aws

Administratorhandbuch

WorkSpaces Sicherer Browser von Amazon

WorkSpaces Sicherer Browser von Amazon: Administratorhandbuch

Table of Contents

Was ist Amazon WorkSpaces Secure Browser?

> **Note**
>
> Amazon WorkSpaces Secure Browser war zuvor als Amazon WorkSpaces Web bekannt.

Amazon WorkSpaces Secure Browser ist ein vollständig verwalteter, Cloud-nativer, gehosteter Browser-Service, der für den sicheren Zugriff auf private Websites und software-as-a-service (SaaS-) Webanwendungen, die Interaktion mit Online-Ressourcen und das Surfen im Internet von einem Einwegcontainer aus verwendet wird. WorkSpaces Secure Browser funktioniert mit den vorhandenen Webbrowsern eines Benutzers, ohne die IT mit der Verwaltung von Geräten, Infrastruktur, spezialisierter Client-Software oder VPN-Verbindungen (Virtual Private Network) zu belasten. Webinhalte werden in den Webbrowser des Benutzers gestreamt, während der eigentliche Browser und die Webinhalte isoliert sind. AWS Durch die Verwendung derselben zugrunde liegenden Technologien, die AWS Endbenutzer-Computing-Dienste wie Amazon WorkSpaces und Amazon WorkSpaces Applications unterstützen, kann WorkSpaces Secure Browser kostengünstiger sein als herkömmliche virtuelle Desktops und die Komplexität reduzieren, verglichen mit der Bereitstellung von Verwaltungssoftware für firmeneigene Geräte. WorkSpaces Secure Browser reduziert das Risiko der Datenexfiltration durch das Streamen von Webinhalten. Es werden kein HTML, kein DOM (Document Object Model) oder sensible Unternehmensdaten an den lokalen Computer übertragen. Durch die Isolierung von Gerät, Unternehmensnetzwerk und Internet voneinander wird die Angriffsfläche des Browsers praktisch eliminiert.

Sie können die Browser-Richtlinien Ihres Unternehmens (einschließlich URL-Zulassen/Blockieren) für alle Sitzungen durchsetzen. Dazu gehören auch Kontrollen auf Sitzungsebene für Zwischenablage, Dateiübertragung und Drucker. Sie können den Zugriff auf vertrauenswürdige Netzwerke oder Geräte auch mithilfe von IP-Zugriffskontrollen einschränken. WorkSpaces Secure Browser ist einfach einzurichten und zu bedienen. Jede Sitzung wird mit einer neuen und vollständig gepatchten Version des Chrome-Browsers gestartet, auf die Unternehmensrichtlinien und -einstellungen angewendet werden.

Versionsverlauf für Amazon WorkSpaces Secure Browser

Am 20. Mai 2024 wurde Amazon WorkSpaces Web in Amazon WorkSpaces Secure Browser umbenannt. Für Bestandskunden gab es keine Änderung an der Art und Weise, wie sie Benutzer

oder Ressourcen mit dem Service verwalten. In der folgenden Liste werden die entsprechenden Aktualisierungen beschrieben, die ebenfalls als Ergebnis dieser Umbenennung vorgenommen wurden.

Der Workspaces-Web-API-Namespace bleibt aus Gründen der Abwärtskompatibilität unverändert. Daher sind die folgenden Ressourcen immer noch dieselben:

- CLI-Befehle.
- CloudWatch Amazon-Metriken. Weitere Informationen finden Sie unter the section called “Überwachung mit CloudWatch”.
- Service-Endpunkte. Weitere Informationen finden Sie unter Amazon WorkSpaces Secure Browser Endpoints and Quotas.
- AWS CloudFormation Ressourcen. Weitere Informationen finden Sie in der Referenz zum Amazon WorkSpaces Secure Browser-Ressourcentyp.
- Servicebezogene Rolle, die workspaces-web enthält. Weitere Informationen finden Sie unter the section called “Verwenden von servicegebundenen Rollen”.
- Konsole mit workspaces-web. URLs
- Dokumentation URLs , die Workspaces-Web enthält. Weitere Informationen finden Sie in der Amazon WorkSpaces Secure Browser-Dokumentation.
- Bestehende ReadOnly verwaltete Rolle. Weitere Informationen finden Sie unter the section called “AWS verwaltete Richtlinien”.
- Name des KMS-Zuschusses.
- UAL (Benutzeraktivitätsprotokollierung) Kinesis-Stream-Präfix.

Darüber hinaus bleibt das bestehende Portal URLs unverändert. URLs für Portale, die vor dem 20. Mai 2024 erstellt wurden, wurde das Format <UUID>.workspaces-web.com verwendet. WorkSpaces Secure Browser-Portale verwenden weiterhin dieses Format und die Domäne workspaces-web.com.

Begriffe, die Sie bei der Verwendung von Amazon WorkSpaces Secure Browser beachten sollten

Um Ihnen den Einstieg in WorkSpaces Secure Browser zu erleichtern, sollten Sie sich mit den folgenden Konzepten vertraut machen.

Identity provider (IdP) (Identitätsanbieter (IdP))

Ein Identitätsanbieter verifiziert die Anmeldeinformationen Ihrer Benutzer. Er stellt dann die Authentifizierungszusicherungen aus, um Zugriff auf einen Dienstanbieter bereitzustellen. Sie können Ihren vorhandenen IdP so konfigurieren, dass er mit WorkSpaces Secure Browser funktioniert.

Der Prozess zur Konfiguration Ihres Identitätsanbieters (IDP) variiert je nach Identitätsanbieter.

Sie müssen die Metadatendatei des Dienstanbieters zu Ihrem Identitätsanbieter hochladen. Andernfalls können sich Ihre Benutzer nicht anmelden. Sie müssen Ihren Benutzern auch Zugriff gewähren, um den WorkSpaces sicheren Browser in Ihrem IdP zu verwenden.

Metadatendokument des Identitätsanbieters

WorkSpaces Secure Browser benötigt spezifische Metadaten von Ihrem Identitätsanbieter (IdP), um Vertrauen aufzubauen. Sie können diese Metadaten zu WorkSpaces Secure Browser hinzufügen, indem Sie eine von Ihrem IdP heruntergeladene Metadaten-Austauschdatei hochladen.

Dienstanbieter (Service Provider, SP)

Ein Dienstanbieter akzeptiert Authentifizierungsbestätigungen und stellt dem Benutzer einen Service zur Verfügung. WorkSpaces Secure Browser fungiert als Dienstanbieter für Benutzer, die von ihrem IdP authentifiziert wurden.

Dienstanbieter-Metadatendokument

Sie müssen die Metadatendetails des Dienstanbieters zur Konfigurationsoberfläche Ihres Identitätsanbieters hinzufügen. Die Einzelheiten dieses Konfigurationsprozesses variieren je nach Anbieter.

SAML 2.0

Ein Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen einem IdP und einem Dienstanbieter.

Virtual Private Cloud (VPC)

Sie können eine vorhandene oder neue VPC, entsprechende Subnetze und Sicherheitsgruppen verwenden, um Ihre Inhalte mit WorkSpaces Secure Browser zu verknüpfen.

Subnetze müssen über eine stabile Internetverbindung verfügen. Außerdem müssen die VPC und die Subnetze über eine stabile Verbindung mit allen internen Websites und Websites für Software as a Service (SaaS) verfügen, damit Benutzer auf diese Ressourcen zugreifen können.

Die VPCs aufgelisteten Subnetze und Sicherheitsgruppen stammen aus derselben Region wie Ihre WorkSpaces Secure Browser-Konsole.

Trust Store (Vertrauensspeicher)

Wenn ein Benutzer, der über WorkSpaces Secure Browser auf eine Website zugreift, einen Datenschutzfehler wie NET: :ERR_CERT_INVALID erhält, verwendet diese Website möglicherweise ein Zertifikat, das von einer privaten Zertifizierungsstelle (PCA) signiert wurde. Möglicherweise müssen Sie das in Ihrem Trust Store hinzufügen oder ändern. PCAs Wenn Sie auf dem Gerät eines Benutzers ein bestimmtes Zertifikat installieren müssen, um eine Website laden zu können, müssen Sie dieses Zertifikat außerdem zu Ihrem Trust Store hinzufügen, damit Ihr Benutzer im WorkSpaces abgesicherten Browser auf diese Site zugreifen kann.

Für öffentlich zugängliche Websites sind in der Regel keine Änderungen an einem Trust Store erforderlich.

Webportale

Ein Webportal bietet Ihren Benutzern über ihren Browser Zugriff auf interne Websites und SaaS-Websites. Sie können in jeder unterstützten Region ein Webportal pro Konto erstellen. Wenn Sie eine Limiterhöhung für mehr als ein Portal anfordern möchten, wenden Sie sich an den Support.

Webportal-Endpunkt

Der Webportal-Endpunkt ist der Zugangspunkt, von dem aus Ihre Benutzer Ihr Webportal starten, nachdem sie sich mit dem für das Portal konfigurierten Identitätsanbieter angemeldet haben.

Der Endpunkt ist öffentlich im Internet verfügbar und kann in Ihr Netzwerk eingebettet werden.

AWS Dienste im Zusammenhang mit Amazon WorkSpaces Secure Browser

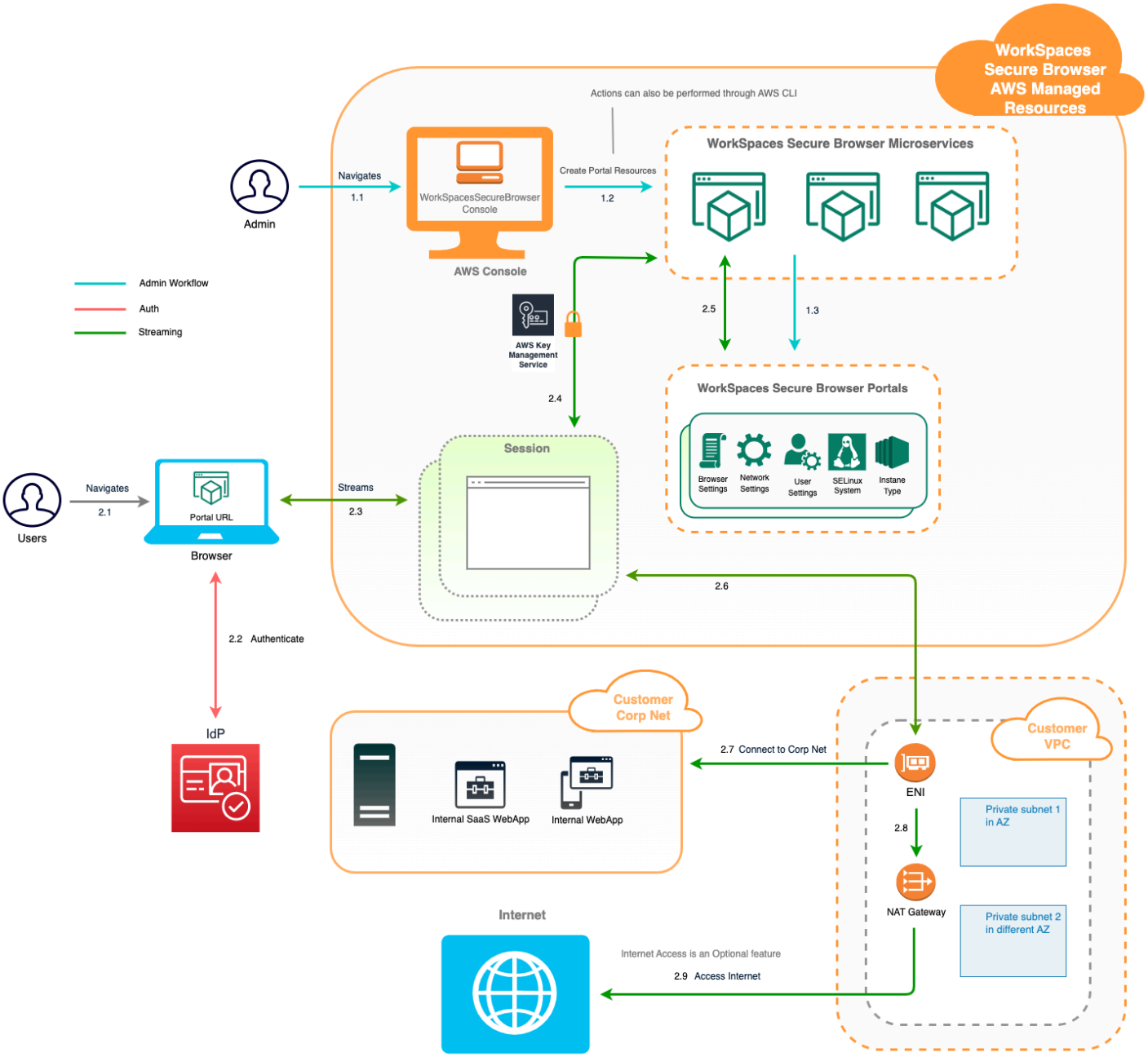
Es gibt mehrere AWS Dienste, die sich auf WorkSpaces Secure Browser beziehen.

WorkSpaces Secure Browser ist eine Funktion von Amazon WorkSpaces im AWS End User Computing-Portfolio. Im Vergleich zu WorkSpaces und AppStream 2.0 wurde WorkSpaces Secure Browser speziell für sichere, webbasierte Workloads entwickelt. WorkSpaces Secure Browser wird automatisch verwaltet, wobei Kapazität, Skalierung und Images bei Bedarf von AWS bereitgestellt und aktualisiert werden. Sie können sich beispielsweise dafür entscheiden, Ihren Softwareentwicklern, die Zugriff auf Desktop-Ressourcen benötigen, einen persistenten Workspace

Desktop und den Contact-Center-Benutzern, die nur Zugriff auf eine Handvoll interner und SaaS-Websites (einschließlich außerhalb Ihres Netzwerks gehosteter Websites) auf Desktop-Computern benötigen, WorkSpaces Secure Browser anzubieten.

Architektur von Amazon WorkSpaces Secure Browser

Das folgende Diagramm zeigt die Architektur von WorkSpaces Secure Browser.



Zugreifen auf Amazon WorkSpaces Secure Browser

Sie können auf verschiedene Arten auf WorkSpaces Secure Browser zugreifen.

Administratoren greifen über die WorkSpaces WorkSpaces Secure Browser Console, das SDK, die CLI oder die API auf Secure Browser zu. Ihre Benutzer greifen über den WorkSpaces Secure Browser-Endpunkt darauf zu.

Amazon WorkSpaces Secure Browser einrichten

Bevor Sie WorkSpaces Secure Browser für den Zugriff auf Ihre internen Websites und SaaS-Anwendungen konfigurieren können, müssen Sie die folgenden Voraussetzungen erfüllen.

Topics

Registrieren und Erstellen eines Benutzers

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung -Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center -Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center - Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center - Benutzerhandbuch.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS-Managementkonsole Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldeinformationen als temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command Line Interface Benutzerhandbuch. • Weitere Informationen finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		AWS SDKs und im Tools-Referenzhandbuch. AWS SDKs
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Ref erenzhandbuch.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldeinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Netzwerke für Amazon WorkSpaces Secure Browser

In den folgenden Themen wird erklärt, wie Sie WorkSpaces Secure Browser-Streaming-Instances einrichten, damit Benutzer eine Verbindung zu ihnen herstellen können. Außerdem wird erklärt, wie Sie Ihren WorkSpaces Secure Browser-Streaming-Instances den Zugriff auf VPC-Ressourcen sowie auf das Internet ermöglichen.

Topics

- Einrichtung einer VPC für Amazon WorkSpaces Secure Browser

- Benutzerverbindungen für Amazon WorkSpaces Secure Browser aktivieren

Einrichtung einer VPC für Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um eine VPC für WorkSpaces Secure Browser einzurichten und zu konfigurieren.

Topics

- VPC-Anforderungen für Amazon WorkSpaces Secure Browser
- Eine neue VPC für Amazon WorkSpaces Secure Browser erstellen
- Aktivieren des Surfens im Internet für Amazon WorkSpaces Secure Browser
- Bewährte VPC-Methoden für WorkSpaces Secure Browser
- Unterstützte Availability Zones für Amazon WorkSpaces Secure Browser

VPC-Anforderungen für Amazon WorkSpaces Secure Browser

Bei der Erstellung des WorkSpaces Secure Browser-Portals wählen Sie eine VPC in Ihrem Konto aus. Sie wählen auch mindestens zwei Subnetze in zwei verschiedenen Availability Zones aus. Diese VPCs und Subnetze müssen die folgenden Anforderungen erfüllen:

- Die VPC muss über eine Standardmietdauer verfügen. VPCs mit Dedicated Tenancy werden nicht unterstützt.
- Aus Gründen der Verfügbarkeit benötigen wir mindestens zwei Subnetze, die in zwei verschiedenen Availability Zones erstellt wurden. Ihre Subnetze müssen über ausreichend IP-Adressen verfügen, um den erwarteten WorkSpaces Secure Browser-Verkehr zu unterstützen. Konfigurieren Sie jedes Ihrer Subnetze mit einer Subnetzmaske, die genügend Client-IP-Adressen für die maximale Anzahl der gleichzeitigen Sitzungen ermöglicht. Weitere Informationen finden Sie unter Eine neue VPC für Amazon WorkSpaces Secure Browser erstellen.
- Alle Subnetze müssen über eine stabile Verbindung zu allen internen Inhalten verfügen, die sich entweder vor Ort AWS Cloud oder vor Ort befinden und auf die Benutzer mit WorkSpaces Secure Browser zugreifen können.

Wir empfehlen Ihnen, aus Gründen der Verfügbarkeit und der Skalierung drei Subnetze in unterschiedlichen Availability Zones auszuwählen. Weitere Informationen finden Sie unter Eine neue VPC für Amazon WorkSpaces Secure Browser erstellen.

WorkSpaces Secure Browser weist Streaming-Instanzen keine öffentliche IP-Adresse zu, um den Internetzugang zu ermöglichen. Sonst wären Ihre Streaming-Instances über das Internet erreichbar. Daher hat keine Streaming-Instance, die mit Ihrem öffentlichen Subnetz verbunden ist, Internetzugang. Wenn Sie möchten, dass Ihr WorkSpaces Secure Browser-Portal sowohl auf öffentliche Internetinhalte als auch auf private VPC-Inhalte zugreifen kann, führen Sie die Schritte unter aus. Uneingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser aktivieren (empfohlen)

Eine neue VPC für Amazon WorkSpaces Secure Browser erstellen

In diesem Abschnitt wird beschrieben, wie Sie mit dem VPC-Assistenten schnell eine VPC mit öffentlichen und privaten Subnetzen erstellen können. Der Assistent erstellt automatisch ein Internet-Gateway und ein NAT-Gateway und konfiguriert Routing-Tabellen für Ihre Subnetze.

