifiez les balises de l'instance Amazon EC2 et vérifiez qu'elles correspondent à la liste ci-dessus.

.....

L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API

Si le module eVDI échoue lors de son contrôle de santé, il affichera ce qui suit dans la section État de l'environnement.



Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

Dans ce cas, le chemin général pour le débogage consiste à consulter les journaux du gestionnaire de clusters CloudWatch. (Recherchez le groupe de journaux nommé`<env-name>/cluster-manager`.)

Problèmes possibles :

- Si les journaux contiennent le texte`Insufficient permissions`, assurez-vous que le ServiceAccount nom d'utilisateur indiqué lors de la création de la pile res est correctement orthographié.

  Exemple de ligne de journal :

```
Insufficient permissions to modify computer account:
 CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
 000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
```

```
(CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
request will be retried in 30 seconds
```

- Vous pouvez accéder au ServiceAccount nom d'utilisateur fourni lors du déploiement de RES depuis la SecretsManager console. Trouvez le secret correspondant dans le gestionnaire de secrets et choisissez Retrieve Plain text. Si le nom d'utilisateur est incorrect, choisissez Modifier pour mettre à jour la valeur secrète. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances apparaîtront dans un état stable.
- Le nom d'utilisateur doit être ServiceAccount « » si vous utilisez les ressources créées par la pile de ressources externes fournie. Si le `DisableADJoin` paramètre a été défini sur False lors de votre déploiement de RES, assurez-vous que l'utilisateur ServiceAccount « » est autorisé à créer des objets informatiques dans l'AD.

- Si le nom d'utilisateur utilisé est correct, mais que les journaux contiennent le texte`Invalid credentials`, le mot de passe que vous avez saisi est peut-être erroné ou a expiré.

  Exemple de ligne de journal :

```
{'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
 'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
 data 532, v4563'}
```

  - Vous pouvez lire le mot de passe que vous avez saisi lors de la création de l'environnement en accédant au secret qui stocke le mot de passe dans la console Secrets Manager. Sélectionnez le secret (par exemple`<env_name>directoryserviceServiceAccountPassword`) et choisissez Récupérer du texte brut.
  - Si le mot de passe indiqué dans le secret est incorrect, choisissez Modifier pour mettre à jour sa valeur dans le secret. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances utiliseront le mot de passe mis à jour et apparaîtront dans un état stable.
  - Si le mot de passe est correct, il se peut qu'il ait expiré dans l'Active Directory connecté. Vous devez d'abord réinitialiser le mot de passe dans Active Directory, puis mettre à jour le secret. Vous pouvez réinitialiser le mot de passe de l'utilisateur dans Active Directory à partir de la console Directory Service :

    1. Choisissez l'ID de répertoire approprié
    2. Choisissez Actions, Réinitialiser le mot de passe utilisateur, puis remplissez le formulaire avec le nom d'utilisateur (par exemple, ServiceAccount « ») et le nouveau mot de passe.

3. Si le nouveau mot de passe est différent du mot de passe précédent, mettez-le à jour dans le secret Secret Manager correspondant (par exemple,`<env_name>directoryserviceServiceAccountPassword`.
4. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances apparaîtront dans un état stable.

.....

Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter

Ce problème peut être lié au problème suivant associé à la synchronisation du compte utilisateur avec AD. Si ce problème apparaît, vérifiez la présence de l'erreur `<user-home-init> account not available yet. waiting for user to be synced` « » dans le groupe de journaux CloudWatch Amazon du gestionnaire de clusters afin de déterminer si la cause est identique ou liée.

.....

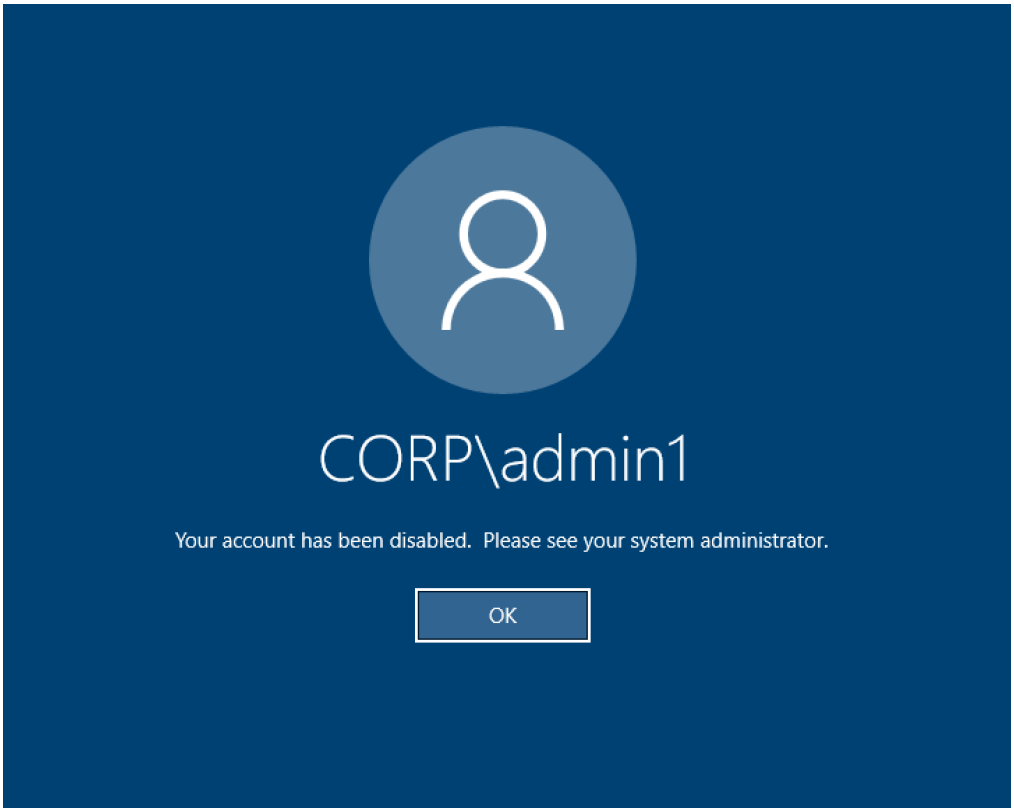
Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init **< >** le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » (où le compte est un nom d'utilisateur)

L'abonné SQS est occupé et bloqué dans une boucle infinie car il ne peut pas accéder au compte utilisateur. Ce code est déclenché lorsque vous essayez de créer un système de fichiers personnel pour un utilisateur lors de la synchronisation utilisateur.

La raison pour laquelle il ne parvient pas à accéder au compte utilisateur peut être que RES n'a pas été configuré correctement pour l'AD utilisé. Par exemple, le `ServiceAccountCredentialsSecretArn` paramètre utilisé lors de la création de BI/RES l'environnement n'était pas la bonne valeur.

.....

Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »



Si l'utilisateur ne parvient pas à se reconnecter à un écran verrouillé, cela peut indiquer qu'il a été désactivé dans l'AD configuré pour RES après s'être connecté avec succès via SSO.

La connexion SSO devrait échouer si le compte utilisateur a été désactivé dans AD.

.....

Problèmes liés aux options DHCP avec la configuration external/customer AD

Si vous rencontrez un message d'erreur indiquant que `"The connection has been closed. Transport error"` vous utilisez les bureaux virtuels Windows lorsque vous utilisez RES avec votre propre Active Directory, consultez le CloudWatch journal dcv-connection-gateway Amazon pour trouver un résultat similaire à ce qui suit :

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }
```

```
Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Si vous utilisez un contrôleur de domaine AD pour vos options DHCP pour votre propre VPC, vous devez :

1. Ajoutez le AmazonProvided DNS aux deux contrôleurs de domaine IPs.
2. Définissez le nom de domaine sur ec2.internal.

Un exemple est présenté ici. Sans cette configuration, le bureau Windows vous donnera une erreur de transport, car il RES/DCV recherche le nom d'hôte ip-10-0-x-xx.ec2.internal.

.....

Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Lorsque vous utilisez le navigateur Web Firefox, le message d'erreur de type MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING peut s'afficher lorsque vous essayez de vous connecter à un bureau virtuel.

Cela est dû au fait que le serveur Web RES est configuré avec TLS + Stapling On mais ne répond pas à la validation par agrafage (voir https://support.mozilla). org/en-US/questions/1372483.

Vous pouvez résoudre ce problème en suivant les instructions disponibles sur : https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing.

.....

Suppression d'environnements

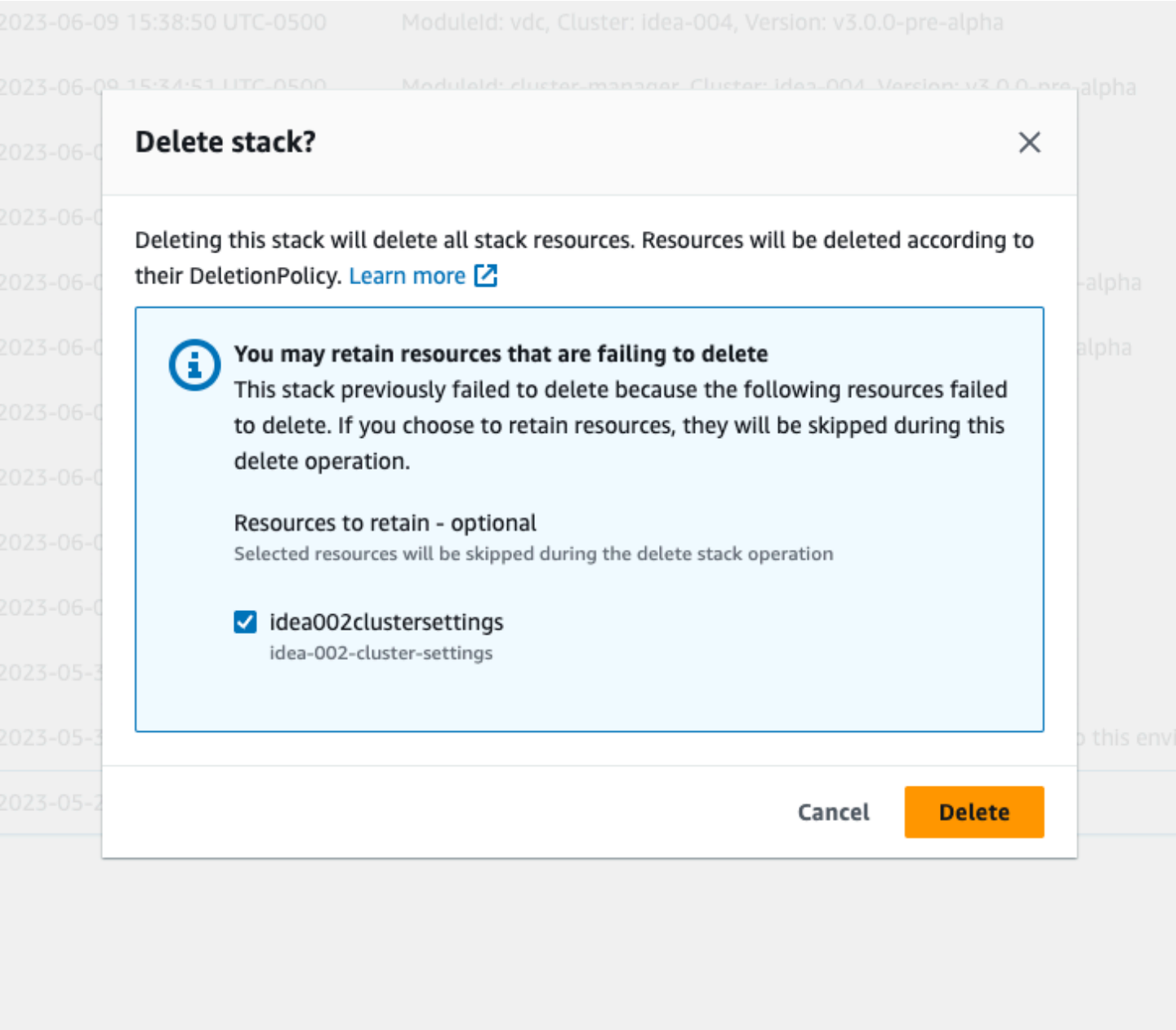
Rubriques

.....

res-xxx-cluster pile dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement en raison de l'erreur « Le rôle n'est pas valide ou ne peut pas être assumé »

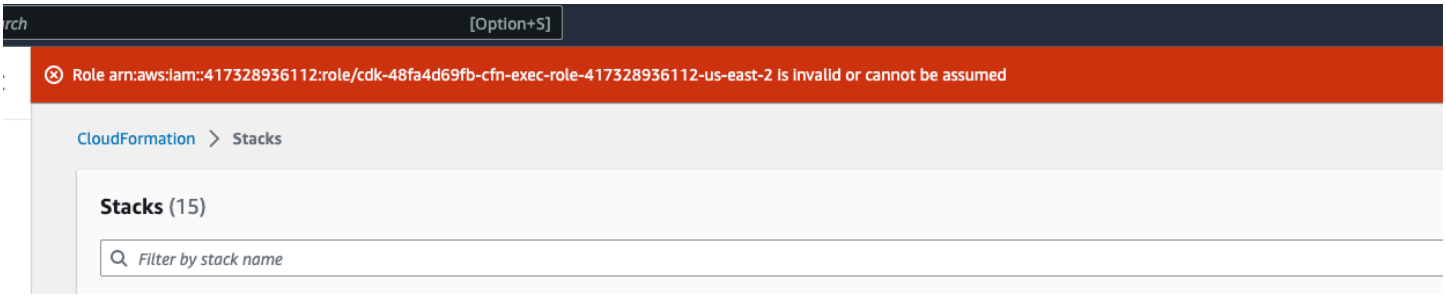
Si vous remarquez que la pile « res-xxx-cluster » est dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement, vous pouvez effectuer les étapes suivantes pour la supprimer.

Si vous voyez la pile dans un état « DELETE_FAILED », essayez d'abord de la supprimer manuellement. Une boîte de dialogue confirmant Delete Stack peut s'afficher. Sélectionnez Delete (Supprimer).



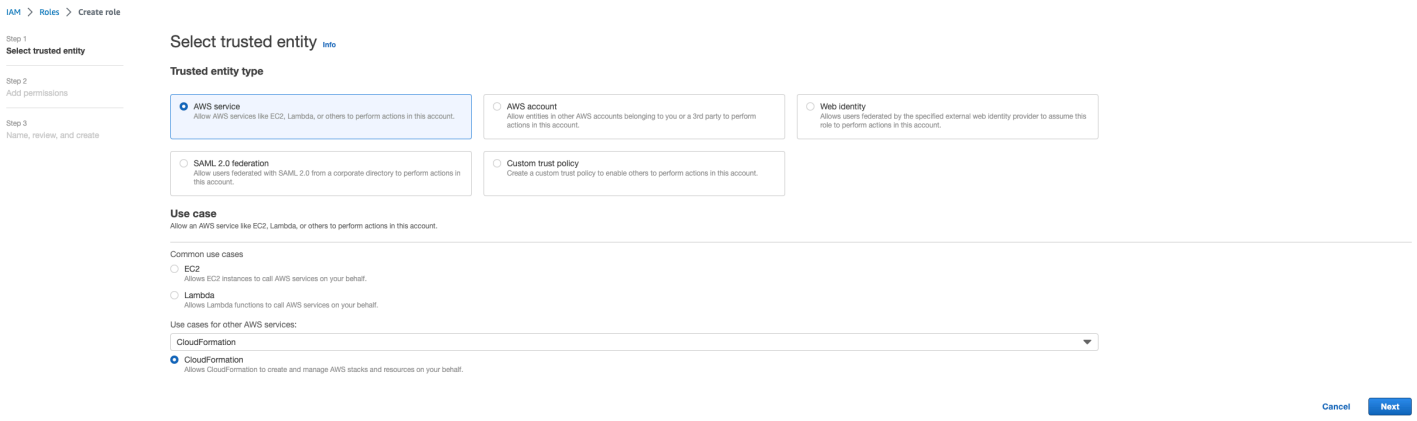
Parfois, même si vous supprimez toutes les ressources de pile requises, vous pouvez toujours voir le message vous demandant de sélectionner les ressources à conserver. Dans ce cas, sélectionnez toutes les ressources comme « ressources à conserver » et choisissez Supprimer.