Weitere Informationen zu dieser Konfiguration finden Sie unter VPC mit öffentlichen und privaten Subnetzen (NAT).

Topics

Schnelle VPC-Einrichtung (1 Minute)

Führen Sie die folgenden Schritte aus, um schnell eine dedizierte VPC für WorkSpaces Secure Browser mit öffentlichen und privaten Subnetzen für den Internetzugang zu erstellen. Wenn Sie eine vorhandene VPC verwenden möchten, überprüfen SieVPC-Anforderungen für Amazon WorkSpaces Secure Browser, ob sie die Anforderungen erfüllt.

> **Note**
>
> Stellen Sie sicher, dass Sie sich in der gewünschten AWS-Region Version befinden. Sie können die Region bei Bedarf in der Konsole ändern.

So richten Sie schnell eine VPC ein

1. Öffnen Sie den VPC-Erstellungsassistenten: VPC mit Ressourcen erstellen. Behalten Sie alle Einstellungen als Standard bei, sofern nicht unten anders angegeben:

- Wählen Sie unter Zu erstellende Ressource die Option VPC und mehr aus.
- Wählen Sie für das Namens-Tag die Option Automatisch generieren aus und geben Sie einen aussagekräftigen Namen für Ihre VPC ein (z. B.). **`WSB-VPC`**
- Für den IPv4 CIDR-Block verwendet die VPC standardmäßig. **`10.0.0.0/16`** Sie können bei Bedarf einen anderen IPv4 CIDR-Block angeben.
- Wählen Sie für Tenancy die Option Standard (VPCs mit dedizierten Mandanten werden nicht unterstützt).
- Wählen Sie für Anzahl der Availability Zones (AZs) die Option 2 aus.
  - Erweitern Sie Anpassen AZs und wählen Sie 2 verschiedene Availability Zones aus, die von WorkSpaces Secure Browser unterstützt werden. Eine Liste der unterstützten AZs Optionen finden Sie unterUnterstützte Availability Zones für Amazon WorkSpaces Secure Browser.
- Wählen Sie für Anzahl der öffentlichen Subnetze den Wert 2 aus.
- Wählen Sie für Anzahl der privaten Subnetze den Wert 2 aus.
- Wenn Sie für Subnetz-CIDR-Blöcke die CIDR-Blöcke in Ihren Subnetzen anpassen müssen, erweitern Sie die Option CIDR-Blöcke für Subnetze anpassen. Stellen Sie sicher, dass jedes Subnetz über ausreichend IP-Adressen für den erwarteten Datenverkehr verfügt.
- Wählen Sie für NAT-Gateways Regional aus, um den Internetzugang für private Subnetze in allen Availability Zones zu aktivieren.
- Wählen Sie für VPC-Endpoints die Option Keine aus. Wenn Sie direkten S3-Zugriff benötigen, ohne das NAT-Gateway zu verwenden, wählen Sie S3-Gateway aus.
- Lassen Sie für DNS-Optionen die DNS-Optionen aktiviert (Standard), um eine korrekte Namensauflösung in Ihrer VPC sicherzustellen.

2. Sehen Sie sich den Vorschaufenster an und wählen Sie dann Create VPC aus.

> **Note**
>
> Für NAT-Gateways und VPC-Endpunkte fallen zusätzliche Gebühren an. Weitere Informationen finden Sie auf der VPC-Preisseite.

Überprüfen Sie Ihre Subnetz-Routing-Tabellen (optional)

Der VPC-Assistent konfiguriert die Routentabellen automatisch für Sie. Wenn Sie Ihre VPC manuell erstellt haben oder die Konfiguration bestätigen möchten, können Sie überprüfen, ob die folgenden Details für Ihre Routing-Tabelle korrekt sind:

- Die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem sich das NAT-Gateway befindet, muss eine Route enthalten, die den Internetdatenverkehr zu einem Internet-Gateway leitet. Dadurch wird sichergestellt, dass Ihr NAT-Gateway Zugriff auf das Internet hat.
- Die Routing-Tabellen, die Ihren privaten Subnetzen zugeordnet sind, müssen so konfiguriert sein, dass der Internetdatenverkehr zum NAT-Gateway geleitet wird. So können die Streaming-Instances innerhalb Ihrer privaten Subnetze mit dem Internet kommunizieren.

So überprüfen und benennen Sie die Subnetz-Routing-Tabellen

1. Wählen Sie im Navigationsbereich Subnetze und dann ein öffentliches Subnetz aus. Zum Beispiel WSB-VPC-Subnet-Public1-US-East-1A.
2. Wählen Sie auf der Registerkarte Route Table (Routing-Tabelle) die ID der Routing-Tabelle aus. Zum Beispiel rtb-12345678.
3. Wählen Sie die -Routing-Tabelle aus. Wählen Sie unter Name das Bearbeitungssymbol (Stift) aus und geben Sie einen Namen für die Tabelle ein. Geben Sie beispielsweise den Namen **`workspacesweb-public-routetable`** ein. Wählen Sie dann das Häkchen aus, um den Namen zu speichern.
4. Stellen Sie bei weiterhin markierter öffentlicher Routing-Tabelle auf der Registerkarte Routen sicher, dass zwei Routen vorhanden sind: eine für den lokalen Datenverkehr sowie eine weitere, über die der übrige Datenverkehr an das Internet-Gateway für die VPC gesendet wird. In der folgenden Tabelle werden diese beiden Routen beschrieben.

Bestimmungsort	Target	Description
CIDR-Block für öffentlic he Subnetze (z. B. IPv4 10.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, der für IPv4 Adressen innerhalb des CIDR-Blocks des öffentlic hen Subnetzes bestimmt ist. IPv4 Dieser Datenverkehr

Bestimmungsort	Target	Description
		wird lokal innerhalb der VPC weitergeleitet.
Verkehr, der an alle anderen IPv4 Adressen gerichtet ist (z. B. 0.0.0.0/0)	Ausgehend (igw-ID)	Datenverkehr, der für alle anderen IPv4 Adressen bestimmt ist, wird an das Internet-Gateway (identifiziert durch IGW-ID) weitergeleitet, das vom VPC-Assistenten erstellt wurde.

5. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie dann ein privates Subnetz aus (z. B.). **`WSB-VPC-subnet-private1-us-east-1a`**
6. Wählen Sie auf der Registerkarte Routing-Tabelle die ID der Routing-Tabelle aus.
7. Wählen Sie die -Routing-Tabelle aus. Wählen Sie unter Name das Bearbeitungssymbol (Stift) aus und geben Sie einen Namen für die Tabelle ein. Geben Sie beispielsweise den Namen **`WSB-VPC-private-routetable`** ein. Wählen Sie dann das Häkchen aus, um den Namen zu speichern.
8. Überprüfen Sie auf der Registerkarte Routes (Routen), ob die Routing-Tabelle die folgenden Routen enthält:

Bestimmungsort	Target	Description
IPv4 CIDR-Block für öffentliche Subnetze (z. B. 10.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, die für IPv4 Adressen innerhalb des IPv4 CIDR-Blocks des öffentlichen Subnetzes bestimmt sind, wird lokal innerhalb der VPC weitergeleitet.
Datenverkehr, der an alle anderen IPv4 Adressen gerichtet ist (z. B. 0.0.0.0/0)	Ausgehend (nat-ID)	Datenverkehr, der für alle anderen IPv4 Adressen bestimmt ist, wird an das

Bestimmungsort	Target	Description
		NAT-Gateway weitergeleitet (identifiziert durch die NAT-ID).
Für S3-Buckets bestimmter Datenverkehr (anwendbar, wenn Sie einen S3-Endpunkt angegeben haben) [pl-ID (com.amazonaws.region.s3)]	Speicher (vpce-ID)	Datenverkehr, der für S3-Buckets bestimmt ist, wird an den S3-Endpunkt weitergeleitet (identifiziert durch vpce-ID).

9. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie dann das zweite private Subnetz aus, das Sie erstellt haben (zum Beispiel **`WorkSpaces Secure Browser Private Subnet2`**).
10. Stellen Sie auf der Registerkarte Routing-Tabelle sicher, dass es sich bei der ausgewählten Routing-Tabelle um die private Routing-Tabelle handelt (z. B. **`workspacesweb-private-routetable`**). Wenn eine andere Routing-Tabelle angezeigt wird, wählen Sie Bearbeiten aus und wählen Sie stattdessen Ihre private Routing-Tabelle aus.

Aktivieren des Surfens im Internet für Amazon WorkSpaces Secure Browser

Sie können wählen, ob Sie uneingeschränktes Surfen im Internet (die empfohlene Option) oder eingeschränktes Surfen im Internet aktivieren möchten.

Topics

- Uneingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser aktivieren (empfohlen)
- Eingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser aktivieren
- Anschlüsse für Internetkonnektivität für Amazon WorkSpaces Secure Browser

Uneingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser aktivieren (empfohlen)

Gehen Sie folgendermaßen vor, um eine VPC mit einem NAT-Gateway für uneingeschränktes Surfen im Internet zu konfigurieren. Dies gewährt WorkSpaces Secure Browser Zugriff auf Websites im öffentlichen Internet und auf private Websites, die in oder mit Ihrer VPC gehostet werden.

So konfigurieren Sie eine VPC mit einem NAT-Gateway für uneingeschränktes Surfen im Internet

Gehen Sie wie folgt vor, wenn Sie möchten, dass Ihr WorkSpaces Secure Browser-Portal sowohl auf öffentliche Internetinhalte als auch auf private VPC-Inhalte zugreifen kann:

> **Note**
>
> Wenn Sie bereits eine VPC konfiguriert haben, führen Sie die folgenden Schritte aus, um Ihrer VPC ein NAT-Gateway hinzuzufügen. Informationen zum Erstellen einer neuen VPC finden Sie unter Eine neue VPC für Amazon WorkSpaces Secure Browser erstellen.

1. Um Ihr NAT-Gateway zu erstellen, führen Sie die Schritte unter Ein NAT-Gateway erstellen aus. Stellen Sie sicher, dass dieses NAT-Gateway über öffentliche Konnektivität verfügt und sich in einem öffentlichen Subnetz in Ihrer VPC befindet.
2. Sie müssen mindestens zwei private Subnetze in verschiedenen Availability Zones angeben. Die Zuweisung Ihrer Subnetze zu verschiedenen Availability Zones trägt zu einer besseren Verfügbarkeit und Fehlertoleranz bei. Informationen zum Erstellen einer VPC mit privaten Subnetzen finden Sie unter. the section called “Schnelle VPC-Einrichtung”

   > **Note**
   >
   > Um sicherzustellen, dass jede Streaming-Instance Internetzugang hat, fügen Sie Ihrem WorkSpaces Secure Browser-Portal kein öffentliches Subnetz hinzu.

3. Aktualisieren Sie die Routing-Tabelle, die ihren privaten Subnetzen zugeordnet ist, um internetgebundenen Datenverkehr zum NAT-Gateway zu leiten. So können die Streaming-Instances innerhalb Ihrer privaten Subnetze mit dem Internet kommunizieren. Informationen dazu, wie Sie eine Routing-Tabelle einem privaten Subnetz zuordnen, finden Sie in den Schritten unter Routing-Tabellen konfigurieren.

Eingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser aktivieren

Die empfohlene Netzwerkkonfiguration eines WorkSpaces Secure Browser-Portals besteht darin, private Subnetze mit NAT-Gateway zu verwenden, sodass das Portal sowohl im öffentlichen Internet als auch in privaten Inhalten surfen kann. Weitere Informationen finden Sie unter the section called “Uneingeschränktes Surfen im Internet”. Möglicherweise müssen Sie jedoch die ausgehende Kommunikation von einem WorkSpaces Secure Browser-Portal zum Internet mithilfe eines

Webproxys steuern. Wenn Sie beispielsweise einen Webproxy als Gateway zum Internet verwenden, können Sie präventive Sicherheitskontrollen implementieren, wie z. B. die Zulassung von Domänen und Inhaltsfilterung. Dies kann auch die Bandbreitennutzung reduzieren und die Netzwerkleistung verbessern, indem häufig aufgerufene Ressourcen wie Webseiten oder Softwareupdates lokal zwischengespeichert werden. In einigen Anwendungsfällen verfügen Sie möglicherweise über private Inhalte, auf die nur über einen Webproxy zugegriffen werden kann.

Möglicherweise sind Sie bereits mit der Konfiguration von Proxyeinstellungen auf verwalteten Geräten oder mit dem Image Ihrer virtuellen Umgebungen vertraut. Dies stellt jedoch eine Herausforderung dar, wenn Sie nicht die Kontrolle über das Gerät haben (z. B. wenn Benutzer Geräte verwenden, die nicht dem Unternehmen gehören oder von diesem verwaltet werden), oder wenn Sie das Image für Ihre virtuelle Umgebung verwalten müssen. Mit WorkSpaces Secure Browser können Sie Proxyeinstellungen mithilfe der im Webbrowser integrierten Chrome-Richtlinien festlegen. Sie können dies tun, indem Sie einen HTTP-Ausgangsproxy für WorkSpaces Secure Browser einrichten.

Diese Lösung basiert auf einem empfohlenen VPC-Proxy-Setup für ausgehende Verbindungen. Die Proxy-Lösung basiert auf dem Open-Source-HTTP-Proxy Squid. Anschließend konfiguriert sie mithilfe der WorkSpaces Secure Browser-Einstellungen das WorkSpaces Secure Browser-Portal für die Verbindung mit dem Proxyendpunkt. Weitere Informationen finden Sie unter So richten Sie einen ausgehenden VPC-Proxy mit Domain-Whitelisting und Inhaltsfilterung ein.

Diese Lösung bietet Ihnen die folgenden Vorteile:

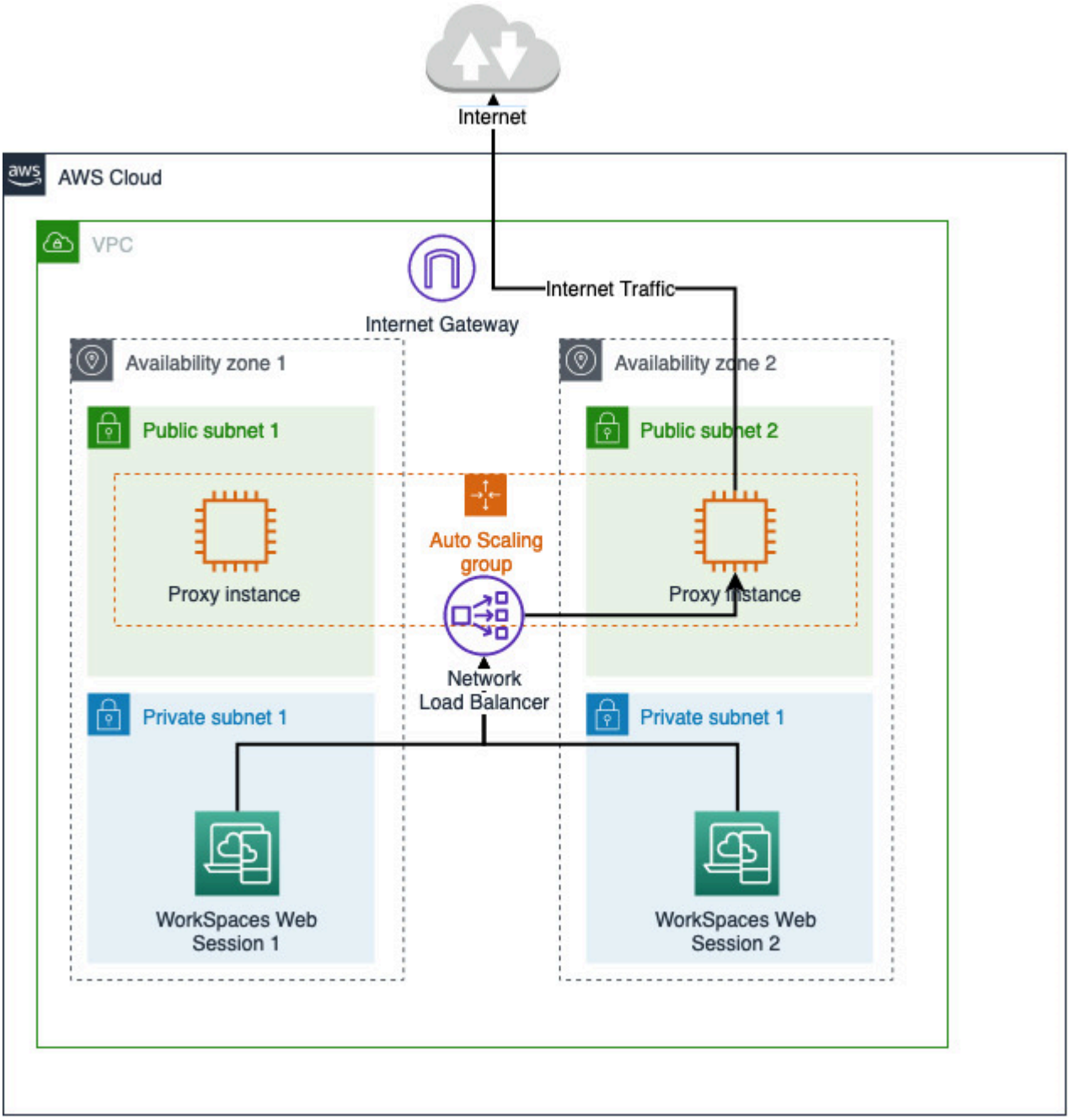
- Ein ausgehender Proxy, der eine Gruppe von auto-scaling Amazon EC2 EC2-Instances umfasst, die von einem Netzwerk-Loadbalancer gehostet werden. Proxy-Instances befinden sich in einem öffentlichen Subnetz, und jede von ihnen ist mit einer Elastic IP verbunden, sodass sie Zugriff auf das Internet haben.
- Ein WorkSpaces Secure Browser-Portal, das in privaten Subnetzen bereitgestellt wird. Sie müssen das NAT-Gateway nicht konfigurieren, um den Internetzugang zu aktivieren. Stattdessen konfigurieren Sie Ihre Browserrichtlinie so, dass der gesamte Internetverkehr über den ausgehenden Proxy läuft. Wenn Sie Ihren eigenen Proxy verwenden möchten, ist die Einrichtung des WorkSpaces Secure Browser-Portals ähnlich.