Vous pouvez voir un message d'erreur qui ressemble à `Role: arn:aws:iam::... is Invalid or cannot be assumed`

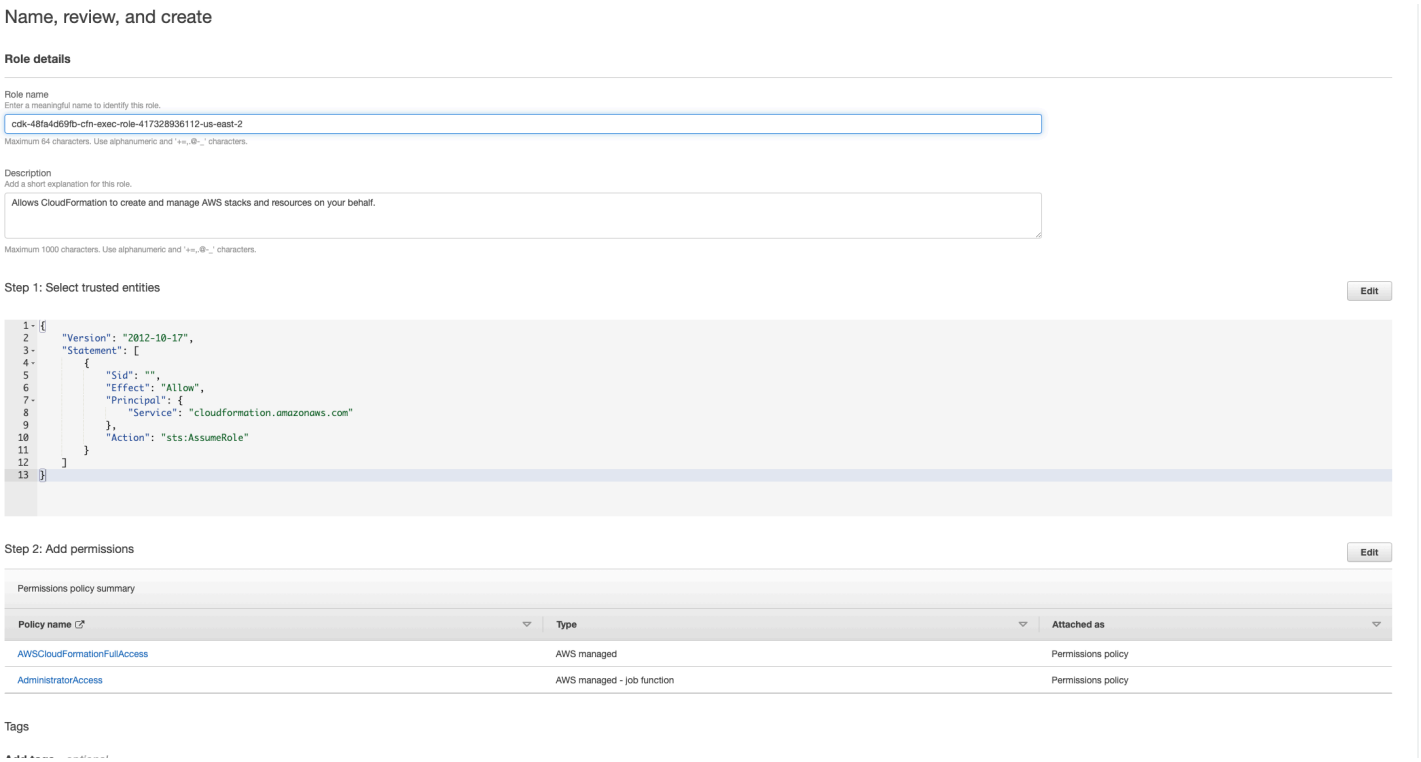


Cela signifie que le rôle requis pour supprimer la pile a d'abord été supprimé avant la pile. Pour contourner ce problème, copiez le nom du rôle. Accédez à la console IAM et créez un rôle portant ce nom à l'aide des paramètres indiqués ici, à savoir :

- Pour Type d'entité de confiance, sélectionnez AWS service.
- Pour Cas d'utilisation, sous `Use cases for other AWS services` Choisir`CloudFormation`.



Choisissez Suivant. Assurez-vous d'accorder les autorisations aux rôles `AWSCloudFormationFullAccess` « » et `AdministratorAccess` « ». Votre page d'évaluation doit ressembler à ceci :



Retournez ensuite sur la CloudFormation console et supprimez la pile. Vous devriez maintenant être en mesure de le supprimer depuis que vous avez créé le rôle. Enfin, accédez à la console IAM et supprimez le rôle que vous avez créé.

.....

Collecte de journaux

Connexion à une instance EC2 depuis la console EC2

- Suivez ces instructions pour vous connecter à votre instance Linux EC2.
- Suivez ces instructions pour vous connecter à votre instance Windows EC2. Ouvrez ensuite Windows PowerShell pour exécuter n'importe quelle commande.

Collecte des journaux des hôtes de l'infrastructure

1. Cluster-manager : récupérez les journaux du gestionnaire de cluster aux emplacements suivants et joignez-les au ticket.
   a. Tous les journaux du groupe de CloudWatch journaux`<env-name>/cluster-manager`.
   b. Tous les journaux situés dans le `/root/bootstrap/logs` répertoire de l'instance `<env-name>-cluster-manager` EC2. Suivez les instructions liées à la section « Connexion à une

instance EC2 depuis la console EC2 » au début de cette section pour vous connecter à votre instance.

2. Contrôleur VDC : récupérez les journaux du contrôleur VDC aux emplacements suivants et joignez-les au ticket.
   a. Tous les journaux du groupe de CloudWatch journaux`<env-name>/vdc-controller`.
   b. Tous les journaux situés dans le `/root/bootstrap/logs` répertoire de l'instance `<env-name>-vdc-controller` EC2. Suivez les instructions liées à la section « Connexion à une instance EC2 depuis la console EC2 » au début de cette section pour vous connecter à votre instance.

L'un des moyens d'obtenir facilement les journaux est de suivre les instructions de la Téléchargement de journaux depuis des instances Linux EC2 section. Le nom du module serait le nom de l'instance.

Collecte des journaux VDI

Identifiez l'instance Amazon EC2 correspondante

Si un utilisateur lançait un VDI avec un nom de session`VDI1`, le nom correspondant de l'instance sur la console Amazon EC2 serait. `<env-name>-VDI1-<user name>`

Collectez les journaux VDI Linux

Connectez-vous à l'instance Amazon EC2 correspondante depuis la console Amazon EC2 en suivant les instructions liées à la section « Connexion à une instance EC2 depuis la console EC2 » au début de cette section. Accédez à tous les journaux dans les `/var/log/dcv/` répertoires `/root/bootstrap/logs` et de l'instance VDI Amazon EC2.

L'un des moyens d'obtenir les journaux serait de les télécharger sur s3, puis de les télécharger à partir de là. Pour cela, vous pouvez suivre ces étapes pour obtenir tous les journaux dans un répertoire, puis les télécharger :

1. Procédez comme suit pour copier les journaux DCV dans le `/root/bootstrap/logs` répertoire :

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Maintenant, suivez les étapes répertoriées dans la section suivante Téléchargement des journaux VDI pour télécharger les journaux.

Collectez les journaux Windows VDI

Connectez-vous à l'instance Amazon EC2 correspondante depuis la console Amazon EC2 en suivant les instructions liées à la section « Connexion à une instance EC2 depuis la console EC2 » au début de cette section. Obtenez tous les journaux dans le `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` répertoire de l'instance VDI EC2.

L'un des moyens d'obtenir les journaux serait de les télécharger sur S3, puis de les télécharger à partir de là. Pour ce faire, suivez les étapes répertoriées dans la section suivante-Téléchargement des journaux VDI.

.....

Téléchargement des journaux VDI

1. Mettez à jour le rôle IAM de l'instance VDI EC2 pour autoriser l'accès à S3.
2. Accédez à la console EC2 et sélectionnez votre instance VDI.
3. Sélectionnez le rôle IAM qu'il utilise.
4. Dans la section Politiques d'autorisation du menu déroulant Ajouter des autorisations, choisissez Joindre des politiques, puis sélectionnez la politique AmazonS3 FullAccess.
5. Choisissez Ajouter des autorisations pour joindre cette politique.
6. Ensuite, suivez les étapes répertoriées ci-dessous en fonction de votre type de VDI pour télécharger les journaux. Le nom du module serait le nom de l'instance.
   a. Téléchargement de journaux depuis des instances Linux EC2pour Linux.
   b. Téléchargement de journaux à partir d'instances Windows EC2pour Windows.
7. Enfin, modifiez le rôle pour supprimer la `AmazonS3FullAccess` politique.