Topics

- Fehlerbehebung bei eingeschränktem Surfen im Internet für Amazon WorkSpaces Secure Browser

Architektur für eingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser

Im Folgenden finden Sie ein Beispiel für ein typisches Proxy-Setup in Ihrer VPC. Die Amazon EC2 EC2-Proxyinstanz befindet sich in öffentlichen Subnetzen und ist mit Elastic IP verknüpft, sodass sie Zugriff auf das Internet haben. Ein Network Load Balancer hostet eine Auto Scaling-Gruppe von Proxy-Instances. Dadurch wird sichergestellt, dass Proxyinstanzen automatisch skaliert werden können und der Network Load Balancer der einzige Proxy-Endpunkt ist, der von WorkSpaces Secure Browser-Sitzungen genutzt werden kann.



Voraussetzungen für eingeschränktes Surfen im Internet für Amazon WorkSpaces Secure Browser

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen:

- Sie benötigen eine bereits bereitgestellte VPC mit öffentlichen und privaten Subnetzen, die sich über mehrere Availability Zones () AZs verteilen. Weitere Informationen zur Einrichtung Ihrer VPC-Umgebung finden Sie unter Standard VPCs.

- Sie benötigen einen einzigen Proxy-Endpunkt, auf den von privaten Subnetzen aus zugegriffen werden kann, in denen WorkSpaces Secure Browser-Sitzungen gespeichert sind (z. B. der DNS-Name des Network Load Balancers). Wenn Sie Ihren vorhandenen Proxy verwenden möchten, stellen Sie sicher, dass er auch über einen einzigen Endpunkt verfügt, auf den von Ihren privaten Subnetzen aus zugegriffen werden kann.

HTTP-Proxy für ausgehenden Datenverkehr für Amazon WorkSpaces Secure Browser

Gehen Sie folgendermaßen vor, um einen HTTP-Ausgangsproxy für WorkSpaces Secure Browser einzurichten.

1. Um einen beispielhaften ausgehenden Proxy für Ihre VPC bereitzustellen, folgen Sie den Schritten unter So richten Sie einen ausgehenden VPC-Proxy mit Domain-Whitelisting und Inhaltsfilterung ein.
   a. Folgen Sie den Schritten unter „Installation (einmalige Einrichtung)“, um die Vorlage für Ihr Konto bereitzustellen. CloudFormation Stellen Sie sicher, dass Sie die richtige VPC und Subnetze als CloudFormation Vorlagenparameter auswählen.
   b. Suchen Sie nach der Bereitstellung den CloudFormation Ausgabeparameter OutboundProxyDomainund. OutboundProxyPort Dies ist der DNS-Name und -Port Ihres Proxys.
   c. Wenn Sie bereits einen eigenen Proxy haben, überspringen Sie diesen Schritt und verwenden Sie den DNS-Namen und -Port Ihres Proxys.
2. Wählen Sie in der WorkSpaces Secure Browser-Konsole Ihr Portal aus und klicken Sie dann auf Bearbeiten.
   a. Wählen Sie in den Netzwerkverbindungsdetails die VPC und die privaten Subnetze aus, die Zugriff auf den Proxy haben.
   b. Fügen Sie in den Richtlinieneinstellungen mithilfe eines JSON-Editors die folgende ProxySettings Richtlinie hinzu. Das `ProxyServer` Feld sollte den DNS-Namen und -Port Ihres Proxys enthalten. Weitere Informationen zur ProxySettings Richtlinie finden Sie unter ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
```

```
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. In Ihrer WorkSpaces Secure Browser-Sitzung sehen Sie, dass der Proxy auf Chrome angewendet ist. Chrome verwendet die Proxyeinstellungen Ihres Administrators.
4. Gehen Sie zu chrome: //policy und dann zum Chrome-Tab „Richtlinien“, um zu bestätigen, dass die Richtlinie angewendet wird.
5. Stellen Sie sicher, dass Ihre WorkSpaces Secure Browser-Sitzung erfolgreich Internetinhalte ohne NAT-Gateway durchsuchen kann. Stellen Sie in den CloudWatch Protokollen sicher, dass die Squid-Proxyzugriffsprotokolle aufgezeichnet wurden.

Fehlerbehebung bei eingeschränktem Surfen im Internet für Amazon WorkSpaces Secure Browser

Wenn Ihre WorkSpaces Secure Browser-Sitzung nach Anwendung der Chrome-Richtlinie immer noch nicht auf das Internet zugreifen kann, gehen Sie wie folgt vor, um Ihr Problem zu lösen:

- Stellen Sie sicher, dass der Proxy-Endpunkt von den privaten Subnetzen aus zugänglich ist, in denen sich Ihr WorkSpaces Secure Browser-Portal befindet. Erstellen Sie dazu eine EC2-Instance im privaten Subnetz und testen Sie die Verbindung von der privaten EC2-Instance zu Ihrem Proxy-Endpunkt.
- Stellen Sie sicher, dass der Proxy über Internetzugang verfügt.
- Stellen Sie sicher, dass die Chrome-Richtlinie korrekt ist.
  - Bestätigen Sie die folgende Formatierung für das `ProxyServer` Feld der Richtlinie:`<Proxy DNS name>:<Proxy port>`. Das Präfix sollte kein `http://` oder `https://` enthalten.
  - Navigieren Sie in der WorkSpaces Secure Browser-Sitzung in Chrome zu chrome: //policy und stellen Sie sicher, dass die ProxySettings Richtlinie erfolgreich angewendet wurde.

Anschlüsse für Internetkonnektivität für Amazon WorkSpaces Secure Browser

Jede WorkSpaces Secure Browser-Streaming-Instance verfügt über eine Kundennetzwerkschnittstelle, die Konnektivität zu den Ressourcen in Ihrer VPC sowie zum Internet bietet, wenn private Subnetze mit NAT-Gateway eingerichtet sind.

Für die Internetkonnektivität müssen die folgenden Ports für alle Ziele geöffnet sein. Wenn Sie eine veränderte oder benutzerdefinierte Sicherheitsgruppe verwenden, müssen Sie die erforderlichen Regeln manuell hinzufügen. Weitere Informationen finden Sie unter Regeln zu Sicherheitsgruppen.

> **Note**
>
> Dies gilt für ausgehenden Datenverkehr.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8.433

Bewährte VPC-Methoden für WorkSpaces Secure Browser

Die folgenden Empfehlungen können Ihnen dabei helfen, Ihre VPC effektiver und sicherer zu konfigurieren.

VPC-Gesamtkonfiguration

- Stellen Sie sicher, dass Ihre VPC-Konfiguration Ihre Skalierungsanforderungen erfüllen kann.
- Stellen Sie sicher, dass Ihre WorkSpaces Secure Browser-Dienstkontingente (auch als Limits bezeichnet) ausreichend sind, um Ihren voraussichtlichen Bedarf zu decken. Um eine Erhöhung des Kontingents zu beantragen, können Sie die Service Quotas Quotas-Konsole unter verwenden https://console.aws.amazon.com/servicequotas/. Informationen zu den Standardkontingenten für WorkSpaces Secure Browser finden Sie unterthe section called “Verwaltung von Servicekontingenten”.
- Wenn Sie planen, Ihren Streaming-Sitzungen Zugang zum Internet zu gewähren, empfehlen wir Ihnen, eine VPC mit einem NAT-Gateway in einem öffentlichen Subnetz zu konfigurieren.

Elastic-Network-Schnittstellen

- Jede WorkSpaces Secure Browser-Sitzung benötigt während der Streaming-Dauer eine eigene elastic network interface. WorkSpaces Secure Browser erstellt so viele elastische Netzwerkschnittstellen (ENIs) wie die maximal gewünschte Kapazität Ihrer Flotte entspricht. Standardmäßig ist das Limit ENIs für jede Region 5000. Weitere Informationen finden Sie unter Netzwerkschnittstellen.

Wenn Sie Kapazität für sehr große Bereitstellungen planen, z. B. Tausende gleichzeitiger Streaming-Sitzungen, sollten Sie die Anzahl ENIs berücksichtigen, die für Ihre Spitzennutzung erforderlich sein könnte. Wir empfehlen, dass Sie Ihr ENI-Limit auf oder über dem für Ihr Webportal konfigurierten maximalen Limit für die gleichzeitige Nutzung halten.

Subnets

- Denken Sie bei der Entwicklung Ihres Plans zur Erhöhung der Benutzerzahl daran, dass für jede WorkSpaces Secure Browser-Sitzung eine eindeutige Client-IP-Adresse aus Ihren konfigurierten Subnetzen erforderlich ist. Daher bestimmt die Größe des Client-IP-Adressraums, der in Ihren Subnetzen konfiguriert ist, die Anzahl der Benutzer, die gleichzeitig streamen können.
- Wir empfehlen, jedes Subnetz mit einer Subnetzmaste zu konfigurieren, die genügend Client-IP-Adressen für die maximale Anzahl der erwarteten gleichzeitigen Benutzer ermöglicht. Überlegen Sie außerdem, ob Sie im Hinblick auf das erwartete Wachstum zusätzliche IP-Adressen hinzufügen. Weitere Informationen finden Sie unter VPC und Subnet-Sizing für. IPv4
- Aus Gründen der Verfügbarkeit und Skalierung empfehlen wir, in jeder einzelnen Availability Zone, die WorkSpaces Secure Browser in Ihrer gewünschten Region unterstützt, ein Subnetz zu konfigurieren. Weitere Informationen finden Sie unter the section called “Eine neue VPC erstellen”.
- Zudem muss sichergestellt sein, dass auf die für Ihre Webanwendungen erforderlichen Netzwerkressourcen über Ihre Subnetze zugegriffen werden kann.

Sicherheitsgruppen

- Verwenden Sie Sicherheitsgruppen, um zusätzliche Zugriffssteuerung für Ihre VPC bereitzustellen.

  Mit Sicherheitsgruppen, die zu Ihrer VPC gehören, können Sie den Netzwerkverkehr zwischen WorkSpaces Secure Browser-Streaming-Instances und Netzwerkressourcen steuern, die von Webanwendungen benötigt werden. Stellen Sie sicher, dass die Sicherheitsgruppen Zugriff auf die Netzwerkressourcen bieten, die von Ihren Webanwendungen benötigt werden.

Unterstützte Availability Zones für Amazon WorkSpaces Secure Browser

Wenn Sie eine Virtual Private Cloud (VPC) für die Verwendung mit WorkSpaces Secure Browser erstellen, müssen sich die Subnetze Ihrer VPC in verschiedenen Availability Zones in der Region befinden, in der Sie Secure Browser starten. WorkSpaces Availability Zones sind unabhängige Standorte, die so aufgebaut sind, dass sie von Fehlern in anderen Availability Zones nicht

betroffen sind. Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern eines einzelnen Standorts schützen. Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen. Wir empfehlen, für jede unterstützte AZ in der gewünschten Region ein Subnetz zu konfigurieren, um maximale Ausfallsicherheit zu erzielen

Eine Availability Zone wird durch einen Regionscode gefolgt von einem Buchstaben als Bezeichner angegeben, z. B. `us-east-1a`. Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes AWS -Konto zu. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS -Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS -Konto.

Um die Availability Zones kontenübergreifend zu koordinieren, müssen Sie die AZ-ID verwenden, die eine eindeutige und konsistente Kennung für eine Availability Zone ist. Dies `use1-az2` ist beispielsweise eine AZ-ID für die `us-east-1` Region, die in jedem Konto denselben Standort hat. AWS

Wenn Sie AZ IDs anzeigen, können Sie den Standort der Ressourcen in einem Konto im Verhältnis zu den Ressourcen in einem anderen Konto bestimmen. Wenn Sie beispielsweise ein Subnetz in der Availability Zone mit der AZ-ID `use1-az2` mit einem anderen Konto teilen, steht dieses Subnetz dem Konto in der Availability Zone zur Verfügung, dessen AZ-ID ebenfalls `use1-az2` ist. Die AZ-ID für jede VPC und jedes Subnetz wird in der Amazon VPC-Konsole angezeigt.

WorkSpaces Secure Browser ist in einer Untergruppe der Availability Zones für jede unterstützte Region verfügbar. In der folgenden Tabelle sind die AZs aufgeführt IDs , die Sie für jede Region verwenden können. Informationen zur Zuordnung von AZ IDs zu Availability Zones in Ihrem Konto finden Sie unter AZ IDs for Your Resources im AWS RAM Benutzerhandbuch.

Name der Region	Regionscode	Unterstützt A-Z IDs
USA Ost (Nord-Virginia)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
USA West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asien-Pazifik (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az3`

Name der Region	Regionscode	Unterstützt A-Z IDs
Asien-Pazifik (Singapur)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Asien-Pazifik (Sydney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Asien-Pazifik (Tokio)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Canada (Central)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
Europe (Frankfurt)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
Europa (Irland)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (London)	eu-west-2	euw2-az1, euw2-az2

Weitere Informationen zu Availability Zones und AZ IDs finden Sie unter Regionen, Availability Zones und Local Zones im Amazon EC2 EC2-Benutzerhandbuch.

Benutzerverbindungen für Amazon WorkSpaces Secure Browser aktivieren

WorkSpaces Secure Browser ist so konfiguriert, dass Streaming-Verbindungen über das öffentliche Internet weitergeleitet werden. Eine Internetverbindung ist erforderlich, um Benutzer zu authentifizieren und die Webressourcen bereitzustellen, die WorkSpaces Secure Browser zum Funktionieren benötigt. Sie müssen die in Zulässige Domains für Amazon WorkSpaces Secure Browser aufgelisteten Domains zulassen, um diesen Datenverkehr zuzulassen.

Die folgenden Themen enthalten Informationen darüber, wie Benutzerverbindungen mit WorkSpaces Secure Browser aktiviert werden.

Topics

- Anforderungen an IP-Adresse und Port für Amazon WorkSpaces Secure Browser

- Zulässige Domains für Amazon WorkSpaces Secure Browser

Anforderungen an IP-Adresse und Port für Amazon WorkSpaces Secure Browser

Für den Zugriff auf WorkSpaces Secure Browser-Instances benötigen Benutzergeräte ausgehenden Zugriff auf die folgenden Ports:

- Port 443 (TCP)
  - Port 443 wird für die HTTPS-Kommunikation zwischen -Benutzergeräten und Streaming-Instances verwendet, wenn die Internet-Endpunkte verwendet werden. Wenn Endbenutzer während Streaming-Sitzungen im Internet surfen, wählt der Web-Browser normalerweise einen Quell-Port im höheren Bereich für das Streamen von Datenverkehr aus. Sie müssen sicherstellen, dass zu diesem Port zurückfließender Datenverkehr zulässig ist.
  - Dieser Port muss für die erforderlichen Domains geöffnet sein, die unter Zulässige Domains für Amazon WorkSpaces Secure Browser aufgeführt sind.
  - AWS veröffentlicht seine aktuellen IP-Adressbereiche, einschließlich der Bereiche, in die das Session Gateway und die CloudFront Domänen möglicherweise aufgelöst werden, im JSON-Format. Weitere Informationen zum Herunterladen der JSON-Datei und zur Anzeige der aktuellen Bereiche finden Sie unter AWS -IP-Adressbereiche. Oder, wenn Sie verwenden AWS Tools for Windows PowerShell, können Sie mit dem Get-AWSPublicIpAddressRange PowerShell Befehl auf dieselben Informationen zugreifen. Weitere Informationen finden Sie unter Abfragen der öffentlichen IP-Adressbereiche für AWS.
- (Optional) Port 53 (UDP)
  - Port 53 wird für die Kommunikation zwischen den Benutzergeräten der und Ihren DNS-Servern verwendet.
  - Dieser Port ist optional, wenn Sie keine DNS-Server für die Domänennamenauflösung verwenden.
  - Der Port muss für die IP-Adressen Ihrer DNS-Server geöffnet sein, damit öffentliche Domain-Namen aufgelöst werden können.

Zulässige Domains für Amazon WorkSpaces Secure Browser

Damit Benutzer über ihren lokalen Browser auf Webportale zugreifen können, müssen Sie die folgenden Domänen zur Zulassungsliste des Netzwerks hinzufügen, von dem aus der Benutzer versucht, auf den Service zuzugreifen.

Ersetzen Sie den Wert in der folgenden Tabelle *{region}* durch den Code der Region, die das Webportal betreibt. Zum Beispiel s3. *{region}*.amazonaws.com sollte s3.eu-west-1.amazonaws.com sein für ein Webportal in der Region Europa (Irland). Eine Liste der Regionscodes finden Sie unter Amazon WorkSpaces Secure Browser Endpoints and Quotas.

Kategorie	Domain oder IP-Adresse
WorkSpaces Sichere Browser-Streaming-Assets	s3. *{region}*.amazonaws.com s3.amazonaws.com Appstream 2. *{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Statische Ressourcen im sicheren Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Sichere Browser-Authentifizierung	*.auth. *{region}*.amazoncognito.com kognitive Identität. *{region}*.amazonaws.com Cognito-IDP. *{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Metriken und Berichte für sichere Browser	*.execute-api. *{region}*.amazonaws.com unagi-na.amazon.com

Abhängig von Ihrem konfigurierten Identitätsanbieter müssen Sie möglicherweise auch zusätzlicher Domains auf die Zulassungsliste setzen. Lesen Sie in der Dokumentation Ihres IdP nach, welche Domains Sie zulassen müssen, damit WorkSpaces Secure Browser diesen Anbieter verwenden kann. Wenn Sie IAM Identity Center verwenden, finden Sie weitere Informationen unter Voraussetzungen für IAM Identity Center.

Erste Schritte mit Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um ein WorkSpaces Secure Browser-Webportal zu erstellen und Benutzern den Zugriff auf interne und SaaS-Websites von ihren vorhandenen Browsern aus zu ermöglichen. Sie können in jeder unterstützten Region ein Webportal pro Konto erstellen.

> **Note**
>
> Um eine Erhöhung des Limits für mehr als ein Portal zu beantragen, wenden Sie sich bitte mit Ihrer AWS-Konto ID, der Anzahl der anzufordernden Portale und an den Support AWS-Region.

Dieser Vorgang dauert mit dem Assistenten zur Erstellung eines Webportals in der Regel fünf Minuten und weitere 15 Minuten, bis das Portal aktiv wird.

Mit der Einrichtung eines Webportals sind keine Kosten verbunden. WorkSpaces Secure Browser bietet pay-as-you-go Preise, einschließlich eines niedrigen monatlichen Preises für Benutzer, die den Service aktiv nutzen. Es gibt keine Vorabkosten, Lizenzen oder langfristige Verpflichtungen.

> **Important**
>
> Bevor Sie beginnen, müssen Sie die erforderlichen Voraussetzungen für ein Webportal erfüllen. Weitere Informationen über Webportal-Voraussetzungen finden Sie unter Amazon WorkSpaces Secure Browser einrichten.

Topics

Ein Webportal für Amazon WorkSpaces Secure Browser erstellen

Führen Sie zur Erstellung eines Webportals diese Schritte aus.

Topics

Netzwerkeinstellungen für Amazon WorkSpaces Secure Browser konfigurieren

Gehen Sie wie folgt vor, um die Netzwerkeinstellungen für WorkSpaces Secure Browser zu konfigurieren.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole zu https://console.aws.amazon.com/workspaces-web/Hause.
2. Wählen Sie WorkSpaces Sicherer Browser, dann Webportale und dann Webportal erstellen aus.
3. Führen Sie auf der Seite Schritt 1: Netzwerkverbindung festlegen die folgenden Schritte aus, um eine Verbindung zwischen Ihrer VPC und Ihrem Webportal herzustellen und Ihre VPC und Subnetze zu konfigurieren.

    1. Wählen Sie für Netzwerkdetails eine VPC mit einer Verbindung zu den Inhalten aus, auf die Ihre Benutzer mit WorkSpaces Secure Browser zugreifen sollen.
    2. Wählen Sie bis zu drei private Subnetze aus, die die folgenden Anforderungen erfüllen. Weitere Informationen finden Sie unter Netzwerke für Amazon WorkSpaces Secure Browser.
        - Sie müssen für die Erstellung eines Portals mindestens zwei private Subnetze auswählen.
        - Um eine hohe Verfügbarkeit für Ihr Webportal zu gewährleisten, empfehlen wir Ihnen, die maximale Anzahl von privaten Subnetzen in eindeutigen Availability Zones für Ihre VPC bereitzustellen.
    3. Wählen Sie eine Sicherheitsgruppe aus.

Konfiguration der Portaleinstellungen für Amazon WorkSpaces Secure Browser

Führen Sie auf der Seite Schritt 2: Webportaleinstellungen konfigurieren die folgenden Schritte aus, um das Surferlebnis Ihrer Benutzer beim Starten einer Sitzung anzupassen.

1. Geben Sie unter Webportaldetails bei Anzeigename einen identifizierbaren Namen für Ihr Webportal ein.
2. Wählen Sie unter Instanztyp den Instanztyp für Ihr Webportal aus dem Drop-down-Menü aus. Geben Sie dann Ihre maximale Anzahl gleichzeitiger Benutzer für das Webportal ein. Weitere Informationen finden Sie unter the section called “Verwaltung von Servicekontingenten”.

   > **Note**
   >
   > Wenn Sie einen neuen Instanztyp auswählen, ändern sich die Kosten für jeden monatlich aktiven Benutzer. Weitere Informationen finden Sie unter Amazon WorkSpaces Secure Browser Pricing.

3. Unter Benutzerdefinierte Domain können Sie eine benutzerdefinierte Domain für Ihr Portal konfigurieren, um den Zugriff über Ihren eigenen Domainnamen statt über den Standard-Portal-Endpunkt zu ermöglichen. Weitere Informationen finden Sie unter the section called “Benutzerdefinierte Domain”. Dies ist optional.
4. Unter Session Logger können Sie einen S3-Bucket zum Speichern von Sitzungsprotokolldateien angeben. Weitere Informationen finden Sie unter the section called “Session Logger einrichten”. Das ist optional.
5. Wählen Sie unter Benutzerzugriffsprotokollierung für Kinesis-Stream-ID den Amazon Kinesis Kinesis-Datenstream aus, an den Sie Protokolldateien senden möchten. Weitere Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”. Dies ist optional.
6. Wählen Sie unter IP-Zugriffskontrolle aus, ob der Zugriff auf vertrauenswürdige Netzwerke beschränkt werden soll. Weitere Informationen finden Sie unter the section called “Verwaltung von IP-Zugriffskontrollen”. Das ist optional.
7. Unter Datenschutzeinstellungen können Sie Richtlinien für WorkSpaces Secure Browser erstellen, um vertrauliche Informationen zu unkenntlich zu machen. Weitere Informationen finden Sie unter the section called “Datenschutzeinstellungen”. Dies ist optional.
8. Unter URL-Filterung können Sie angeben, welche URLs Endbenutzer auf bestimmte URLs Kategorien oder Domain-Kategorien zugreifen oder diese blockieren dürfen, um den Zugriff einzuschränken. Weitere Informationen finden Sie unter the section called “Filterung von Webinhalten”. Das ist optional.

1. Um das Surfen in Sitzungen auf einige ausgewählte Domains zu beschränken, aktivieren Sie den Schalter Alle blockieren URLs und klicken Sie auf URL hinzufügen, um die Liste der Endbenutzer anzuzeigen, auf die URLs Ihre Endbenutzer zugreifen dürfen.
2. Um eine Liste der URLs zu blockierenden Domains für Endbenutzer zu erstellen, klicken Sie auf URL hinzufügen, um die URLs zu blockierende Person aufzulisten, oder klicken Sie auf Kategorien hinzufügen, um Kategorien von blockierten Domains auszuwählen (z. B. Soziale Netzwerke).

9. Unter Richtlinieneinstellungen können Sie mithilfe der Chrome-Richtlinien, die für die neueste stabile Version des Webportals verfügbar sind, jede beliebige Browserrichtlinie festlegen. Weitere Informationen finden Sie unter the section called “Verwaltung der Browserrichtlinie”. Dies ist optional.

   1. Sie können schnell einige der gängigsten Richtlinien im Visual Editor auswählen
      - Geben Sie unter Start-URL — optional eine Domain ein, die als Startseite verwendet werden soll, wenn Benutzer ihren Browser starten. Es muss für Ihre VPC eine stabile Verbindung mit dieser URL hergestellt sein.
      - Aktivieren oder deaktivieren Sie Privates Browsing und Löschen des Verlaufs, um dieses Feature während einer Benutzersitzung ein- oder auszuschalten

        > **Note**
        >
        > URLs Besucher, die beim privaten Surfen besucht wurden oder bevor ein Benutzer seinen Browserverlauf löscht, können nicht in der Benutzerzugriffsprotokollierung aufgezeichnet werden. Weitere Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”.

      - Geben Sie für Browser-Lesezeichen — optional — den Anzeigenamen, die Domain und den Ordner für alle Lesezeichen ein, die Ihren Benutzern in ihrem Browser angezeigt werden sollen. Wählen Sie dann Lesezeichen hinzufügen aus.

        > **Note**
        >
        > Domain ist ein Pflichtfeld für Browserlesezeichen.
        > In Chrome finden Nutzer verwaltete Lesezeichen im Ordner Verwaltete Lesezeichen auf der Lesezeichen-Symbolleiste.

2. Sie können Richtlinien auch direkt hinzufügen oder bearbeiten, indem Sie den JSON-Editor anstelle des visuellen Editors verwenden. Das spezifische Format einer Richtlinie finden Sie in der Chrome Enterprise-Richtlinienliste.
3. Sie können auch die in Ihrer Organisation verwendeten Chrome-Richtlinien importieren, indem Sie eine JSON-Datei in das Webportal hochladen. Einzelheiten finden Sie unter the section called “Tutorial: Eine benutzerdefinierte Browserrichtlinie einrichten”

   Wenn Sie eine Richtliniendatei hochladen, können Sie die verfügbaren Richtlinien in der Datei in der Konsole sehen. Sie können jedoch nicht alle Richtlinien im visuellen Editor bearbeiten. In der Konsole werden unter Zusätzliche JSON-Richtlinien Richtlinien in Ihrer JSON-Datei aufgeführt, die Sie nicht mit dem visuellen Editor bearbeiten können. Um Änderungen an diesen Richtlinien vorzunehmen, müssen Sie sie manuell bearbeiten.

10. Fügen Sie Ihrem Portal Tags hinzu. Sie können Tags verwenden, um nach Ihren AWS Ressourcen zu suchen oder diese zu filtern. Tags bestehen aus einem Schlüssel und einem optionalen Wert und sind mit Ihrer Portalressource verknüpft. Das ist optional.
11. Wählen Sie Next (Weiter), um fortzufahren.

Benutzereinstellungen für Amazon WorkSpaces Secure Browser konfigurieren

Führen Sie auf der Seite Schritt 3: Benutzereinstellungen auswählen die folgenden Schritte aus, um auszuwählen, auf welche Features Ihre Benutzer während ihrer Sitzung über die obere Navigationsleiste zugreifen können. Wählen Sie dann Weiter aus:

1. Unter Anpassung des Brandings können Sie die Anmelde- und Ladebildschirme, die Ihren Endbenutzern angezeigt werden, anpassen, indem Sie visuelle Elemente, Textinhalte und Nutzungsbedingungen ändern. Weitere Informationen finden Sie unter the section called “Anpassung des Brandings”. Das ist optional.
2. Wählen Sie unter Berechtigungen aus, ob die Erweiterung für Single Sign-On aktiviert werden soll. Weitere Informationen finden Sie unter the section called “Verwaltung der Single Sign-On-Erweiterung”.
3. Wählen Sie unter Benutzern erlauben, von ihrem Webportal aus auf einem lokalen Gerät zu drucken, die Option Erlaubt oder Nicht erlaubt aus.

4. Wählen Sie für Benutzern erlauben, Deeplinks zu ihrem Webportal zu erstellen, die Option Erlaubt oder Nicht zulässig aus. Weitere Informationen zu Deep-Links finden Sie unter. the section called “Deep-Links”
5. Wählen Sie für Benutzern erlauben, die lokale Authentifizierung in ihrer Portalsitzung zu verwenden, die Option Erlaubt oder Nicht zugelassen aus. Weitere Informationen zur Webauthentifizierung finden Sie unterthe section called “Umleitung der Webauthentifizierung”.
6. Wählen Sie unter Steuerelemente in der Werkzeugleiste unter Funktionen die gewünschten Einstellungen aus.
7. Unter Einstellungen können Sie die Präsentationsansicht der Werkzeugleiste zu Beginn der Sitzung verwalten, einschließlich des Status der Werkzeugleiste (angedockt oder getrennt), des Designs (dunkler oder heller Modus), der Sichtbarkeit der Symbole und der maximalen Bildschirmauflösung für die Sitzung. Lassen Sie diese Einstellungen unkonfiguriert, um Endbenutzern die volle Kontrolle über diese Optionen zu gewähren. Weitere Informationen finden Sie unter the section called “Steuerelemente der Symbolleiste”.
8. Geben Sie für Sitzungs-Timeouts Folgendes an:

   - Wählen Sie für Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) die Zeitspanne aus, für die eine Streaming-Sitzung aktiv bleiben kann, nachdem der Benutzer die Verbindung getrennt hat. Wenn Benutzer nach einer Verbindungstrennung oder Netzwerkunterbrechung innerhalb dieses Zeitraums erneut eine Verbindung herstellen möchten, werden sie wieder mit der vorherigen Sitzung verbunden. Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance verbunden.

     Wenn ein Benutzer die Sitzung beendet, gilt die Zeitüberschreitung beim Trennen nicht. Stattdessen wird der Benutzer aufgefordert, alle geöffneten Dokumente zu speichern, und wird dann sofort von der Streaming-Instance getrennt. Die vom Benutzer verwendete Instance wird dann beendet.
   - Wählen Sie für Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) die Zeitspanne aus, für die Benutzer im Leerlauf (inaktiv) verbleiben können, bevor sie von ihrer Streaming-Sitzung getrennt werden und bevor das Zeitintervall unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) beginnt. Benutzer werden benachrichtigt, bevor sie aufgrund von Inaktivität getrennt werden. Wenn sie versuchen, vor Ablauf des unter Disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung in Minuten) angegebenen Zeitintervalls wieder eine Verbindung mit der Streaming-Sitzung herzustellen, werden sie mit ihrer vorherigen Sitzung verbunden. Andernfalls werden sie mit einer neuen Sitzung mit einer neuen Streaming-Instance

verbunden. Die Einstellung wird durch den Wert „0“ deaktiviert. Wenn dieser Wert deaktiviert ist, werden Benutzer nicht aufgrund von Inaktivität getrennt.

> **Note**
>
> Benutzer gelten als inaktiv, wenn sie während ihrer Streaming-Sitzung keine Tastatur- oder Mauseingaben mehr vornehmen. Datei-Uploads und -Downloads, Audio-Eingabe, Audio-Ausgabe und Pixeländerungen gelten nicht als Benutzeraktivitäten. Wenn Benutzer nach Ablauf des Zeitintervalls unter Idle disconnect timeout in minutes (Zeitlimit für die Verbindungstrennung bei Leerlauf in Minuten) weiterhin inaktiv sind, wird ihre Verbindung getrennt.

Konfiguration Ihres Identitätsanbieters für Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um Ihren Identity Provider (IdP) zu konfigurieren.

Topics

Auswahl des Identitätsanbietertyps für Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser bietet zwei Authentifizierungstypen: Standard und AWS IAM Identity Center. Sie wählen den Authentifizierungstyp, der für Ihr Portal verwendet werden soll, auf der Seite Identitätsanbieter konfigurieren aus.

- Für Standard (Standardoption) verbinden Sie Ihren SAML 2.0-Identitätsanbieter eines Drittanbieters (wie Okta oder Ping) direkt mit Ihrem Portal. Weitere Informationen finden Sie unter the section called “Standardauthentifizierungstyp”. Der Standardtyp unterstützt sowohl SP-initiierte als auch IDP-initiierte Authentifizierungsabläufe.
- Für IAM Identity Center (erweiterte Option) verbinden Sie das IAM Identity Center mit Ihrem Portal. Um diesen Authentifizierungstyp verwenden zu können, müssen sich Ihr IAM Identity Center und Ihr WorkSpaces Secure Browser-Portal beide im selben System befinden. AWS-Region Weitere Informationen finden Sie unter the section called “Authentifizierungstyp für IAM Identity Center”.

Topics

Konfiguration des Standardauthentifizierungstyps für Amazon WorkSpaces Secure Browser

Der Standardauthentifizierungstyp ist der Standardauthentifizierungstyp. Es kann vom Service Provider initiierte (SP-initiierte) und vom Identitätsanbieter initiierte (IdP-initiierte) Anmeldeabläufe mit Ihrem SAML 2.0-kompatiblen IdP unterstützen. Gehen Sie wie folgt vor, um den Standardauthentifizierungstyp zu konfigurieren, um Ihren SAML 2.0-IdP eines Drittanbieters (wie Okta oder Ping) direkt mit Ihrem Portal zu verbinden.

Topics

Konfiguration Ihres Identitätsanbieters im Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um Ihren Identitätsanbieter zu konfigurieren:

1. Wählen Sie auf der Seite Identitätsanbieter konfigurieren des Erstellungsassistenten die Option Standard aus.
2. Wählen Sie Weiter mit Standard-IdP.
3. Laden Sie die SP-Metadatendatei herunter und lassen Sie die Registerkarte für einzelne Metadatenwerte geöffnet.
   - Wenn die SP-Metadatendatei verfügbar ist, wählen Sie Metadatendatei herunterladen, um das Service Provider (SP) -Metadatendokument herunterzuladen, und laden Sie die Service Provider-Metadatendatei im nächsten Schritt auf Ihren IdP hoch. Ohne diese Option können sich Benutzer nicht anmelden.
   - Wenn Ihr Anbieter keine SP-Metadatendateien hochlädt, geben Sie die Metadatenwerte manuell ein.

4. Wählen Sie unter SAML-Anmeldetyp auswählen zwischen SP-initiierten und IDP-initiierten SAML-Assertionen oder nur SP-initiierten SAML-Assertionen.
   - Durch SP-initiierte und IdP-initiierte SAML-Assertionen kann Ihr Portal beide Arten von Anmeldeabläufen unterstützen. Portale, die IDP-initiierte Flows unterstützen, ermöglichen es Ihnen, SAML-Assertions dem Service Identity Federation-Endpunkt zu präsentieren, ohne dass Benutzer eine Sitzung starten müssen, indem sie die Portal-URL aufrufen.
     - Wählen Sie diese Option, damit das Portal unaufgefordert vom IDP initiierte SAML-Assertions akzeptieren kann.
     - Für diese Option muss ein Standard-Relay-Status in Ihrem SAML 2.0-Identity Provider konfiguriert sein. Der Relay-State-Parameter für Ihr Portal befindet sich in der Konsole unter IdP-initiierte SAML-Anmeldung, oder Sie können ihn aus der SP-Metadatendatei unter kopieren. `<md:IdPInitRelayState>`
     - Hinweis
       - Das Folgende ist das Format des Relay-Status:. `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=ExIdentity-Provider`
       - Wenn Sie den Wert aus der SP-Metadatendatei kopieren und einfügen, stellen Sie sicher, dass Sie `&` zu wechseln&. `&`ist ein XML-Escape-Zeichen.
   - Wählen Sie nur SP-initiierte SAML-Assertionen für das Portal aus, um nur SP-initiierte Anmeldeabläufe zu unterstützen. Diese Option lehnt unaufgeforderte SAML-Assertions aus vom IDP initiierten Anmeldeabläufen ab.

   > **Note**
   >
   > Einige Drittanbieter IdPs ermöglichen es Ihnen, eine benutzerdefinierte SAML-Anwendung zu erstellen, die von IdP initiierte Authentifizierungserlebnisse mithilfe von SP-initiierten Abläufen bereitstellen kann. Ein Beispiel finden Sie unter Eine Okta-Lesezeichenanwendung hinzufügen.