> **Note**
>
> Tous VDIs utilisent le même rôle IAM qui est `<env-name>-vdc-host-role-<region>`

.....

Téléchargement de journaux depuis des instances Linux EC2

Connectez-vous à l'instance EC2 à partir de laquelle vous souhaitez télécharger les journaux et exécutez les commandes suivantes pour télécharger tous les journaux dans un compartiment s3 :

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

Ensuite, accédez à la console S3, sélectionnez le bucket avec son nom `<environment_name>-cluster-<region>-<aws_account_number>` et téléchargez le `<module_name>_logs.tar.gz` fichier précédemment téléchargé.

.....

Téléchargement de journaux à partir d'instances Windows EC2

Connectez-vous à l'instance EC2 à partir de laquelle vous souhaitez télécharger les journaux et exécutez les commandes suivantes pour télécharger tous les journaux dans un compartiment S3 :

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

Ensuite, accédez à la console S3, sélectionnez le bucket avec son nom `<environment_name>-cluster-<region>-<aws_account_number>` et téléchargez le `<module_name>_logs.zip` fichier précédemment téléchargé.

.....

Collecte des journaux ECS pour l' WaitCondition erreur

1. Accédez à la pile déployée et sélectionnez l'onglet Ressources.
2. Développez Deploy ResearchAndEngineeringStudio→ → Installer → Tâches CreateTaskDef→ CreateContainer→ → LogGroup, puis sélectionnez le groupe de journaux pour ouvrir CloudWatch les journaux.
3. Récupérez le dernier journal de ce groupe de journaux.

.....

Environnement de démonstration

Rubriques

- Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité
- Demo Stack Keycloak ne fonctionne pas

.....

Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité

Problème

Si vous essayez de vous connecter et que vous recevez une « erreur inattendue lors du traitement de la demande d'authentification auprès du fournisseur d'identité », vos mots de passe ont peut-être expiré. Il peut s'agir du mot de passe de l'utilisateur sous lequel vous essayez de vous connecter ou de votre compte Active Directory Service.

Mitigation

1. Réinitialisez les mots de passe de l'utilisateur et du compte de service dans la console du service d'annuaire.
2. Mettez à jour les mots de passe des comptes de service dans Secrets Manager pour qu'ils correspondent au nouveau mot de passe que vous avez saisi ci-dessus :
   - pour la pile Keycloak : -... PasswordSecret - RESExternal-... - DirectoryService-... avec description : mot de passe pour Microsoft Active Directory
   - pour RES : res- ServiceAccountPassword -... avec description : mot de passe du compte Active Directory Service
3. Accédez à la console EC2 et mettez fin à l'instance du gestionnaire de clusters. Les règles Auto Scaling déclencheront automatiquement le déploiement d'une nouvelle instance.

.....

Demo Stack Keycloak ne fonctionne pas

Problème

Si votre serveur Keycloak est tombé en panne et que, lorsque vous l'avez redémarré, l'adresse IP de l'instance a changé, cela a peut-être entraîné une rupture de keycloak : la page de connexion de votre portail RES ne se charge pas ou reste bloquée dans un état de chargement qui ne se résout jamais.

Mitigation

Vous devrez supprimer l'infrastructure existante et redéployer la pile Keycloak pour rétablir le bon état de Keycloak. Procédez comme suit :

1. Accédez à Cloudformation. Vous devriez y voir deux piles liées à Keycloak :
   - `<env-name>-RESSsoKeycloak-<random characters>`(Pile 1)

     `<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-*`(Pile 2)
2. Supprimez Stack1. Si vous êtes invité à supprimer la pile imbriquée, sélectionnez Oui pour supprimer la pile imbriquée.

   Assurez-vous que la pile a été complètement supprimée.
3. Téléchargez le modèle de stack RES SSO Keycloak ici.

4. Déployez cette pile manuellement avec exactement les mêmes valeurs de paramètres que la pile supprimée. Déployez-le depuis la CloudFormation console en accédant à Create Stack → Avec de nouvelles ressources (standard) → Choisir un modèle existant → Télécharger un fichier modèle. Renseignez les paramètres requis en utilisant les mêmes entrées que la pile supprimée. Vous pouvez trouver ces entrées dans votre pile supprimée en modifiant le filtre sur la CloudFormation console et en accédant à l'onglet Paramètres. Assurez-vous que le nom de l'environnement, la paire de clés et les autres paramètres correspondent aux paramètres de la pile d'origine.
5. Une fois la pile déployée, votre environnement est prêt à être réutilisé. Vous pouvez les trouver ApplicationUrl dans l'onglet Sorties de la pile déployée.

.....

Problèmes connus

- Problèmes connus 2024.x
  - (2024.12 et 2024.12.01) Échec de Regex lors de l'enregistrement d'un nouvel utilisateur de Cognito
  - (2024.12.01 et versions antérieures) Erreur de mauvais certificat non valide lors de la connexion au VDI à l'aide d'un domaine personnalisé
  - (2024.12 et 2024.12.01) Les utilisateurs d'Active Directory ne peuvent pas se connecter par SSH à Bastion Host
  - (2024.10) L'arrêt automatique du VDI est interrompu pour les environnements RES déployés dans des environnements isolés VPCs
  - (2024.10 et versions antérieures) Impossible de lancer VDI pour les types d'instances Graphic Enhanced
  - (2024.08) Préparation à une défaillance de l'AMI d'infrastructure
  - (2024.08) Les bureaux virtuels ne parviennent pas à monter le compartiment read/write Amazon S3 avec l'ARN du compartiment racine et un préfixe personnalisé
  - (2024.06) L'application d'un instantané échoue lorsque le nom du groupe AD contient des espaces
  - (2024.06 et versions antérieures) Les membres du groupe ne sont pas synchronisés avec RES lors de la synchronisation AD

- (2024.06 et versions antérieures) CVE-2024-6387, Regre, vulnérabilité de sécurité dans et Ubuntu SSHion RHEL9 VDIs
- (2024.04-2024.04.02) La limite d'autorisation IAM fournie n'est pas attachée au rôle des instances VDI
- (2024.04.02 et versions antérieures) Les instances Windows NVIDIA dans ap-southeast-2 (Sydney) ne démarrent pas
- (2024.04 et 2024.04.01) Échec de la suppression RES dans GovCloud
- (2024.04 - 2024.04.02) Le bureau virtuel Linux peut être bloqué à l'état « REPRISE » au redémarrage
- (2024.04.02 et versions antérieures) Impossible de synchroniser les utilisateurs AD dont l'attribut SAMAccount Name inclut des majuscules ou des caractères spéciaux
- (2024.04.02 et versions antérieures) La clé privée pour accéder à l'hôte Bastion n'est pas valide

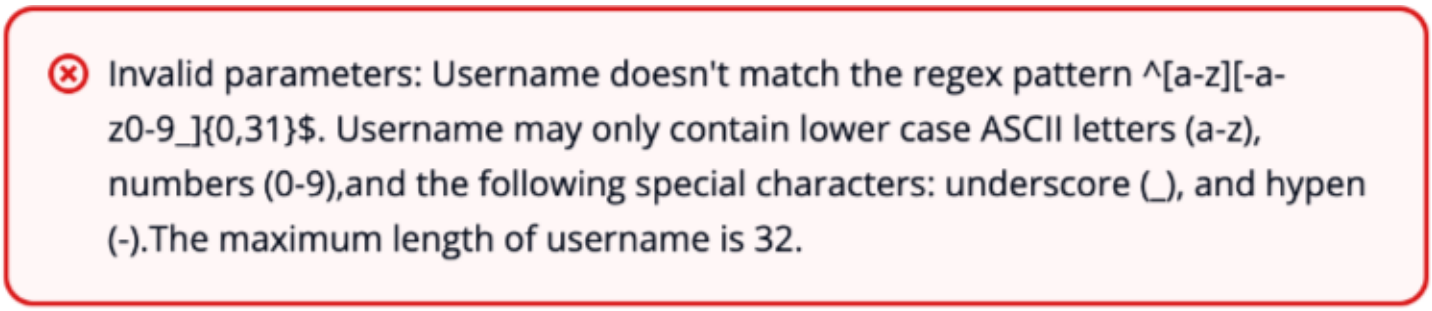
Problèmes connus 2024.x

.....