5. Wählen Sie aus, ob Sie das Signieren von SAML-Anfragen an diesen Anbieter aktivieren möchten. Durch die SP-initiierte Authentifizierung kann Ihr IdP überprüfen, ob die Authentifizierungsanfrage vom Portal stammt, wodurch verhindert wird, dass andere Anfragen von Drittanbietern akzeptiert werden.

a. Laden Sie das Signaturzertifikat herunter und laden Sie es auf Ihren IdP hoch. Das gleiche Signaturzertifikat kann für die einmalige Abmeldung verwendet werden.

b. Aktivieren Sie die signierte Anfrage in Ihrem IdP. Der Name kann je nach IdP unterschiedlich sein.

> **Note**
>
> RSA- SHA256 ist der einzige unterstützte Algorithmus zum Signieren von Anfragen und Standardanfragen.

6. Wählen Sie aus, ob Sie die Option Verschlüsselte SAML-Assertionen erforderlich aktivieren möchten. Auf diese Weise können Sie die SAML-Assertion verschlüsseln, die von Ihrem IdP stammt. Es kann verhindern, dass Daten in SAML-Assertionen zwischen dem IdP und dem Secure Browser abgefangen werden. WorkSpaces

> **Note**
>
> Das Verschlüsselungszertifikat ist in diesem Schritt nicht verfügbar. Es wird nach dem Start Ihres Portals erstellt. Nachdem Sie das Portal gestartet haben, laden Sie das Verschlüsselungszertifikat herunter und laden Sie es auf Ihren IdP hoch. Aktivieren Sie dann die Assertion-Verschlüsselung in Ihrem IdP (der Name kann je nach IdP unterschiedlich sein).

7. Wählen Sie aus, ob Sie Single Logout aktivieren möchten. Single Logout ermöglicht es Ihren Endbenutzern, sich mit einer einzigen Aktion sowohl von ihrer IdP- als auch von ihrer WorkSpaces Secure Browser-Sitzung abzumelden.

   a. Laden Sie das Signaturzertifikat vom WorkSpaces Secure Browser herunter und laden Sie es auf Ihren IdP hoch. Dies ist dasselbe Signaturzertifikat, das im vorherigen Schritt für das Signieren von Anfragen verwendet wurde.

   b. Für die Verwendung von Single Logout müssen Sie eine Single Logout-URL in Ihrem SAML 2.0-Identitätsanbieter konfigurieren. Sie finden die Single Logout-URL für Ihr Portal in der Konsole unter Details zum Dienstanbieter (SP) — Individuelle Metadatenwerte anzeigen oder in der SP-Metadatendatei unter. `<md:SingleLogoutService>`

   c. Aktivieren Sie Single Logout in Ihrem IdP. Der Name kann je nach IdP unterschiedlich sein.

Konfiguration Ihres IdP auf Ihrem eigenen IdP

Gehen Sie wie folgt vor, um Ihren IdP auf Ihrem eigenen IdP zu konfigurieren.

1. Öffnen Sie eine neue Registerkarte in Ihrem Browser.
2. Fügen Sie Ihre Portal-Metadaten zu Ihrem SAML-IdP hinzu.

   Laden Sie entweder das SP-Metadatendokument, das Sie im vorherigen Schritt heruntergeladen haben, auf Ihren IdP hoch, oder kopieren Sie die Metadatenwerte und fügen Sie sie in die richtigen Felder in Ihrem IdP ein. Einige Anbieter erlauben das Hochladen von Dateien nicht.

   Die Einzelheiten dieses Vorgangs können je nach Anbieter variieren. In der Dokumentation Ihres Anbieters finden Sie Hilfe the section called “Hinweise für bestimmte IdPs” zum Hinzufügen der Portaldetails zu Ihrer IdP-Konfiguration.
3. Bestätigen Sie die NameID für Ihre SAML-Assertion.

   Stellen Sie sicher, dass Ihr SAML-IdP NameID in der SAML-Assertion mit dem Benutzer-E-Mail-Feld füllt. NameID und Benutzer-E-Mail werden verwendet, um Ihren SAML-Verbundbenutzer im Portal eindeutig zu identifizieren. Verwenden Sie das persistente SAML-Namen-ID-Format.
4. Optional: Konfigurieren Sie den Relay-Status für die IDP-initiierte Authentifizierung.

   Wenn Sie im vorherigen Schritt SP-initiierte und IdP-initiierte SAML-Assertionen akzeptieren ausgewählt haben, folgen Sie den Schritten in Schritt 2 von, the section called “IdP-Konfiguration im WorkSpaces Secure Browser” um den Standard-Relay-Status für Ihre IdP-Anwendung festzulegen.
5. Optional: Konfigurieren Sie das Signieren von Anfragen. Wenn Sie im vorherigen Schritt SAML-Anfragen an diesen Anbieter signieren ausgewählt haben, folgen Sie den Schritten in Schritt 3 von, the section called “IdP-Konfiguration im WorkSpaces Secure Browser” um das Signaturzertifikat auf Ihren IdP hochzuladen und das Signieren von Anfragen zu aktivieren. Einige, IdPs wie Okta, erfordern möglicherweise, dass Ihre NameID zum Typ „persistent“ gehört, um die Anforderungssignierung verwenden zu können. Stellen Sie sicher, dass Sie Ihre NameID für Ihre SAML-Assertion bestätigen, indem Sie die obigen Schritte ausführen.
6. Optional: Konfigurieren Sie die Assertion-Verschlüsselung. Wenn Sie Verschlüsselte SAML-Assertionen von diesem Anbieter erfordern ausgewählt haben, warten Sie, bis die Portalerstellung abgeschlossen ist, und folgen Sie dann Schritt 4 unter „Metadaten hochladen“ unten, um das Verschlüsselungszertifikat auf Ihren IdP hochzuladen und die Assertionsverschlüsselung zu aktivieren.

7. Optional: Konfigurieren Sie Single Logout. Wenn Sie Single Logout ausgewählt haben, folgen Sie den Schritten in Schritt 5 von, the section called “IdP-Konfiguration im WorkSpaces Secure Browser” um das Signaturzertifikat auf Ihren IdP hochzuladen, geben Sie Single Logout URL ein und aktivieren Sie Single Logout.
8. Gewähren Sie Ihren Benutzern in Ihrem IdP Zugriff auf die Verwendung von WorkSpaces Secure Browser.
9. Laden Sie eine Metadaten-Austauschdatei von Ihrem Identitätsanbieter herunter. Im nächsten Schritt laden Sie diese Metadaten in den WorkSpaces Secure Browser hoch.

Abschluss der IdP-Konfiguration im Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um die IdP-Konfiguration im WorkSpaces Secure Browser abzuschließen.

1. Kehren Sie zur WorkSpaces Secure Browser-Konsole zurück. Laden Sie auf der Seite Identitätsanbieter konfigurieren des Erstellungsassistenten unter IdP-Metadaten entweder eine Metadatendatei hoch oder geben Sie eine Metadaten-URL von Ihrem IdP ein. Das Portal verwendet diese Metadaten von Ihrem IdP, um Vertrauen aufzubauen.
2. Um eine Metadatendatei hochzuladen, wählen Sie unter IdP-Metadatendokument die Option Datei auswählen aus. Laden Sie die XML-formatierte Metadatendatei von Ihrem Identitätsanbieter hoch, die Sie im vorherigen Schritt heruntergeladen haben.
3. Um eine Metadaten-URL zu verwenden, gehen Sie zu Ihrem IdP, den Sie im vorherigen Schritt eingerichtet haben, und rufen Sie dessen Metadaten-URL ab. Kehren Sie zur WorkSpaces Secure Browser-Konsole zurück und geben Sie unter IdP-Metadaten-URL die Metadaten-URL ein, die Sie von Ihrem IdP erhalten haben.
4. Klicken Sie anschließend auf Next.
5. Für Portale, auf denen Sie die Option Verschlüsselte SAML-Assertionen von diesem Anbieter anfordern aktiviert haben, müssen Sie das Verschlüsselungszertifikat aus dem Abschnitt Portal-IdP-Details herunterladen und auf Ihren IdP hochladen. Anschließend können Sie die Option dort aktivieren.

> **Note**
>
> WorkSpaces Für Secure Browser muss der Betreff oder die NameID zugeordnet und in der SAML-Assertion in den Einstellungen Ihres IdP festgelegt werden. Ihr Identitätsanbieter kann diese Zuordnungen automatisch erstellen. Wenn diese Zuordnungen nicht korrekt

konfiguriert sind, können sich Ihre Benutzer nicht beim Webportal anmelden und keine Sitzung starten.
WorkSpaces Für Secure Browser müssen die folgenden Angaben in der SAML-Antwort enthalten sein. Sie *<Your SP Entity ID>* können die Service Provider-Details oder das Metadaten-Dokument Ihres Portals entweder über die Konsole oder die CLI aufrufen.
<Your SP ACS URL>