(2024.12 et 2024.12.01) Échec de Regex lors de l'enregistrement d'un nouvel utilisateur de Cognito

Description du bogue

Si vous tentez d'enregistrer des utilisateurs de AWS Cognito via le portail Web dont le préfixe d'e-mail contient » . «, par exemple`<firstname>.<lastname>@<company>.com`, cela provoquera une erreur indiquant que le nom d'utilisateur de Cognito ne correspond pas au modèle d'expression régulière défini.



Cette erreur est due au fait que RES génère automatiquement des noms d'utilisateur à partir du préfixe de courrier électronique de l'utilisateur. Cependant, les noms d'utilisateur marqués de «. » ne

sont pas des utilisateurs valides pour VDIs certaines distributions Linux prises en charge par RES. Ce correctif supprime tout «. » dans le préfixe d'e-mail lors de la génération d'un nom d'utilisateur afin que le nom d'utilisateur soit valide sous RES Linux. VDIs

Versions concernées

Versions RES 2024.12 et 2024.12.01

Mitigation

1. Exécutez les commandes suivantes pour télécharger `patch.py` et `cognito_sign_up_email_fix.patch` pour la version 2024.12 ou `cognito_sign_up_email_fix.patch` pour la version 2024.12.01, en les `<output-directory>` remplaçant par le répertoire dans lequel vous souhaitez télécharger le script de correctif et le fichier de correctif, et par le nom de votre `<environment-name>` environnement RES :

   a. Le correctif s'applique aux normes RES 2024.12 et 2024.12.01.

   b. Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.

   c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>
RES_VERSION=<res-version> # either 2024.12 or 2024.12.01

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/cognito_sign_up_email_fix.patch --output
 ${OUTPUT_DIRECTORY}/cognito_sign_up_email_fix.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif ont été téléchargés. Exécutez la commande de correctif suivante :

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --
res-version ${RES_VERSION} --module cluster-manager --patch ${OUTPUT_DIRECTORY}/
cognito_sign_up_email_fix.patch
```

3. Redémarrez l'instance de Cluster Manager pour votre environnement. Vous pouvez également mettre fin à l'instance depuis la console de gestion Amazon EC2.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

4. Vérifiez l'état de l'instance de Cluster Manager en vérifiant l'activité du groupe de dimensionnement automatique en commençant par son nom`<RES-EnvironmentName>-cluster-manager-asg`. Attendez que la nouvelle instance soit lancée avec succès.

.....

(2024.12.01 et versions antérieures) Erreur de mauvais certificat non valide lors de la connexion au VDI à l'aide d'un domaine personnalisé

Description du bogue

Lorsque vous déployez la recette External Resources et RES avec un nom de domaine de portail personnalisé, vous CertificateRenewalNode ne parvenez pas à actualiser le certificat TLS pour la connexion VDI avec l'erreur suivante dans : `/var/log/user-data.log`

```
{
  "type": "urn:ietf:params:acme:error:unauthorized",
  "detail": "Error finalizing order :: OCSP must-staple extension is no longer
 available: see https://letsencrypt.org/2024/12/05/ending-ocsp",
  "status": 403
}
```

Par conséquent, vous rencontrerez une erreur indiquant `net::ERR_CERT_DATE_INVALID` (Chrome) ou `Error code: SSL_ERROR_BAD_CERT_DOMAIN` (FireFox) lorsque vous vous connecterez à votre portail Web VDIs dans le RES.

Versions concernées

2024.12.01 et versions antérieures

Mitigation

1. Accédez à la console EC2. Si une instance est nomméeCertificateRenewalNode-, mettez-la hors service.
2. Accédez à la console Lambda. Ouvrez le code source de la fonction Lambda nommée. -CertificateRenewalLambda- Identifiez la ligne commençant par `./acme.sh --issue --dns dns_aws --ocsp-must-staple --keylength 4096` et supprimez l'`--ocsp-must-staple`argument.
3. Sélectionnez Déployer et attendez que le changement de code prenne effet.
4. Pour déclencher manuellement la fonction Lambda : allez dans l'onglet Test, puis sélectionnez Test. Aucune saisie supplémentaire n'est requise. Cela devrait créer une instance de certificat EC2 qui met à jour le certificat et PrivateKey les secrets dans Secret Manager. L'instance sera automatiquement résiliée une fois les secrets mis à jour.
5. Mettez fin à l'instance dcv-gateway existante : `<env-name>-vdc-gateway` et attendez que le groupe auto scaling en déploie automatiquement une nouvelle.

Détails de l'erreur

Let's Encrypt mettra fin au support OCSP en 2025. À compter du 30 janvier 2025, les demandes OCSP Must-Staple échoueront sauf si le compte demandeur a préalablement émis un certificat contenant l'extension OCSP Must Staple. Consultez le site https://letsencrypt.org/2024/12/05/ending-ocsp/ pour plus de détails.

.....

(2024.12 et 2024.12.01) Les utilisateurs d'Active Directory ne peuvent pas se connecter par SSH à Bastion Host

Description du bogue

Les utilisateurs d'Active Directory reçoivent un message d'erreur de refus d'autorisation lorsqu'ils se connectent à l'hôte Bastion en suivant les instructions du portail Web RES.

L'application Python qui s'exécute sur l'hôte Bastion ne parvient pas à lancer le service SSSD en raison d'une variable d'environnement manquante. Par conséquent, les utilisateurs d'AD sont inconnus du système d'exploitation et ne peuvent pas se connecter.

Versions concernées

2024.12 et 2024.12.01

Mitigation

1. Connectez-vous à l'instance Bastion Host depuis la console EC2.
2. Modifiez `/etc/environment` et ajoutez `environment_name=<res-environment-name>` une nouvelle ligne sous IDEA_CLUSTER_NAME.
3. Exécutez les commandes suivantes sur l'instance :

```
source /etc/environment
sudo service supervisord restart
sudo systemctl restart supervisord
```

4. Réessayez de vous connecter à l'hôte Bastion en suivant les instructions du portail Web RES.

.....

(2024.10) L'arrêt automatique du VDI est interrompu pour les environnements RES déployés dans des environnements isolés VPCs

Description du bogue

Avec la version 2024.10 RES, l'arrêt automatique du VDI a été ajouté VDIs pour les personnes inactives pendant un certain temps. Ce paramètre peut être configuré dans Paramètres du bureau → Serveur → Session.

L'arrêt automatique VDI n'est actuellement pas pris en charge pour les environnements RES déployés de manière isolée VPCs.

Versions concernées

2024,10

Mitigation

Nous travaillons actuellement sur un correctif qui sera inclus dans une future version. Cependant, il est toujours possible de s'arrêter manuellement VDIs dans les environnements RES déployés de manière isolée VPCs.

.....

(2024.10 et versions antérieures) Impossible de lancer VDI pour les types d'instances Graphic Enhanced

Description du bogue

Lorsqu'un VDI Amazon Linux 2 - x86_64, RHEL 8 - x86_64 ou RHEL 9 x86_64 est lancé sur un type d'instance graphique amélioré (g4, g5), l'instance reste bloquée dans l'état de provisionnement. Cela signifie que l'instance n'atteindra jamais l'état « Prêt » et ne sera jamais disponible pour la connexion.

Cela se produit parce que le serveur X n'instancie pas correctement sur les instances. Après avoir appliqué ce correctif, nous vous suggérons également d'augmenter la taille du volume racine de vos piles logicielles pour les instances graphiques à 50 Go afin de garantir un espace suffisant pour installer toutes les dépendances.

Versions concernées

Toutes les versions RES 2024.10 ou antérieures.

Mitigation

1. Téléchargez les fichiers patch.py et graphic_enhanced_instance_types_fix.patch en les remplaçant `<output-directory>` par le répertoire dans lequel vous souhaitez télécharger le script de correctif et le fichier de correctif et par le nom de votre environnement RES dans la commande ci-dessous : `<environment-name>`

   a. Le correctif ne s'applique qu'à RES 2024.10.

   b. Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.

   c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patches/graphic_enhanced_instance_types_fix.patch --
output ${OUTPUT_DIRECTORY}/graphic_enhanced_instance_types_fix.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif ont été téléchargés. Exécutez la commande de correctif suivante :

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.10 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
graphic_enhanced_instance_types_fix.patch
```

3. Pour mettre fin à l'instance de Virtual Desktop Controller (vdc-controller) de votre environnement, exécutez les commandes suivantes en remplaçant le nom de votre environnement RES tel qu'il est indiqué.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

4. Lancez une nouvelle instance une fois que le groupe cible commençant par le nom `<RES-EnvironmentName>-vdc-ext` est devenu sain. Nous recommandons que toute nouvelle pile logicielle que vous enregistrez pour les instances graphiques dispose d'au moins 50 Go de stockage.

.....

(2024.08) Préparation à une défaillance de l'AMI d'infrastructure

Description du bogue

Lorsque vous préparez des AMI à l'aide d'EC2 Image Builder conformément aux instructions répertoriées dans la documentation des prérequis, le processus de création échoue avec le message d'erreur suivant :

```
CmdExecution: [ERROR] Command execution has resulted in an error
```

Cela est dû à des erreurs dans le fichier de dépendances fourni dans la documentation.

Versions concernées

2024,08

Mitigation

Créez de nouvelles ressources EC2 Image Builder :

(Suivez ces étapes si vous n'avez jamais préparé AMIs les instances RES)

1. Téléchargez le res-infra-dependenciesfichier .tar.gz mis à jour.
2. Suivez les étapes répertoriées sous Prepare Amazon Machine Images (AMIs) sur la page Prérequis.

Réutilisation des ressources précédentes d'EC2 Image Builder :

(Suivez ces étapes si vous vous êtes préparé AMIs pour les instances RES)

1. Téléchargez le res-infra-dependenciesfichier .tar.gz mis à jour.
2. Accédez à EC2 Image Builder → Composants → Cliquez sur le composant créé pour préparer AMIs RES.
3. Notez l'emplacement S3 indiqué sous Contenu → Étape de téléchargement RESInstall des scripts → entrées → source.
4. L'emplacement S3 ci-dessus contient le fichier de dépendances précédemment utilisé. Remplacez ce fichier par le fichier téléchargé lors de la première étape.

.....

(2024.08) Les bureaux virtuels ne parviennent pas à monter le compartiment read/write Amazon S3 avec l'ARN du compartiment racine et un préfixe personnalisé

Description du bogue

Research and Engineering Studio 2024.08 ne parvient pas à monter des compartiments read/write S3 sur une instance d'infrastructure de bureau virtuel (VDI) lorsqu'il utilise un ARN de bucket racine (c'est-à-dire`arn:aws:s3:::example-bucket`) et un préfixe personnalisé (nom du projet ou nom du projet et nom d'utilisateur).

Les configurations de bucket qui ne sont pas concernées par ce problème sont les suivantes :

- compartiments en lecture seule

- compartiments de lecture/écriture avec un préfixe intégré à l'ARN du compartiment (c'est-à-direarn:aws:s3:::example-bucket/example-folder-prefix) et un préfixe personnalisé (nom du projet ou nom du projet et nom d'utilisateur)
- compartiments de lecture/écriture avec un ARN de compartiment racine, mais aucun préfixe personnalisé

Une fois que vous avez provisionné une instance VDI, le répertoire de montage spécifié pour ce compartiment S3 ne comportera pas de compartiment monté. Bien que le répertoire de montage du VDI soit présent, il sera vide et ne contiendra pas le contenu actuel du bucket. Lorsque vous écrivez un fichier dans le répertoire à l'aide du terminal, l'erreur `Permission denied, unable to write a file` est générée et le contenu du fichier n'est pas transféré dans le compartiment S3 correspondant.

Versions concernées

2024,08

Mitigation

1. Pour télécharger le script de correctif et le fichier de correctif (`patch.pyets3_mount_custom_prefix_fix.patch`), exécutez la commande suivante en les `<output-directory>` remplaçant par le répertoire dans lequel vous souhaitez télécharger le script de correctif et le fichier de correctif et `<environment-name>` par le nom de votre environnement RES :

   a. Le correctif ne s'applique qu'à RES 2024.08.

   b. Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.

   c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations Amazon S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
 ${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante :

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. Pour mettre fin à l'instance de Virtual Desktop Controller (vdc-controller) de votre environnement, exécutez les commandes suivantes. (Vous avez déjà défini le nom de votre environnement RES à la `ENVIRONMENT_NAME` variable lors de la première étape.)

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> Pour les configurations VPC privées, si ce n'est pas déjà fait, pour la `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` fonction, assurez-vous d'ajouter le nom `AWS_STS_REGIONAL_ENDPOINTS` et la `Environment variable` valeur de. `regional` Pour plus d'informations, consultez Conditions requises pour les compartiments Amazon S3 pour les déploiements de VPC isolés.

4. Une fois que le groupe cible commençant par le nom *`<RES-EnvironmentName>`*`-vdc-ext` sera rétabli, un nouveau groupe VDIs devra être lancé pour que les compartiments read/write S3 dotés de l'ARN du bucket root et d'un préfixe personnalisé soient correctement montés.

.....

(2024.06) L'application d'un instantané échoue lorsque le nom du groupe AD contient des espaces

Problème

RES 2024.06 ne parvient pas à appliquer les instantanés des versions précédentes si les noms des groupes AD contiennent des espaces.

Les journaux du gestionnaire de clusters (sous le `<environment-name>/cluster-manager` groupe de CloudWatch journaux) incluront l'erreur suivante lors de la synchronisation AD :

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

L'erreur est due au fait que RES n'accepte que les noms de groupes répondant aux exigences suivantes :

- Il ne peut contenir que des lettres ASCII minuscules et majuscules, des chiffres, un tiret (-), un point (.) et un trait de soulignement (_)
- Le tiret (-) n'est pas autorisé comme premier caractère
- Il ne doit pas contenir d'espace.

Versions concernées

2024,06

Mitigation

1. Pour télécharger le script de correctif et le fichier de correctif (patch.py et groupname_regex.patch), exécutez la commande suivante, en les `<output-directory>` remplaçant par le répertoire dans lequel vous souhaitez placer les fichiers et par le nom de votre environnement `<environment-name>` RES :

   a. Le correctif ne s'applique qu'à RES 2024.06

   b. Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.

   c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES :

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante :

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Pour redémarrer l'instance de Cluster Manager pour votre environnement, exécutez les commandes suivantes : Vous pouvez également mettre fin à l'instance depuis la console de gestion Amazon EC2.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> Le correctif permet aux noms de groupes AD de contenir des lettres ASCII minuscules et majuscules, des chiffres, des tirets (-), des points (.), des traits de soulignement (_) et des espaces d'une longueur totale comprise entre 1 et 30 inclus.

.....

(2024.06 et versions antérieures) Les membres du groupe ne sont pas synchronisés avec RES lors de la synchronisation AD

Description du bogue

Les membres du groupe ne se synchroniseront pas correctement avec RES si le GroupOU est différent de l'UserOU.

RES crée un filtre ldapsearch lorsqu'il tente de synchroniser les utilisateurs d'un groupe AD. Le filtre actuel utilise incorrectement le paramètre UserOu au lieu du paramètre GroupOu. Le résultat est que la recherche ne renvoie aucun utilisateur. Ce comportement ne se produit que dans les cas où UserSOU et GroupOu sont différents.