- Ein `AudienceRestriction` Anspruch mit einem `Audience` Wert, der Ihre SP-Entitäts-ID als Ziel der Antwort festlegt. Beispiel:

```
<saml:AudienceRestriction>
    <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- Ein `Response`-Anspruch mit einem `InResponseTo`-Wert, der der ursprünglichen SAML-Anforderungs-ID entspricht. Beispiel:

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- Ein `SubjectConfirmationData` Anspruch mit dem `Recipient` Wert Ihrer SP ACS-URL und einem `InResponseTo` Wert, der der ursprünglichen SAML-Anforderungs-ID entspricht. Beispiel:

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Secure Browser validiert Ihre Anforderungsparameter und SAML-Assertionen. Für IDP-initiierte SAML-Assertionen müssen die Details Ihrer Anfrage als `RelayState` Parameter im Hauptteil einer HTTP-POST-Anfrage formatiert werden. Der Anfragetext muss auch Ihre SAML-Assertion als Parameter enthalten. `SAMLResponse` Beide sollten vorhanden sein, wenn Sie den vorherigen Schritt ausgeführt haben.
Im Folgenden finden Sie einen `POST` Beispieltext für einen vom IDP initiierten SAML-Anbieter.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Hinweise zur Verwendung bestimmter Funktionen IdPs mit Amazon WorkSpaces Secure Browser

Um sicherzustellen, dass Sie den SAML-Verbund für Ihr Portal korrekt konfigurieren, finden Sie unter den folgenden Links die Dokumentation von Commons Used IdPs.

IdP	Einrichtung der SAML-Anwendung	Benutzerverwaltung	IDP-initiierte Authentifizierung	Signierung anfordern	Assertion-Verschlüsselung	Einmaliges Abmelden
Okta	Erstellen Sie SAML-App-Integrationen	Benutzerverwaltung	SAML-Feldreferenz für den Assistenten zur Anwendungsintegration	SAML-Feldreferenz für den Assistenten zur Anwendungsintegration	SAML-Feldreferenz für den Assistenten zur Anwendungsintegration	SAML-Feldreferenz für den Assistenten zur Anwendungsintegration
Geben Sie ein	Erstellen Sie Ihre eigene Anwendung	Schnellstart: Erstellen Sie ein Benutzerkonto und weisen Sie es zu	Aktivieren Sie Single Sign-On für eine Unternehmensanwendung	SAML: Signaturverifizierung anfordern	Konfigurieren Sie die SAML-Token-Verschlüsselung von Microsoft Entra	SAML-Protokoll mit einmaliger Anmeldung
Ping	Fügen Sie eine SAML-Anwendung hinzu	Benutzer	IDP-initiiertes SSO aktivieren	Konfiguration der Anmeldung mit Authentifizierungsanforderungen für	Unterstützt PingOne for Enterprise Verschlüsselung?	SAML 2.0-Einzelabmeldung

IdP	Einrichtung der SAML-Anwendung	Benutzerverwaltung	IDP-initiierte Authentifizierung	Signierung anfordern	Assertion-Verschlüsselung	Einmaliges Abmelden
				Enterprise PingOne		
Ein Login	Benutzerdefinierter SAML-Konnektor (erweitert) (4266907)	Fügen OneLogin Sie Benutzer manuell hinzu	Benutzerdefinierter SAML-Konnektor (erweitert) (4266907)	Benutzerdefinierter SAML-Konnektor (erweitert) (4266907)	Benutzerdefinierter SAML-Konnektor (erweitert) (4266907)	Benutzerdefinierter SAML-Konnektor (erweitert) (4266907)
IAM Identity Center	Richten Sie Ihre eigene SAML 2.0-Anwendung ein	Richten Sie Ihre eigene SAML 2.0-Anwendung ein	Richten Sie Ihre eigene SAML 2.0-Anwendung ein	–	–	–

Konfiguration des IAM Identity Center-Authentifizierungstyps für Amazon WorkSpaces Secure Browser

Für den Typ IAM Identity Center (erweitert) verbinden Sie IAM Identity Center mit Ihrem Portal. Wählen Sie diese Option nur aus, wenn Folgendes auf Sie zutrifft:

- Ihr IAM Identity Center ist im selben AWS-Konto und AWS-Region wie Ihr Webportal konfiguriert.
- Wenn Sie verwenden AWS Organizations, verwenden Sie ein Verwaltungskonto.

Bevor Sie ein Webportal mit dem Authentifizierungstyp IAM Identity Center erstellen, müssen Sie IAM Identity Center als eigenständigen Anbieter einrichten. Weitere Informationen finden Sie unter Erste Schritte mit den häufigsten Aufgaben in IAM Identity Center. Oder Sie können Ihren SAML 2.0-IdP mit dem IAM Identity Center verbinden. Weitere Informationen finden Sie unter Connect einem externen Identitätsanbieter herstellen. Andernfalls müssen Sie Ihrem Webportal keine Benutzer oder Gruppen zuweisen.

Wenn Sie IAM Identity Center bereits verwenden, können Sie IAM Identity Center als Anbietertyp auswählen und die folgenden Schritte ausführen, um Benutzer oder Gruppen zu Ihrem Webportal hinzuzufügen, anzuzeigen oder zu entfernen.

> **Note**
>
> Um diesen Authentifizierungstyp verwenden zu können, muss sich Ihr IAM Identity Center im selben AWS-Konto und AWS-Region wie Ihr WorkSpaces Secure Browser-Portal befinden. Wenn sich Ihr IAM Identity Center in einem separaten AWS-Konto oder befindet AWS-Region, folgen Sie den Anweisungen für den Standard-Authentifizierungstyp. Weitere Informationen finden Sie unter the section called “Standardauthentifizierungstyp”.
> Wenn Sie das IAM Identity Center verwenden AWS Organizations, können Sie mit einem Verwaltungskonto nur WorkSpaces Secure Browser-Portale erstellen, die in IAM Identity Center integriert sind.

Topics

Ein Webportal mit IAM Identity Center erstellen

Gehen Sie folgendermaßen vor, um ein Webportal mit IAM Identity Center zu erstellen.

So erstellen Sie ein Webportal mit IAM Identity Center

1. Wählen Sie bei der Portalerstellung unter Schritt 4: Identity Provider konfigurieren die Option AWS IAM Identity Center.
2. Wählen Sie Weiter mit IAM Identity Center.
3. Wählen Sie auf der Seite „Benutzer und Gruppen zuweisen“ die Registerkarte „ and/or Benutzergruppen“.
4. Markieren Sie das Kästchen neben den Benutzern oder Gruppen, die Sie dem Portal hinzufügen möchten.

5. Nachdem Sie Ihr Portal erstellt haben, können sich die Benutzer, denen Sie zugeordnet haben, mit ihrem IAM Identity Center-Benutzernamen und Passwort bei WorkSpaces Secure Browser anmelden.

Verwaltung Ihres Webportals mit IAM Identity Center

Gehen Sie wie folgt vor, um Ihr Webportal mit IAM Identity Center zu verwalten.

So verwalten Sie ein Webportal mit IAM Identity Center

1. Nachdem Sie Ihr Portal erstellt haben, wird es in der IAM Identity Center-Konsole als konfigurierte Anwendung aufgeführt.
2. Damit Sie auf die Konfiguration dieser Anwendung zugreifen können, wählen Sie in der Seitenleiste Anwendungen aus und suchen Sie nach einer konfigurierten Anwendung mit einem Namen, der dem Anzeigenamen Ihres Webportals entspricht.

> **Note**
>
> Wenn Sie keinen Anzeigenamen eingegeben haben, wird stattdessen die GUID Ihres Portals angezeigt. Die GUID ist die ID, die der Endpunkt-URL Ihres Webportals vorangestellt wird.

Hinzufügen zusätzlicher Benutzer und Gruppen zu einem Webportal

Gehen Sie wie folgt vor, um einem vorhandenen Webportal weitere Benutzer und Gruppen hinzuzufügen.

So fügen Sie zusätzliche Benutzer und Gruppen einem vorhandenen Webportal hinzu

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale, wählen Sie Ihr Webportal aus und klicken Sie dann auf Bearbeiten.
3. Wählen Sie Einstellungen für Identitätsanbieter und Weitere Benutzer und Gruppen zuweisen aus. Von hier aus können Sie Ihrem Webportal Benutzer und Gruppen hinzufügen.

> **Note**
>
> Sie können keine Benutzer oder Gruppen über die IAM-Identity-Center-Konsole hinzufügen. Sie müssen dies auf der Bearbeitungsseite Ihres WorkSpaces Secure Browser-Portals tun.

Benutzer und Gruppen für Ihr Webportal anzeigen oder entfernen

Verwenden Sie die in der Tabelle Zugewiesene Benutzer verfügbaren Aktionen, um Benutzer und Gruppen für Ihr Webportal anzuzeigen oder zu entfernen. Weitere Informationen finden Sie unter Zugriff auf Anwendungen verwalten

> **Note**
>
> Sie können Benutzer und Gruppen auf der Bearbeitungsseite des WorkSpaces Secure Browserportals nicht anzeigen oder entfernen. Sie müssen dies von der Bearbeitungsseite Ihrer IAM-Identity-Center-Konsole aus tun.

Ändern des Identitätsanbietertyps für Amazon WorkSpaces Secure Browser

Sie können den Authentifizierungstyp Ihres Portals jederzeit ändern. Gehen Sie dazu wie folgt vor.

- Um von IAM Identity Center zu Standard zu wechseln, folgen Sie den Schritten unterthe section called “Standardauthentifizierungstyp”.
- Um von Standard zu IAM Identity Center zu wechseln, folgen Sie den Schritten unter. the section called “Authentifizierungstyp für IAM Identity Center”

Die Implementierung von Änderungen am Identitätsanbietertyp kann bis zu 15 Minuten dauern. Laufende Sitzungen werden nicht automatisch beendet.

Sie können sich die Änderungen des Identitätsanbietertyps in Ihrem Portal ansehen, AWS CloudTrail indem Sie sich die Ereignisse `UpdatePortal` ansehen. Der Typ ist in den Anforderungs- und Antwort-Payloads des Ereignisses sichtbar.

Starten eines Webportals mit Amazon WorkSpaces Secure Browser

Wenn Sie mit der Konfiguration Ihres Webportals fertig sind, können Sie es wie folgt starten.

1. Überprüfen Sie auf der Seite Schritt 5: Überprüfen und starten die Einstellungen, die Sie für Ihr Webportal ausgewählt haben. Sie können Bearbeiten auswählen, um die Einstellungen in einem bestimmten Abschnitt zu ändern. Sie können diese Einstellungen auch später auf der Registerkarte Webportale der Konsole ändern.
2. Wenn Sie fertig sind, wählen Sie Webportal starten aus.
3. Wenn Sie den Status Ihres Webportals anzeigen möchten, wählen Sie Webportale, Ihr Portal und dann Details anzeigen aus.

   Ein Webportal hat einen der folgenden Status:

   - Unvollständig: In der Konfiguration des Webportals fehlen die erforderlichen Identitätsanbieter-Einstellungen.
   - Ausstehend: Das Webportal wendet Änderungen bei seinen Einstellungen an.
   - Aktiv: Das Webportal ist bereit und kann verwendet werden.
4. Warten Sie bis zu 15 Minuten, bis Ihr Portal aktiv wird.

Testen Sie Ihr Webportal im Amazon WorkSpaces Secure Browser

Nachdem Sie ein Webportal erstellt haben, können Sie sich beim WorkSpaces Secure Browser-Endpunkt anmelden, um Ihre verbundenen Websites wie ein Endbenutzer zu durchsuchen.

Wenn Sie diese Schritte bereits in the section called “Konfiguration des Identitätsanbieters” abgeschlossen haben, können Sie diesen Abschnitt überspringen und bei Verteilen Ihres Webportals im Amazon WorkSpaces Secure Browser fortfahren.

1. Die WorkSpaces Secure Browser-Konsole zu https://console.aws.amazon.com/workspaces-web/Hause öffnen? region=us-ost-1#/.
2. Wählen Sie WorkSpaces Sicherer Browser, Webportale, wählen Sie Ihr Webportal und dann Details anzeigen
3. Rufen Sie unter Webportal-Endpunkt die angegebene URL für Ihr Portal auf. Der Webportal-Endpunkt ist der Zugangspunkt, von dem aus Ihre Benutzer Ihr Webportal starten, nachdem sie sich mit dem für das Portal konfigurierten Identitätsanbieter angemeldet haben. Er ist öffentlich im Internet verfügbar und kann in Ihr Netzwerk eingebettet werden.

4. Wählen Sie auf der Anmeldeseite für WorkSpaces Secure Browser die Option Anmelden, SAML aus und geben Sie Ihre SAML-Anmeldeinformationen ein.
5. Wenn Sie die Seite „Ihre Sitzung wird vorbereitet“ sehen, wird Ihre WorkSpaces Secure Browser-Sitzung gestartet. Schließen oder verlassen Sie diese Seite nicht.
6. Der Webbrowser wird gestartet und zeigt Ihre Startup-URL und jedes andere zusätzliche Verhalten an, das in den Richtlinieneinstellungen Ihres Browsers konfiguriert wurde.
7. Sie können jetzt zu verbundenen Websites navigieren, indem Sie Links auswählen oder die Adressleiste URLs eingeben.

Verteilen Ihres Webportals im Amazon WorkSpaces Secure Browser

Wenn Sie bereit sind, dass Ihre Benutzer mit der Nutzung von WorkSpaces Secure Browser beginnen können, wählen Sie aus den folgenden Optionen für die Verteilung des Portals:

- Fügen Sie Ihr Portal zu Ihrem SAML-Anwendungsgateway hinzu, damit Benutzer eine Sitzung direkt von ihrem IdP aus starten können. Sie können dies über den vom IdP initiierten Anmeldevorgang mit Ihrem SAML 2.0-kompatiblen IdP tun. Weitere Informationen finden Sie unter SP-initiierte und IDP-initiierte SAML-Assertionen in. the section called “Standardauthentifizierungstyp” Alternativ können Sie eine benutzerdefinierte SAML-Anwendung erstellen, die IDP-initiierte Authentifizierungserlebnisse mithilfe von SP-initiierten Flows bereitstellen kann. Weitere Informationen finden Sie unter Erstellen einer Bookmark-App-Integration.
- Fügen Sie die Portal-URL einer Website hinzu, deren Besitzer Sie sind, und verwenden Sie eine Browserumleitung, um Benutzer zum Webportal weiterzuleiten.
- Senden Sie die Portal-URL per E-Mail an Ihre Benutzer oder übertragen Sie sie auf ein Gerät, das Sie als Browserstartseite oder als Lesezeichen verwalten.
- Verwenden Sie anstelle der Portal-URL eine benutzerdefinierte Domain, wenn Sie eine für Ihr Portal eingerichtet haben, um Ihren Benutzern ein stärker integriertes Branding-Erlebnis zu bieten. Weitere Informationen finden Sie unter the section called “Benutzerdefinierte Domain”.

Verwaltung Ihres Webportals im Amazon WorkSpaces Secure Browser

Nachdem Sie Ihr Webportal eingerichtet haben, können Sie es mit den folgenden Aktionen verwalten.

Topics

Webportaldetails im Amazon WorkSpaces Secure Browser anzeigen

Gehen Sie wie folgt vor, um die Details des Webportals anzuzeigen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale, wählen Sie Ihr Webportal und dann Details anzeigen aus.

Bearbeiten eines Webportals im Amazon WorkSpaces Secure Browser

Gehen Sie folgendermaßen vor, um ein Webportal zu bearbeiten.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale, wählen Sie Ihr Webportal aus und klicken Sie dann auf Bearbeiten.

> **Note**
>
> Änderungen an den Netzwerkeinstellungen oder den Einstellungen für die Zeitüberschreitung beenden sofort alle aktiven Portalsitzungen. Benutzer werden getrennt und müssen sich erneut verbinden, um eine neue Sitzung zu beginnen. Änderungen der Zwischenablageberechtigungen, der Dateiübertragungsberechtigungen oder Auf lokalem Gerät ausdrucken gelten ab der ersten neuen Sitzung. Derzeit aktive Sitzungen werden nicht getrennt. Bei Benutzern, die mit aktiven Sitzungen verbunden sind, werden die Änderungen erst wirksam, wenn sie die Verbindung trennen und eine Verbindung mit einer neuen Sitzung herstellen.

Löschen eines Webportals im Amazon WorkSpaces Secure Browser

Gehen Sie folgendermaßen vor, um ein Webportal zu löschen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale, wählen Sie Ihr Webportal und dann Löschen aus.

Verwaltung von Servicekontingenten für Ihr Portal im Amazon WorkSpaces Secure Browser

Wenn Sie Ihre erstellen AWS-Konto, legen wir automatisch Standard-Servicekontingenten (auch als Limits bezeichnet) für die Ressourcennutzung mit fest AWS-Services. Administratoren müssen sich über zwei Kontingente im Klaren sein, die möglicherweise erhöht werden müssen, um ihren Anwendungsfall zu unterstützen. Diese beiden Kontingente sind die Anzahl der Webportale, die Sie in jeder Region erstellen können, und die Anzahl der maximalen gleichzeitigen Sitzungen, die Sie mit jedem verfügbaren Instanztyp in jeder Region unterstützen können. Sie können eine Erhöhung für diese Dienste auf der Seite „Service Quotas“ in der AWS Konsole beantragen.

In der folgenden Tabelle sind die Standardgrenzwerte für Servicekontingenten aufgeführt.

Standardkontingente innerhalb und AWS-Region nach Konto	Wert
Webportale	3
Maximale Anzahl gleichzeitiger Sitzungen - standard.regular	25
Maximale Anzahl gleichzeitiger Sitzungen — standard.large	10
Maximale Anzahl gleichzeitiger Sitzungen - standard.xlarge	5

Die Ihrem Konto zugewiesenen Servicekontingente für jede Region können Sie jederzeit auf der Seite Servicekontingente einsehen.

> **Important**
>
> Servicekontingente AWS-Region gelten jeweils einzeln. Sie müssen jeweils eine Erhöhung der Servicekontingenten beantragen AWS-Region , wenn Sie mehr Ressourcen benötigen. Weitere Informationen finden Sie unter Amazon WorkSpaces Secure Browser-Endpunkte und Kontingente.

Topics

Eine Erhöhung des Servicekontingents im Amazon WorkSpaces Secure Browser beantragen

Gehen Sie wie folgt vor, um eine Erhöhung der Servicequote zu beantragen.

1. Öffnen Sie das AWS-Support-Dashboard.
2. Wählen Sie Erhöhung des Servicelimits aus.

   > **Important**
   >
   > WorkSpaces Die Secure Browser-Dienstkontingente gelten jeweils für eine Region. Sie müssen in jeder AWS-Region eine Service-Quota-Erhöhung beantragen, in der Sie mehr Ressourcen benötigen. Weitere Informationen finden Sie unter AWS-Service-Endpunkte.

3. Geben Sie in der Beschreibung des Anwendungsfalls die folgenden Informationen an:

- Wenn Sie eine Erhöhung der Webportal-Anzahl beantragen, geben Sie diesen Ressourcentyp und Ihre AWS-Konto-ID, die Region, in der Sie die Erhöhung wünschen, und den neuen Grenzwert an.
- Wenn Sie eine Erhöhung der maximal möglichen gleichzeitigen Sitzungen beantragen, geben Sie diesen Ressourcentyp und Ihre AWS-Konto-ID, die Region, in der Sie die Erhöhung wünschen, den ARN des Webportals und den neuen Grenzwert an.

4. (Optional) Um mehrere Service-Quota-Erhöhungen gleichzeitig zu beantragen, füllen Sie eine Anfrage zur Erhöhung des Kontingents im Abschnitt „Anfragen“ aus und wählen Sie dann Weitere Anfrage hinzufügen aus.

Erhöhung des Portals im Amazon WorkSpaces Secure Browser beantragen

Ein Portal ist die grundlegende Ressource des Dienstes. Jedes Portal ist eine Verbindung zwischen Ihrem SAML 2.0-Identitätsanbieter und Ihrer Netzwerkverbindung zum Internet und allen privaten Webinhalten. Jedes Portal kann über eigene Richtlinien und Benutzereinstellungen für den Portalbrowser verfügen, sodass Administratoren in der Regel mehrere Portale in derselben Region erstellen, um unterschiedliche Anwendungsfälle abzudecken. Sie können beispielsweise Gruppe A Zugriff auf eine bestimmte Website mit restriktiven Richtlinien gewähren (z. B. sind Zwischenablage und Dateiübertragung deaktiviert) und Gruppe B Zugriff auf das allgemeine Internet ohne URL-Filterung gewähren. Sie können ein Portal in jeder unterstützten AWS-Region Version erstellen. Informationen zur aktuellen Serviceverfügbarkeit finden Sie unter AWS-Services nach Regionen.

So fordern Sie eine Erhöhung Ihrer Service Quota an

1. Öffnen Sie die Seite mit den Service Quotas in der gewünschten Region.
2. Wählen Sie Anzahl der Webportale.
3. Wählen Sie Erhöhung auf Kontoebene beantragen aus.
4. Geben Sie unter Kontingentwert erhöhen den gewünschten Gesamtbetrag für das Kontingent ein.

Eine Erhöhung der maximalen Anzahl gleichzeitiger Sitzungen im Amazon WorkSpaces Secure Browser beantragen

Das maximale Kontingent für gleichzeitige Sitzungen ist die höchste Anzahl von Benutzern, die gleichzeitig mit einem Portal verbunden werden können. Wenn das Servicekontingent für die

maximale Anzahl gleichzeitiger Sitzungen nicht angemessen festgelegt ist, stellen Benutzer möglicherweise fest, dass eine Sitzung nicht verfügbar ist, wenn sie sich anmelden. Kunden müssen nicht nur dieses Servicekontingent erhöhen, sondern auch sicherstellen, dass ihre VPC und Subnetze über ausreichend IP-Speicherplatz verfügen, um die maximale Anzahl gleichzeitiger Sitzungen zu unterstützen.

Um eine Erhöhung der maximalen Anzahl gleichzeitiger Sitzungen zu beantragen

1. Öffnen Sie die Seite mit den Service Quotas in der gewünschten Region.
2. Wählen Sie „Anzahl der maximalen gleichzeitigen Sitzungen pro Portal“ für den Instanztyp, den Sie erhöhen möchten.
3. Wählen Sie Erhöhung auf Kontoebene beantragen aus.
4. Geben Sie unter Kontingentwert erhöhen den gewünschten Gesamtbetrag für das Kontingent ein.

> **Note**
>
> Gehen Sie bei großen oder dringenden Erhöhungen zur Seite mit dem Verlauf Ihrer Servicekontingente, wählen Sie den Link in der Statusspalte Ihrer Anfrage aus, stellen Sie einen Link zu Ihrem Support-Fall her und fügen Sie eine Antwort mit Details zu Ihrem Anwendungsfall and/or der Dringlichkeit hinzu. Diese Informationen helfen dem Serviceteam, Anfragen zu priorisieren und sicherzustellen, dass Ihrem Konto ausreichend Kapazität zugewiesen wird.

Beispiel für ein Limit für Amazon WorkSpaces Secure Browser

Nehmen wir als Beispiel an, ein Administrator konfiguriert zwei Webportale in USA Ost (Nord-Virginia) für insgesamt 125 Benutzer. Vor der Erstellung des Webportals identifiziert der Administrator das erste Webportal (Portal A), das 100 Benutzer unterstützt. Beim Testen des Workflows für diese Benutzer stellt der Administrator fest, dass sie den XL-Instanztyp benötigen, um das Streaming von Audio und Video während der Sitzung zu unterstützen. Das zweite Webportal (Portal B) muss für bis zu 25 Benutzer verfügbar sein, um den Zugriff auf eine einzelne statische Webseite zu unterstützen, die in der VPC des Kunden gehostet wird. Beim Testen dieses Anwendungsfalls stellt der Administrator fest, dass der Standard-Instanztyp diesen Anwendungsfall unterstützen kann.

Für Portal A muss der Administrator eine Anfrage zur Erhöhung des Servicekontingents einreichen, um das Limit für XL-Instances von den Standardwerten der Region (d. h. 5) auf 100 anzuheben.

Sobald der Vorgang abgeschlossen ist, kann der Administrator die Kapazität zuweisen, indem er das Webportal bearbeitet. Für Portal B kann der Administrator weitermachen, ohne eine Erhöhung des Kontingents zu beantragen (d. h., da die Region ein Standardkontingent von 25 für den Standard-Instanztyp hat).

Andere Servicekontingente im Amazon WorkSpaces Secure Browser

Sie können Erhöhungen für andere Kontingente, die auf der Seite Service Quotas aufgeführt sind, einsehen und beantragen. In der Praxis werden es die meisten Kunden für unnötig halten, Erhöhungen für diese Limits zu beantragen. Diese Kontingente lassen sich grob in zwei Typen unterteilen: Anzahl und Rate.

Wenn Sie bei Zahlenkontingenten eine Erhöhung der Servicequote für die Anzahl der Webportale einreichen, erhalten Sie automatisch eine Erhöhung der Anzahl der Unterressourcen, die für die Erstellung eines eindeutigen Portals erforderlich sind. Dies wird auf der Seite mit den Service Quotas angezeigt. Wenn Sie beispielsweise eine Erhöhung der Portale von 3 auf 5 beantragen, erhalten Sie automatisch eine Erhöhung des Servicekontingents von 3 auf 5, sowohl für die Browser- als auch für die Benutzereinstellungen. Sie haben die Möglichkeit, Subressourcen nach Wunsch wiederzuverwenden oder neue zu erstellen.

In seltenen Fällen finden Kunden möglicherweise einen Anwendungsfall für die Erhöhung der Anzahl oder Rate anderer Ressourcenkontingente. Beispielsweise möchten Administratoren möglicherweise die Anzahl der Browsereinstellungen erhöhen, um zusätzliche Portalkonfigurationen zu testen. Diese Anfragen für Servicekontingente werden auf einer bestimmten case-by-case Grundlage geprüft und erfüllt.

Bei Preiskontingenten sollten die in Service Quotas angegebenen Ratenlimits unabhängig vom Kontoportallimit nicht angepasst werden müssen.

Steuerung des Intervalls für die erneute Authentifizierung eines SAML-IdP-Tokens im Amazon Secure Browser WorkSpaces

Wenn ein Benutzer ein WorkSpaces Secure Browser-Portal besucht, kann er sich anmelden, um eine Streaming-Sitzung zu starten. Jede Sitzung beginnt auf der Startseite, sofern sie sich nicht vor weniger als 5 Minuten angemeldet haben. Das Portal sucht nach Identitätsanbieter-Token, um festzustellen, ob der Benutzer beim Starten einer Sitzung zur Eingabe von Anmeldeinformationen aufgefordert werden soll. Ein Benutzer ohne gültiges Identitätsanbieter-Token muss einen Benutzernamen, ein Passwort und (optional) eine Multifaktor-Authentifizierung (MFA) eingeben, um

eine Streaming-Sitzung zu starten. Wenn ein Benutzer bereits ein SAML-IdP-Token generiert hat, indem er sich bei seinem Identitätsanbieter oder einer von demselben Identitätsanbieter geschützten App angemeldet hat, wird er nicht nach Anmeldeinformationen gefragt.

Wenn ein Benutzer über ein gültiges SAML-IdP-Token verfügt, kann er auf WorkSpaces Secure Browser zugreifen. Sie können das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern.

So steuern Sie das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens

1. Legen Sie die Dauer der Zeitüberschreitung vom Identitätsanbieter bei Ihrem SAML-Identitätsanbieter fest. Wir empfehlen, die Dauer der Zeitüberschreitung vom Identitätsanbieter so zu konfigurieren, dass die kürzeste Zeit gewählt wird, die ein Benutzer benötigt, um seine Aufgaben zu erledigen.

   - Weitere Informationen zu Okta finden Sie unter Eine begrenzte Sitzungsdauer für alle Richtlinien durchsetzen.
   - Weitere Informationen zu Azure AD finden Sie unter Konfigurieren der Sitzungssteuerelemente für Authentifizierung.
   - Weitere Informationen zu Sitzungen finden Sie unter Sitzungen.
   - Weitere Informationen dazu finden Sie AWS IAM Identity Center unter Sitzungsdauer festlegen.
2. Legen Sie die Inaktivitäts- und Leerlauf-Timeout-Werte Ihres WorkSpaces Secure Browser-Portals fest. Diese Werte steuern die Zeitspanne zwischen der letzten Interaktion eines Benutzers und dem Ende einer WorkSpaces Secure Browser-Sitzung aufgrund von Inaktivität. Wenn eine Sitzung endet, verliert ein Benutzer seinen Sitzungsstatus (einschließlich geöffneter Registerkarten, nicht gespeicherter Webinhalte und Verlauf) und kehrt zu Beginn der nächsten Sitzung in einen neuen Status zurück. Weitere Informationen finden Sie in Schritt 5 unter the section called “Erstellung eines Webportals”.

   > **Note**
   >
   > Wenn bei der Sitzung eines Benutzers ein Timeout auftritt, der Benutzer aber immer noch über ein gültiges SAML-IdP-Token verfügt, muss er seinen Benutzernamen und sein Passwort nicht eingeben, um eine neue WorkSpaces Secure Browser-Sitzung zu starten. Um zu kontrollieren, wie Token erneut authentifiziert werden, folgen Sie den Anleitungen im vorherigen Schritt.

Protokollierung von Benutzeraktivitäten im Amazon WorkSpaces Secure Browser einrichten

WorkSpaces Secure Browser bietet zwei Optionen für die Protokollierung von Benutzeraktivitäten und sicherheitsrelevanten Ereignissen:

- Session Logger erfasst eine Vielzahl von Sitzungsereignissen. Diese Protokolle werden an einen Amazon S3 S3-Bucket in Ihrem Konto übermittelt, was eine einfache Integration mit Ihrer bevorzugten SIEM-Plattform ermöglicht.
- Die Benutzerzugriffsprotokollierung erfasst die kritischsten Sitzungsereignisse. Diese Protokolle werden zur Verarbeitung und Analyse in Echtzeit in einen Amazon Kinesis Kinesis-Stream gestreamt.

Beide Protokollierungsoptionen werden auf Portalebene konfiguriert. Sie müssen jede Option einzeln für jedes Portal einrichten, in dem die Protokollierung aktiv sein soll. Sie können je nach Ihren Anforderungen für jedes Portal eine der Optionen oder beide aktivieren.

Sie sind dafür verantwortlich, alle Anforderungen zu erfüllen, die für die Protokollierung oder Überwachung von Benutzeraktivitäten bei der Verwendung dieser Funktion gelten, einschließlich der Protokollierung oder Überwachung von Mitarbeiteraktivitäten.

Topics

Session Logger für Amazon WorkSpaces Secure Browser einrichten

> **Warning**
>
> Durch die Aktivierung von Session Logger werden die folgenden Chrome-Funktionen deaktiviert:
>
> - Inkognito-Modus
> - Entwicklertools
> - Chrome-Profilwechsel

Um den Sitzungslogger für ein WorkSpaces Secure Browser-Portal zu aktivieren, müssen Sie zunächst den Amazon S3 S3-Bucket identifizieren, in dem Sitzungsereignisse gesammelt werden. Sie können einen vorhandenen Bucket verwenden, der bereits ähnliche Protokolle speichert, oder einen neuen Bucket speziell für diesen Zweck erstellen.

Der Amazon S3 S3-Bucket muss über eine Bucket-Richtlinie verfügen, die WorkSpaces Secure Browser die Erlaubnis erteilt, Protokolle in den Bucket zu schreiben. Wir empfehlen, den Amazon S3 S3-Bucket in derselben AWS-Konto Region wie Ihr WorkSpaces Secure Browser-Portal zu platzieren.

Es gibt keine Benennungspflicht für den Amazon S3 S3-Bucket. Gehen Sie wie folgt vor, um einen neuen Bucket zu erstellen, oder lesen Sie im Amazon Simple Storage Service-Benutzerhandbuch den Abschnitt Erstellen eines Allzweck-Buckets. Anleitungen zur Konfiguration von Berechtigungen finden Sie unter Bucket-Richtlinien für Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie für Ihren Amazon S3 S3-Bucket. Stellen Sie sicher, dass Sie die Richtlinie mit dem Namen Ihres Amazon S3 S3-Buckets aktualisieren. Beachten Sie, dass der Principal „workspaces-web.amazonaws.com“ lautet.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowSessionLogger",
          "Effect": "Allow",
          "Principal": {
              "Service": "workspaces-web.amazonaws.com"
          },
          "Action": [
              "s3:PutObject"
          ],
          "Resource": [
              "arn:aws:s3:::bucket-name/*"
          ]
      }
  ]
}
```

Die Aktivierung von Session Logger auf Ihrem WorkSpaces Secure Browser-Portal kann zu Gebühren von Amazon S3 führen. Informationen finden Sie unter Amazon S3 – Preise.

Weitere Informationen zu den sitzungsbezogenen Ereignissen, die von Session Logger erfasst werden, finden Sie unter. the section called “Sitzungsereignisse im Session Logger”

S3-Buckets mit KMS-Verschlüsselung (optional)

WorkSpaces Secure Browser Session Logger unterstützt Amazon S3 S3-Buckets mit aktivierter AWS KMS Verschlüsselung vollständig. Um die ordnungsgemäße Protokollierungsfunktion mit Ihrem verschlüsselten Amazon S3 S3-Bucket sicherzustellen, müssen Sie Session Logger die erforderlichen Berechtigungen zur Verwendung Ihres AWS KMS Schlüssels gewähren.

Fügen Sie Ihrer AWS KMS Schlüsselkonfiguration die folgende Richtlinie hinzu:

```
{
  "Sid": "Session Logger",
  "Effect": "Allow",
  "Principal": {
    "Service": "workspaces-web.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
```

Wählen Sie in der AWS Konsole das WorkSpaces Secure Browser-Portal aus, in dem Sie Ereignisse erfassen möchten, und klicken Sie auf die Registerkarte Sitzungsprotokollierung und dann auf Bearbeiten.

Geben Sie die folgenden Informationen ein, um den Sitzungslogger für das Portal zu konfigurieren:

- S3-Standort (erforderlich): Der Name Ihres Amazon S3 S3-Buckets, in den Ereignisse übertragen werden.
- Schlüsselpräfix (optional): Der Ordner, in den Ereignisse übermittelt werden. Wenn der Ordner nicht existiert, wird er erstellt. Wenn das Feld leer gelassen wird, schreibt Session Logger Ereignisse in das Stammverzeichnis des Amazon S3 S3-Buckets.

Unter Erweitert können Sie die folgenden Felder konfigurieren:

- Ereignisfilter: Dies ist die Liste der Ereignisse, die von Session Logger überwacht werden.
  - Alle: Wenn Sie diese Option auswählen, werden alle aktuellen und future Ereignisse überwacht
  - Einschließen: Auf diese Weise können Sie manuell bestimmte Ereignisse auswählen, die überwacht werden sollen. Nur die explizit ausgewählten Ereignisse werden protokolliert. Neue Ereignisse, die in future Updates eingeführt werden, werden nicht überwacht, es sei denn, sie werden manuell zur Auswahl hinzugefügt.
- Dateiformat
  - JSON (Standard): Dies ist ein Dateiformat, bei dem jede Protokolldatei als eine Reihe von Ereignissen dargestellt wird. Wir empfehlen dieses Format für die meisten Anwendungsfälle.
  - JSONLines: Dies ist ein Dateiformat, das für Amazon Athena optimiert ist.
- Ordnerstruktur: Dies bestimmt, wie die Protokolldateien gespeichert werden.
  - Flach (Standard): Alle Protokolldateien befinden sich in einem einzigen Ordner.
  - Nach Datum verschachtelt: Die Protokolldateien sind nach Datum und Uhrzeit in Ordnern angeordnet. Partitioniert für Amazon Athena und optimiert für Amazon Athena Athena-Abfragen.

Sie können das Session Logger-Setup testen und sicherstellen, dass der Session-Logger ordnungsgemäß funktioniert. Sobald die Konfiguration abgeschlossen ist, versucht das System, eine Testdatei mit dem Namen in den angegebenen Amazon S3 S3-Bucket und Ordner `_workspaces_secure_browser.tmp` zu schreiben. Dies dient der Validierung sowohl der Protokollierungsfunktion als auch der Einrichtung von Berechtigungen.

Sie können auch eine Testsitzung ausführen, indem Sie eine Secure Browser-Sitzung im Portal starten und den Browser wie gewohnt verwenden. Session Logger schreibt während einer aktiven Sitzung oder wenn die Sitzung endet, alle 15 Minuten Protokolldateien in Ihren konfigurierten Amazon S3 S3-Bucket.

Nachdem Sie die Sitzung beendet oder auf das nächste Protokollierungsintervall gewartet haben, überprüfen Sie den Amazon S3 S3-Bucket, um sicherzustellen, dass die Protokolldateien für Ihre Sitzung wie erwartet generiert und gespeichert wurden.

Benutzerzugriffsprotokollierung für Amazon WorkSpaces Secure Browser einrichten

Um die Benutzerzugriffsprotokollierung in der WorkSpaces Secure Browser-Konsole zu aktivieren, wählen Sie unter Benutzerzugriffsprotokollierung die Kinesis Stream-ID aus, die Sie für den Datenempfang verwenden möchten. Die aufgezeichneten Daten werden direkt in diesen Stream übertragen.

Weitere Informationen zur Erstellung eines Amazon-Kinesis-Datenstroms finden Sie unter Was sind Amazon Kinesis Data Streams?

Um Protokolle vom WorkSpaces Secure Browser zu empfangen, benötigen Sie einen Amazon Kinesis Data Stream, der mit "amazon-workspaces-web-*“ beginnt. Für Ihren Amazon Kinesis Kinesis-Datenstream muss entweder die serverseitige Verschlüsselung deaktiviert sein oder Von AWS verwaltete Schlüssel für die serverseitige Verschlüsselung verwendet werden.

Weitere Informationen zur Einstellung der serverseitigen Verschlüsselung in Amazon Kinesis finden Sie unter Wie beginne ich mit serverseitiger Verschlüsselung?.

Verwaltung der Browserrichtlinie im Amazon WorkSpaces Secure Browser

Sie können jede benutzerdefinierte Browserrichtlinie mithilfe der Chrome-Richtlinien festlegen, die für die neueste stabile Version von WorkSpaces Secure Browser verfügbar sind. Wenn Sie im WorkSpaces Secure Browser-Portal eine Richtlinie festlegen, gilt die Richtlinie für alle Sitzungen, die von diesem Webportal verwaltet werden.

Es gibt mehr als 300 Richtlinien, die Sie auf ein Webportal anwenden können. Weitere Informationen, einschließlich der vollständigen Liste der Chrome-Richtlinien, finden Sie in der Chrome Enterprise-Richtlinienliste.

Sie haben drei Möglichkeiten, eine Chrome-Richtlinie festzulegen:

1. Verwenden des visuellen Editors im Webportal

   Wenn Sie die Konsolenansicht verwenden, um ein Webportal zu erstellen, können Sie einige der gängigsten Richtlinien im visuellen Editor anwenden:

   - `StartURL`
   - Aktivieren und Deaktivieren von privatem Browsing

- Löschung des Verlaufs
- Lesezeichen und Lesezeichenordner

2. Verwenden des JSON-Editors im Webportal

   Sie können Richtlinien auch direkt hinzufügen oder bearbeiten, indem Sie den JSON-Editor anstelle des visuellen Editors verwenden.

   Das spezifische Format einer Richtlinie finden Sie in der Chrome Enterprise-Richtlinienliste.

3. Eine JSON-Datei in das Webportal hochladen

   Sie können auch die in Ihrer Organisation verwendeten Chrome-Richtlinien importieren, indem Sie eine JSON-Datei in das Webportal hochladen.

   Einzelheiten finden Sie unter the section called “Tutorial: Eine benutzerdefinierte Browserrichtlinie einrichten”

WorkSpaces Secure Browser wendet eine grundlegende Browserrichtlinienkonfiguration zusammen mit allen von Ihnen angegebenen Richtlinien auf alle Portale an. Sie können einige dieser Richtlinien mit Ihrer benutzerdefinierten JSON-Datei bearbeiten. Weitere Informationen finden Sie unter the section called “Bearbeitung der grundlegenden Browserrichtlinie”.

Topics

- Tutorial: Eine benutzerdefinierte Browserrichtlinie im Amazon WorkSpaces Secure Browser einrichten
- Bearbeiten der grundlegenden Browserrichtlinie im Amazon WorkSpaces Secure Browser

Tutorial: Eine benutzerdefinierte Browserrichtlinie im Amazon WorkSpaces Secure Browser einrichten

Sie können jede unterstützte Chrome-Richtlinie für Linux festlegen, indem Sie eine JSON-Datei hochladen. Weitere Informationen zu den Chrome-Richtlinien finden Sie in der Liste der Chrome Unternehmensrichtlinien. Wählen Sie dort die Linux-Plattform aus. Suchen und überprüfen Sie dann die Richtlinien für die neueste stabile Version.

Im folgenden Tutorial erstellen Sie ein Webportal mit den folgenden Richtlinienkontrollen:

- Lesezeichen einrichten

- Standard-Startseiten einrichten
- Verhindern, dass der Benutzer andere Erweiterungen installiert
- Verhindern, dass der Benutzer den Verlauf löscht
- Verhindern, dass der Benutzer auf den Inkognitomodus zugreift
- Installieren Sie vorab die Erweiterung Okta-Plug-in für alle Sitzungen.

Topics

Schritt 1: Ein Webportal erstellen

Um Ihre JSON-Datei für Chrome-Richtlinien hochzuladen, müssen Sie ein WorkSpaces Secure Browser-Portal erstellen. Weitere Informationen finden Sie unter the section called “Erstellung eines Webportals”.

Schritt 2: Richtlinien sammeln

Suchen Sie in den Chrome-Richtlinien nach gewünschten Richtlinien. Sie verwenden dann die Richtlinien, um im nächsten Schritt eine JSON-Datei zu erstellen.

1. Gehen Sie zur Liste der Chrome-Unternehmensrichtlinien.
2. Wählen Sie die Plattform Linux und dann die neueste Chrome-Version aus.
3. Suchen Sie nach den Richtlinien, die Sie festlegen möchten. Suchen Sie in diesem Beispiel nach Erweiterungen, um Richtlinien für deren Verwaltung zu finden. Jede Richtlinie enthält eine Beschreibung, einen Namen für die Linux-Einstellung und einen Beispielwert.
4. Aus den Suchergebnissen gehen 3 Richtlinien hervor, die bei gemeinsamer Verwendung die Unternehmensanforderungen erfüllen:
   - ExtensionSettings – installiert eine Erweiterung beim Start des Browsers.
   - ExtensionInstallBlocklist – verhindert die Installation bestimmter Erweiterungen.
   - ExtensionInstallAllowlist— Ermöglicht die Installation bestimmter Erweiterungen.

5. Zusätzliche Richtlinien erfüllen die verbleibenden Anforderungen;
   - ManagedBookmarks— Fügt Webseiten Lesezeichen hinzu.
   - RestoreOnStartupURLs— Konfiguriert, welche Webseiten geöffnet werden, wenn ein neues Browserfenster geöffnet wird.
   - AllowDeletingBrowserHistory— Konfiguriert, ob Benutzer ihren Browserverlauf löschen können.
   - IncognitoModeAvailability— Konfiguriert, ob Benutzer auf den Inkognito-Modus zugreifen können.

Schritt 3: Eine benutzerdefinierte JSON-Richtliniendatei erstellen

Erstellen Sie eine JSON-Datei mit einem Texteditor, einer Vorlage und den Richtlinien, die Sie im vorherigen Schritt gefunden haben.

1. Öffnen Sie einen Texteditor.
2. Kopieren Sie die folgende Vorlage und fügen Sie ihn in Ihren Texteditor ein:

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
```

```
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

Schritt 4: Ihre Richtlinien zur Vorlage hinzufügen

Fügen Sie der Vorlage Ihre benutzerdefinierten Richtlinien für jede Unternehmensanforderung hinzu.

1. Richten Sie ein Lesezeichen ein. URLs
   a. Fügen Sie unter dem `value`-Schlüssel für jedes hinzuzufügende Lesezeichen die Schlüsselpaare `name` und `url` hinzu.
   b. Setzen Sie `bookmark-url-1` auf `https://www.amazon.com`.
   c. Setzen Sie `bookmark-url-2` auf `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. Richten Sie den Start URLs ein. Mit dieser Richtlinie können Administratoren die Webseiten festlegen, die angezeigt werden, wenn ein Benutzer ein neues Browserfenster öffnet.
   a. Legen Sie den Wert für `RestoreOnStartup` auf `4` fest. Dies legt die `RestoreOnStartup` Aktion fest, mit der eine Liste geöffnet werden soll URLs . Sie können bei Ihrem Start auch andere Aktionen verwenden URLs. Weitere Informationen finden Sie in der Liste der Chrome-Unternehmensrichtlinien.
   b. Auf `RestoreOnStartupURLs` https://www.aboutamazon.com /news setzen.

```
    "RestoreOnStartup":
        {
```

```
            "value": 4
        },
    "RestoreOnStartupURLs":
        {
            "value":
            [
                "https://www.aboutamazon.com/news"
            ]
        },
```

3. Wenn Sie verhindern möchten, dass der Benutzer seinen Browserverlauf löscht, legen Sie `AllowDeletingBrowserHistory` auf `false` fest.

```
    "AllowDeletingBrowserHistory":
        {
            "value": false
        },
```

4. Wenn Sie den Zugriff auf den Inkognitomodus für Ihre Benutzer deaktivieren möchten, legen Sie `IncognitoModeAvailability` auf 1 fest.

```
    "IncognitoModeAvailability":
        {
            "value": 1
        }
```

5. Richten Sie das Okta-Plug-in mit den folgenden Richtlinien ein und setzen Sie es durch:

   - `ExtensionSettings` – installiert eine Erweiterung beim Start des Browsers. Der Erweiterungswert ist auf der Hilfeseite des Okta-Plug-ins verfügbar.
   - `ExtensionInstallBlocklist` – verhindert die Installation bestimmter Erweiterungen. Verwenden Sie einen *-Wert, um standardmäßig alle Erweiterungen zu verhindern. Administratoren können auf der `ExtensionInstallAllowlist` steuern, welche Erweiterungen zugelassen werden sollen.