Versions concernées

Toutes les versions RES 2024.06 ou antérieures

Mitigation

Pour résoudre le problème, procédez comme suit :

1. Pour télécharger le script patch.py et le fichier group_member_sync_bug_fix.patch, exécutez les commandes suivantes, en les remplaçant par `<output-directory>` le répertoire local dans lequel vous souhaitez télécharger les fichiers et par la version de RES que vous souhaitez patcher : `<res_version>`

   > **Note**
   >
   > - Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.
   > - Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.
   > - Le correctif ne prend en charge que les versions RES 2024.04.02 et 2024.06. Si vous utilisez le 2024.04 ou le 2024.04.01, vous pouvez suivre les étapes répertoriées dans la section pour mettre à jour votre environnement Mises à jour mineures des versions vers le 2024.04.02 avant d'appliquer le correctif.
   >   - Version RES : RES 2024.04.02

Lien de téléchargement du correctif : 2024.04.02_group_member_sync_bug_fix.patch

- Version RES : RES 2024.06

  Lien de téléchargement du correctif : 2024.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES :

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. Pour redémarrer l'instance de cluster-manager de votre environnement, exécutez les commandes suivantes :

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 et versions antérieures) CVE-2024-6387, Regre, vulnérabilité de sécurité dans et Ubuntu SSHion RHEL9 VDIs

Description du bogue

Le CVE-2024-6387, baptisé regre, a été identifié sur le SSHion serveur OpenSSH. Cette vulnérabilité permet à des attaquants distants non authentifiés d'exécuter du code arbitraire sur le serveur cible, ce qui représente un risque sérieux pour les systèmes qui utilisent OpenSSH pour sécuriser les communications.

Pour RES, la configuration standard consiste à passer par l'hôte bastion pour accéder en SSH aux bureaux virtuels, et l'hôte bastion n'est pas affecté par cette vulnérabilité. Cependant, l'AMI (Amazon Machine Image) par défaut que nous fournissons RHEL9 et Ubuntu2024 VDIs (infrastructure de bureau virtuel) dans TOUTES les versions RES utilisent une version OpenSSH vulnérable aux menaces de sécurité.

Cela signifie que les versions existantes RHEL9 et Ubuntu2024 VDIs pourraient être exploitables, mais l'attaquant aurait besoin d'accéder à l'hôte du bastion.

Vous trouverez plus de détails sur le problème ici.

Versions concernées

Toutes les versions RES 2024.06 ou antérieures.

Mitigation

Ubuntu RHEL9 et Ubuntu ont publié des correctifs pour OpenSSH qui corrigent la faille de sécurité. Ils peuvent être extraits à l'aide du gestionnaire de packages correspondant à la plateforme.

Si vous avez un système existant RHEL9 ou Ubuntu VDIs, nous vous recommandons de suivre les VDIs instructions relatives au PATCH EXISTING ci-dessous. Pour les futurs patchs VDIs, nous vous recommandons de suivre les VDIs instructions de PATCH FUTURE. Ces instructions décrivent comment exécuter un script pour appliquer la mise à jour de la plateforme sur votre VDIs.

CORRECTIF EXISTANT VDIs

1. Exécutez la commande suivante qui corrigera tous les Ubuntu existants et RHEL9 VDIs :

    a. Le script de correctif nécessite la AWS CLI v2.

b. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations de AWS Systems Manager pour envoyer une commande d'exécution de Systems Manager.

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. Vous pouvez vérifier que le script a bien été exécuté sur la page Exécuter la commande. Cliquez sur l'onglet Historique des commandes, sélectionnez l'ID de commande le plus récent et vérifiez que toutes les instances IDs ont un message de réussite.

FUTUR DU PATCH VDIs

1. Pour télécharger le script de correctif et le fichier de correctif (patch.py et update_openssh.patch), exécutez les commandes suivantes, en les `<output-directory>` remplaçant par le répertoire dans lequel vous souhaitez télécharger les fichiers et `<environment-name>` par le nom de votre environnement RES :

> **Note**
>
> - Le correctif ne s'applique qu'à RES 2024.06.
> - Le script de correctif nécessite AWS CLI (v2), Python 3.9.16 ou supérieur et Boto3.
> - Configurez votre copie de la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Exécutez la commande de correctif suivante :

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. Redémarrez l'instance du contrôleur VDC pour votre environnement à l'aide des commandes suivantes :

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

Important

Les futurs correctifs ne VDIs sont pris en charge que sur les versions RES 2024.06 et ultérieures. Pour corriger les futurs environnements RES dont les versions sont antérieures VDIs à 2024.06, commencez par mettre à niveau l'environnement RES vers 2024.06 en suivant les instructions fournies à l'adresse :. Mises à jour majeures des versions

.....

(2024.04-2024.04.02) La limite d'autorisation IAM fournie n'est pas attachée au rôle des instances VDI

Le problème

Les sessions de bureau virtuel n'héritent pas correctement de la configuration des limites d'autorisation de leur projet. Cela est dû au fait que la limite d'autorisations définie par le paramètre IAMPermission Boundary n'a pas été correctement attribuée à un projet lors de sa création.

Versions concernées

2024,04 - 2024,04.02

Mitigation

Suivez ces étapes pour VDIs hériter correctement de la limite d'autorisations attribuée à un projet :

1. Pour télécharger le script de correctif et le fichier de correctif (patch.py et vdi_host_role_permission_boundary.patch), exécutez la commande suivante, en les remplaçant par le répertoire local dans lequel vous souhaitez placer les fichiers : `<output-directory>`

   a. Le correctif ne s'applique qu'à RES 2024.04.02. Si vous utilisez la version 2024.04 ou 2024.04.01, vous pouvez suivre les étapes répertoriées dans le document public pour les mises à jour de version mineures afin de mettre à jour votre environnement vers la version 2024.04.02.

   b. Le script de correctif nécessite AWS CLI (v2), Python 3.9.16 ou supérieur et Boto3.

   c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES :

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Redémarrez l'instance de cluster-manager dans votre environnement en exécutant cette commande, en la `<environment-name>` remplaçant par le nom de votre environnement RES. Vous pouvez également mettre fin à l'instance depuis la console de gestion Amazon EC2.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 et versions antérieures) Les instances Windows NVIDIA dans ap-southeast-2 (Sydney) ne démarrent pas

Le problème

Les Amazon Machine Images (AMIs) sont utilisées pour créer des bureaux virtuels (VDIs) dans RES avec des configurations spécifiques. Chaque AMI possède un identifiant associé qui diffère selon les régions. L'ID AMI configuré dans RES pour lancer des instances Windows Nvidia dans ap-southeast-2 (Sydney) est actuellement incorrect.

L'AMI-ID `ami-0e190f8939a996caf` pour ce type de configuration d'instance n'est pas correctement répertorié dans ap-southeast-2 (Sydney). L'ID AMI `ami-027cf6e71e2e442f4` doit être utilisé à la place.

Les utilisateurs obtiendront le message d'erreur suivant lorsqu'ils essaieront de lancer une instance avec l'`ami-0e190f8939a996caf`AMI par défaut.

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id '[ami-0e190f8939a996caf]' does not exist
```

Étapes pour reproduire le bogue, y compris un exemple de fichier de configuration :

- Déployez RES dans la région ap-southeast-2.
- Lancez une instance à l'aide de la pile logicielle par défaut Windows-NVIDIA (ID `ami-0e190f8939a996caf` AMI).

Versions concernées

Toutes les versions de RES 2024.04.02 ou antérieures sont concernées

Mitigation

Les mesures d'atténuation suivantes ont été testées sur la version RES 2024.01.01 :

- Enregistrez une nouvelle pile logicielle avec les paramètres suivants
  - ID D'AMI : `ami-027cf6e71e2e442f4`
  - Système d'exploitation : Windows
  - Fabricant du GPU : NVIDIA
  - Minimum. Taille de stockage (Go) : 30
  - Minimum. RAM (GO) : 4
- Utilisez cette pile logicielle pour lancer des instances Windows-NVIDIA

.....

(2024.04 et 2024.04.01) Échec de la suppression RES dans GovCloud

Le problème

Pendant le processus de suppression RES, le `UnprotectCognitoUserPool` Lambda désactive la protection contre la suppression pour les groupes d'utilisateurs de Cognito qui seront supprimés ultérieurement. L'exécution Lambda est démarrée par le. `InstallerStateMachine`

En raison des différences de version de la AWS CLI par défaut entre la version commerciale et les GovCloud régions, l'`update_user_pool`appel dans le Lambda échouera dans les GovCloud régions.

Les clients recevront le message d'erreur suivant lorsqu'ils tenteront de supprimer RES dans une GovCloud région :

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Étapes pour reproduire le bogue :

- Déployer RES dans une GovCloud région
- Supprimer la pile RES

Versions concernées

Versions RES 2024.04 et 2024.04.01

Mitigation

Les mesures d'atténuation suivantes ont été testées sur la version 2024.04 de RES :

- Ouvrez le `UnprotectCognitoUserPool` Lambda
  - Convention de dénomination : *<env-name>*-`InstallerTasksUnprotectCognitoUserPool-...`
- Paramètres d'exécution -> Modifier -> Sélectionnez Runtime `Python 3.11` -> Enregistrer.
- Ouverte CloudFormation.
- Supprimer la pile RES -> laisser Retain Installer Resource NON COCHÉE -> Supprimer.

.....

(2024.04 - 2024.04.02) Le bureau virtuel Linux peut être bloqué à l'état « REPRISE » au redémarrage

Le problème

Les bureaux virtuels Linux peuvent rester bloqués en état « REPRISE » lors du redémarrage après un arrêt manuel ou programmé.

Une fois l'instance redémarrée, le AWS Systems Manager n'exécute aucune commande à distance pour créer une nouvelle session DCV et le message de journal suivant est absent des journaux du contrôleur vdc (sous le groupe de CloudWatch journaux) : `<environment-name>/vdc/controller` CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Versions concernées

2024,04 - 2024,04.02

Mitigation

Pour récupérer les bureaux virtuels bloqués à l'état « REPRISE », procédez comme suit :

1. Connectez-vous en SSH à l'instance problématique depuis la console EC2.
2. Exécutez les commandes suivantes sur l'instance :

```
sudo su -
/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
configure_post_reboot.sh
sudo reboot
```

3. Attendez que l'instance redémarre.

Pour éviter que les nouveaux bureaux virtuels ne rencontrent le même problème :

1. Pour télécharger le script de correctif et le fichier de correctif (patch.py et vdi_stuck_in_resuming_status.patch), exécutez la commande suivante en les remplaçant par le répertoire dans lequel vous souhaitez placer les fichiers : `<output-directory>`

> **Note**
>
> - Le correctif ne s'applique qu'à RES 2024.04.02.
> - Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.
> - Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES et `<aws-region>` par la région dans laquelle RES est déployé :

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Pour redémarrer l'instance de contrôleur VDC pour votre environnement, exécutez les commandes suivantes, en `<environment-name>` remplaçant par le nom de votre environnement RES :

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 et versions antérieures) Impossible de synchroniser les utilisateurs AD dont l'attribut SAMAccount Name inclut des majuscules ou des caractères spéciaux

Le problème

RES ne parvient pas à synchroniser les utilisateurs AD après la configuration du SSO pendant au moins deux heures (deux cycles de synchronisation AD). Les journaux du gestionnaire de clusters (sous le `<environment-name>/cluster-manager` groupe de CloudWatch journaux) incluent l'erreur suivante lors de la synchronisation AD :

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

L'erreur est due au fait que RES n'accepte qu'un SAMAccount nom d'utilisateur répondant aux exigences suivantes :

- Il ne peut contenir que des lettres ASCII minuscules, des chiffres, un point (.), un trait de soulignement (_).
- Le point ou le trait de soulignement ne sont pas autorisés comme premier ou dernier caractère.
- Il ne peut pas contenir deux points continus ou deux traits de soulignement (par exemple,.., __, ._, _.).

Versions concernées

2024.04.02 et versions antérieures

Mitigation

1. Pour télécharger le script de correctif et le fichier de correctif (patch.py et samaccountname_regex.patch), exécutez la commande suivante, en les remplaçant par le répertoire dans lequel vous `<output-directory>` souhaitez placer les fichiers :

   > **Note**
   >
   > - Le correctif ne s'applique qu'à RES 2024.04.02.
   > - Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.
   > - Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

   ```
   OUTPUT_DIRECTORY=<output-directory>

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
   ```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
 ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES :

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Pour redémarrer l'instance de Cluster Manager pour votre environnement, exécutez les commandes suivantes en `<environment-name>` remplaçant par le nom de votre environnement RES. Vous pouvez également mettre fin à l'instance depuis la console de gestion Amazon EC2.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 et versions antérieures) La clé privée pour accéder à l'hôte Bastion n'est pas valide

Le problème

Lorsqu'un utilisateur télécharge la clé privée pour accéder à l'hôte Bastion depuis le portail Web RES, la clé n'est pas correctement formatée : plusieurs lignes sont téléchargées en une seule ligne, ce qui rend la clé non valide. L'utilisateur obtiendra le message d'erreur suivant lorsqu'il tentera d'accéder à l'hôte du bastion avec la clé téléchargée :

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
```

```
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)
```

Versions concernées

2024.04.02 et versions antérieures

Mitigation

Nous vous recommandons d'utiliser Chrome pour télécharger les clés, car ce navigateur n'est pas concerné.

Le fichier clé peut également être reformaté en créant une nouvelle ligne après `-----BEGIN PRIVATE KEY-----` et une autre ligne juste avant. `-----END PRIVATE KEY-----`

.....

Notifications

Chaque EC2 instance Amazon est fournie avec deux licences Remote Desktop Services (Terminal Services) à des fins d'administration. Ces informations sont disponibles pour vous aider à fournir ces licences à vos administrateurs. Vous pouvez également utiliser AWS Systems Manager Session Manager, qui permet de vous connecter à distance aux EC2 instances Amazon sans RDP et sans avoir besoin de licences RDP. Si des licences Remote Desktop Services supplémentaires sont nécessaires, l'utilisateur de Remote Desktop CALs doit être acheté auprès de Microsoft ou d'un revendeur de licences Microsoft. Les utilisateurs de Remote Desktop bénéficiant d' CALs une assurance logicielle active bénéficient des avantages de la mobilité des licences et peuvent être transférés vers des environnements locataires (partagés) AWS par défaut. Pour plus d'informations sur l'acquisition de licences sans les avantages liés à l'assurance logicielle ou à la mobilité des licences, consultez cette section de la FAQ.

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques AWS actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. AWS les responsabilités et les obligations envers ses clients sont régies par AWS des accords, et le présent document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne le modifie pas.

Research and Engineering Studio on AWS est licencié selon les termes de la licence Apache version 2.0 disponible auprès de l'Apache Software Foundation.

Révisions

Pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub

Date	Modifier
Mars 2025	• Version de sortie 2025.03 Sections ajoutées — • Désactiver un projet. • Supprime un projet.. • Tableau de bord d'analyse des coûts. Sections modifiées — • Bureaux virtuels. • Piles de logiciels () AMIs. • Configurez Res Ready AMIs. • Réglages du bureau. • Configuration de l'accès SSH. • Synchronisation Active Directory.
décembre 2024	• Version de sortie 2024.12 Sections ajoutées — • Synchronisation Active Directory. • Configuration des autorisations de bureau. • Configuration de l'accès au navigateur de fichiers. • Configuration de l'accès SSH. • Configuration des utilisateurs d'Amazon Cognito. Sections modifiées — • Limites de l'environnement.

Date	Modifier
	• Configuration d'un VPC privé (facultatif).
Octobre 2024	• Version de sortie 2024.10 : Ajout du support pour — • Limites de l'environnement. • Profils de partage de bureau. • Arrêt automatique de l'interface de bureau virtuel.
août 2024	• Version de sortie 2024.08 : Ajout du support pour — • montage de compartiments Amazon S3 sur des instances d'infrastructure de bureau virtuel (VDI) Linux. Consultez Compartiments Amazon S3. • des autorisations de projet personnal isées, un modèle d'autorisation amélioré qui permet de personnaliser les rôles existants et d'ajouter des rôles personnal isés. Consultez Stratégie d'autorisation. • Guide de l'utilisateur : Résolution des problèmes section élargie.
Juin 2024	• Sortie de la version 2024.06 — Support d'Ubuntu, autorisations du propriétaire du projet. • Guide de l'utilisateur : ajouté Création d'un environnement de démonstration
Avril 2024	Version de publication 2024.04 — Modèles prêts pour le RES AMIs et pour le lancement de projets

Date	Modifier
Mars 2024	Rubriques de résolution des problèmes supplémentaires, conservation CloudWatch des journaux, désinstallation des versions mineures
Février 2024	Version de publication 2024.01.01 — modèle de déploiement mis à jour
Janvier 2024	Version de sortie 2024.01
Décembre 2023	GovCloud instructions et modèles ajoutés
Novembre 2023	Première version

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.