- `ExtensionInstallAllowlist` ermöglicht Ihnen die Installation bestimmter Erweiterungen. Da `ExtensionInstallBlocklist` auf * festgelegt ist, fügen Sie hier den Okta-Plug-in-Wert hinzu, um dies zuzulassen.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie zum Aktivieren des Okta-Plug-ins:

```
"ExtensionInstallBlocklist": {
    "value": [
        "*",
        ]
},
"ExtensionInstallAllowlist": {
    "value": [
        "glnpjglilkicbckjpbgcfkogebgllemb",
       ]
},
"ExtensionSettings": {
    "value": {
        "glnpjglilkicbckjpbgcfkogebgllemb": {
            "installation_mode": "force_installed",
            "update_url": "https://clients2.google.com/service/update2/crx",
            "toolbar_pin": "force_pinned"
    }
}
```

Schritt 5: Laden Sie Ihre JSON-Datei für Richtlinien auf Ihr Webportal hoch

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unter. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. Wählen Sie WorkSpaces Secure Browser und anschließend Webportale aus.
3. Wählen Sie Ihr Webportal und dann Bearbeiten aus.
4. Wählen Sie Richtlinieneinstellungen und anschließend JSON-Datei-Upload aus.
5. Wählen Sie Datei auswählen aus. Navigieren Sie zu Ihrer JSON-Datei, wählen Sie sie aus und laden Sie sie hoch.
6. Wählen Sie Speichern.

Bearbeiten der grundlegenden Browserrichtlinie im Amazon WorkSpaces Secure Browser

Um den Service bereitzustellen, wendet WorkSpaces Secure Browser eine grundlegende Browserrichtlinie auf alle Portale an. Diese Basisrichtlinie wird zusätzlich zu den Richtlinien angewendet, die Sie in der Konsolenansicht oder beim JSON-Upload angeben. Im Folgenden finden Sie eine Liste der Richtlinien, die vom Service im JSON-Format angewendet werden:

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

Kunden können an den folgenden Richtlinien keine Änderungen vornehmen:

- `DefaultDownloadDirectory` – diese Richtlinie kann nicht bearbeitet werden. Der Service überschreibt alle Änderungen an dieser Richtlinie.

- `DownloadDirectory` – diese Richtlinie kann nicht bearbeitet werden. Der Service überschreibt alle Änderungen an dieser Richtlinie.

Die Basislinie `URLAllowlist` und `URLBlocklist` die Richtlinien können nicht überschrieben werden. Beachten Sie, dass die JSON-Browser-Richtliniendatei, die Ihrem Webportal zugeordnet ist, diese Basisrichtlinien nicht enthält. Um eine vollständige Liste aller angewandten Richtlinien und ihrer Werte zu sehen, navigieren Sie in einer Remote-Browsing-Sitzung zu „chrome: //policy“.

Kunden können die folgenden Richtlinien für ihr Webportal aktualisieren:

- `DownloadRestrictions` – die Standardeinstellung ist auf 1 festgelegt, damit Downloads verhindert werden, die von Chrome Safe Browsing als bösartig eingestuft wurden. Weitere Informationen finden Sie unter Verhindern, dass Benutzer schädliche Dateien herunterladen. Sie können einen Wert von `0` bis `4` festlegen.

Konfiguration des Eingabemethoden-Editors für Amazon WorkSpaces Secure Browser

Ein Eingabemethoden-Editor (IME) ist ein Hilfsprogramm, das dem Endbenutzer Optionen zur Texteingabe in Sprachen bietet, die ein anderes Tastaturlayout als eine QWERTY-Tastatur verwenden. IMEs hilft Benutzern bei der Eingabe von Text in Sprachen mit größeren, komplexeren Sprachgruppen wie Japanisch, Chinesisch und Koreanisch. WorkSpaces Secure Browser-Sitzungen beinhalten standardmäßig IME-Unterstützung. Benutzer können alternative Sprachen über die IME-Symbolleiste in der Sitzung oder mithilfe von Tastenkombinationen auswählen.

Die folgenden Sprachen werden derzeit vom IME von WorkSpaces Secure Browser unterstützt:

- Englisch
- Vereinfachtes Chinesisch (Pinyin)
- Traditionelles Chinesisch (Bopomofo)
- Japanisch
- Koreanisch

Wenn Sie eine Sprache aus der IME-Symbolleiste auswählen möchten, führen Sie die folgenden Schritte aus:

1. Wählen Sie das Drop-down-Menü zur Sprachauswahl auf der rechten Seite der schwarzen oberen Bedienfeldleiste aus. In der Standardeinstellung zeigt die Auswahltaste en für Englisch an.
2. Wählen Sie im Drop-down-Menü die gewünschte Sprache aus.
3. Wählen Sie im Untermenü, das nach der Auswahl einer Sprache angezeigt wird, zusätzliche Sprachdetails aus.

Wenn Sie eine Sprache mithilfe von Tastenkombinationen auswählen möchten, verwenden Sie Folgendes:

- Alle Sprachen
  - Wenn Sie Shift+Control+Left Alt drücken, können Sie den IME vorwärts durchgehen (bzw. zum richtigen Tastaturlayout wechseln).
  - Verwenden Sie die Sprachauswahl in der oberen Bedienfeldleiste, um auf die Sprach- und Eingabeeinstellungen zuzugreifen. Falls nicht sichtbar, aktivieren Sie es über Werkzeugleiste → Einstellungen → Allgemein → Tastatureingabemethode.
- Japanisch
  - Für MacOS-Benutzer: Wenn Sie eine US-Eingabequelle verwenden, können Eingabeprobleme auftreten. Um dieses Problem zu lösen:
    1. Wähle auf deinem macOS eine japanische Eingangsquelle (z. B. Japanisch — Kana oder Japanisch — Romaji) anstelle der US-Eingangsquelle.
    2. Gehen Sie in der WorkSpaces Secure-Browser-Sitzung zu Werkzeugleiste → Einstellungen → Tastatur → Optionstasteneinstellung und wählen Sie die Option Option () als Remote-Alt-Taste verwenden (Mac) aus, um sicherzustellen, dass die Tastenkombinationen ordnungsgemäß funktionieren.
  - Eingabezeichen konvertieren
    - Um Zeichen in Hiragana umzuwandeln, drücken Sie. F6
    - Um Zeichen in Katakana umzuwandeln, drücken Sie. F7
    - Um Zeichen in Hankaku-Katakana (Katakana mit halber Breite) umzuwandeln, drücken Sie F8
    - Um Zeichen ins Lateinische zu konvertieren, drücken Sie. F10
    - Drücken Sie, um Zeichen in das lateinische Breitformat umzuwandelnF9.
  - Zwischen den Eingabemodi wechseln
    - Um von Hiragana zu Katakana zu wechseln, drücken Sie. Alt/Option+K

    - Um von Katakana zu Hankaku Katakana zu wechseln, drücken Sie. Alt/Option+K
    - Um von Hankaku Katakana (Katakana mit halber Breite) zurück zu Hiragana zu wechseln, drücken Sie. Alt/Option+K
    - Drücken Sie, um von einem beliebigen japanischen Modus oder von Wide Latin zu Latein zu wechseln. Alt/Option+L
    - Um von Latin zu Wide Latin zu Wide Latin zu wechseln, drücken SieAlt/Option+L.
    - Um von einem beliebigen Modus zu Direct Input zu wechseln, drücken SieHenkaku/Zenkaku key.
    - Um von Direct Input zurück zu Hiragana zu wechseln, drücken Sie. Henkaku/Zenkaku key
- Koreanisch
    - Zur Auswahl von Hangul drücken Sie Shift+Space.
    - Zur Auswahl von Hanja drücken Sie F9.

Um die Bildschirmtastatur in Ihren WorkSpaces Secure Browser-Sitzungen auszuschalten, wenden Sie sich an. Support

Konfiguration der sitzungsinternen Lokalisierung für Amazon WorkSpaces Secure Browser

Wenn ein Benutzer eine Sitzung startet, erkennt WorkSpaces Secure Browser die lokalen Browser-Sprach- und Zeitzoneneinstellungen des Benutzers und wendet sie auf die Sitzung an. Dies wirkt sich auf die Anzeigesprache während der Sitzung aus und trägt dazu bei, dass die angezeigte Uhrzeit mit der aktuellen Uhrzeit am Standort des Benutzers übereinstimmt.

Die Sitzungssprache wird in der folgenden Prioritätsreihenfolge festgelegt:

1. Die ForcedLanguagesRichtlinie in den Browsereinstellungen des Webportals. Weitere Informationen finden Sie unter ForcedLanguages.
2. Die lokale Browserspracheinstellung des Endbenutzers.
3. Der Standardwert ist Englisch (en-US).

Die Zeitzone wird durch die lokalen Zeitzoneneinstellungen bestimmt, die im Browser des Endbenutzers angegeben sind. Wenn die Zeitzoneneinstellung nicht gültig ist, wird UTC verwendet.

Die folgenden Komponenten in WorkSpaces Secure Browser unterstützen die Lokalisierung:

- WorkSpaces Anmeldeseite für Secure Browser
- WorkSpaces Statusmeldungen des Secure Browser-Portals (einschließlich Meldungen und Fehler beim Laden)
- Chrome-Browser
- Kontextmenü des Systems und das Fenster Speichern unter

Topics

Unterstützte Sprachcodes für Amazon WorkSpaces Secure Browser

Die folgende Liste zeigt die Sprachcodes, die derzeit von WorkSpaces Secure Browser unterstützt werden. Wenn der lokale Browser des Benutzers so eingestellt ist, dass er einen nicht unterstützten Sprachcode verwendet, wird für die Sitzung standardmäßig Englisch (en-US) verwendet.

- Deutsch
  - de – Deutsch
  - de-AT – Deutsch (Österreich)
  - de-DE – Deutsch (Deutschland)
  - de-CH – Deutsch (Schweiz)
  - de-LI – Deutsch (Liechtenstein)
- Englisch
  - en – Englisch
  - en-AU – Englisch (australisch)
  - en-CA – Englisch (Kanada)
  - en-IN – Englisch (Indien)
  - en-NZ – Englisch (Neuseeland)
  - en-ZA – Englisch (Südliches Afrika)
  - en-GB – Englisch (Großbritannien und Nordirland)
  - en-US – Englisch (USA)
- Spanisch

  - es – Spanisch
  - es-AR – Spanisch (Argentinien)
  - es-CL – Spanisch (Chile)
  - es-CO – Spanisch (Kolumbien)
  - es-CR – Spanisch (Costa Rica)
  - es-HN – Spanisch (Honduras)
  - es-419 – Spanisch (lateinamerikanisch)
  - es-MX – Spanisch (Mexiko)
  - es-PE – Spanisch (Peru)
  - es-ES – Spanisch (Spanien)
  - es-US – Spanisch (Vereinigte Staaten)
  - es-UY – Spanisch (Uruguay)
  - es-VE – Spanisch (Venezuela)
- Französisch
  - fr – Französisch
  - fr-CA – Französisch (Kanada)
  - fr-FR – Französisch (Frankreich)
  - fr-CH – Französisch (Schweiz)
- Indonesisch
  - id – Indonesisch
  - id-ID – Indonesisch (Indonesien)
- Italienisch
  - it – Italienisch
  - it-IT – Italienisch (Italien)
  - it-CH – Italienisch (Schweiz)
- Japanisch
  - ja – Japanisch
  - ja-JP – Japanisch (Japan)
- Koreanisch
  - ko – Koreanisch

  - ko-KR – Koreanisch (Korea)
- Portugiesisch
  - pt – Portugiesisch
  - pt-BR – Portugiesisch (Brasilien)
  - pt-PT – Portugiesisch (Portugal)
- Chinesisch
  - zh – Chinesisch
  - zh-CN – Chinesisch (China)
  - zh-HK – Chinesisch (Hongkong)
  - zh-TW – Chinesisch (Taiwan)

Auswahl von Sprachen in den Browsereinstellungen des Benutzers

Gehen Sie wie folgt vor, um die lokalen Browsereinstellungen eines Benutzers festzulegen.

- Wählen Sie in Chrome Einstellungen und dann Sprachen aus. Ordnen Sie die Sprachen dann nach Ihren Wünschen.
- Wählen Sie in Firefox Einstellungen, Allgemein, Sprache und die Sprache aus dem Drop-down-Menü aus.
- Wählen Sie in Edge Einstellungen und dann Sprachen aus. Ordnen Sie die Sprachen dann nach Ihren Wünschen.

Verwaltung von IP-Zugriffskontrollen im Amazon WorkSpaces Secure Browser

> **Important**
>
> Es werden nur IP-Zugriffskontrollen unterstützt IPv4. Benutzer, die IPv6 nur von Netzwerken aus eine Verbindung herstellen, werden blockiert.

WorkSpaces Mit Secure Browser können Sie steuern, von welchen IP-Adressen aus auf Ihr Webportal zugegriffen werden kann. Mit IP–Zugriffseinstellungen können Sie Gruppen

vertrauenswürdiger IP-Adressen definieren und verwalten und Benutzern nur dann Zugriff auf ihr Portal gewähren, wenn sie mit einem vertrauenswürdigen Netzwerk verbunden sind.

Standardmäßig ermöglicht WorkSpaces Secure Browser Benutzern den Zugriff auf ihr Webportal von überall aus. Eine IP-Zugriffskontrollgruppe fungiert als virtuelle Firewall, die filtert, mit welcher IP-Adresse ein Benutzer eine Verbindung mit dem Webportal herstellen kann. Bei Zuweisung zu Ihrem Webportal erkennen die IP-Zugriffseinstellungen die Benutzer-IP vor der Authentifizierung, um festzustellen, ob sie für eine Verbindung berechtigt sind. Sobald die Verbindung hergestellt ist, überwacht WorkSpaces Secure Browser kontinuierlich die IP-Adresse eines Benutzers, um sicherzustellen, dass er über ein vertrauenswürdiges Netzwerk verbunden bleibt. Wenn sich die IP-Adresse eines Benutzers ändert, erkennt WorkSpaces Secure Browser die Sitzung und beendet sie.

Fügen Sie Regeln zu Ihrer IP-Zugriffskontrollgruppe hinzu und ordnen die Gruppe dann Ihrem Webportal zu, um die CIDR-Adressbereiche anzugeben. Sie können jede IP-Zugriffseinstellung mindestens einem Webportal zuordnen. Um die öffentlichen IP-Adressen und IP-Adressbereiche für Ihre vertrauenswürdigen Netzwerke anzugeben, fügen Sie den IP-Zugriffskontrollgruppen Regeln hinzu. Wenn Ihre Benutzer über ein NAT-Gateway oder VPN auf ihr Webportal zugreifen, müssen Sie Regeln erstellen, die den Datenverkehr von den öffentlichen IP-Adressen für das NAT-Gateway oder VPN zulassen.

> **Note**
>
> Kunden sind dafür verantwortlich, die potenziellen rechtlichen Probleme zu verstehen, die sich aus der Verwendung von WorkSpaces Secure Browser ergeben, und müssen sicherstellen, dass ihre Nutzung von WorkSpaces Secure Browser allen geltenden Gesetzen und Vorschriften entspricht. Dazu gehören Gesetze, die die Fähigkeit eines Arbeitgebers regeln, die Nutzung des WorkSpaces Secure Browsers durch einen Mitarbeiter zu überwachen, einschließlich der Aktivitäten, die innerhalb der Anwendung ausgeführt werden.

Topics

Eine IP-Zugriffskontrollgruppe im Amazon WorkSpaces Secure Browser erstellen

> **Important**
>
> Es werden nur IP-Zugriffskontrollen unterstützt IPv4. Benutzer, die IPv6 nur von Netzwerken aus eine Verbindung herstellen, werden blockiert.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu erstellen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollen aus.
3. Wählen Sie IP-Zugriffskontrollgruppe erstellen aus.
4. Geben Sie im Dialogfeld IP-Zugriffskontrollgruppe erstellen einen Namen (erforderlich) und eine Beschreibung (optional) für die Gruppe ein.
5. Geben Sie die IP-Adresse oder den CIDR-IP-Bereich ein, den Sie der Quelle zuordnen möchten, und eine Beschreibung (optional).
6. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
7. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, klicken Sie auf Speichern.

Zuordnen einer IP-Zugriffseinstellung zu einem Webportal im Amazon WorkSpaces Secure Browser

> **Important**
>
> Es werden nur IP-Zugriffskontrollen unterstützt IPv4. Benutzer, die IPv6 nur von Netzwerken aus eine Verbindung herstellen, werden blockiert.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe einem vorhandenen Webportal zuzuordnen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im linken Navigationsbereich die Option Webportale aus.
3. Wählen Sie das Webportal aus und klicken Sie auf Bearbeiten.
4. Wählen Sie unter IP-Zugriffskontrollgruppe die IP-Zugriffskontrollgruppen für das Webportal aus.
5. Wählen Sie Speichern.

Gehen Sie folgendermaßen vor, um bei Erstellung eines Webportals eine IP-Zugriffskontrollgruppe zuzuordnen.

1. Führen Sie in the section called “Portaleinstellungen” die Schritte 1 bis 4 aus, um auf IP-Zugriffskontrolle (optional) zuzugreifen.
2. Wählen Sie IP-Zugriffskontrollen erstellen aus.
3. Geben Sie im Dialogfeld IP-Gruppe erstellen einen Namen (erforderlich) und eine Beschreibung (optional) für die Gruppe ein.
4. Geben Sie die IP-Adresse oder den CIDR-IP-Bereich ein, den Sie der Quelle zuordnen möchten, und eine Beschreibung (optional).
5. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
6. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, wählen Sie IP-Zugriffskontrolle erstellen aus.
7. Ihre IP-Zugriffskontrollgruppe wird beim Start diesem Webportal zugeordnet.

Bearbeiten einer IP-Zugriffskontrollgruppe im Amazon WorkSpaces Secure Browser

Sie können eine Regel für eine IP-Zugriffseinstellung jederzeit löschen. Wenn Sie eine Regel entfernen, die verwendet wurde, um eine Verbindung mit einem Webportal zuzulassen, werden alle Benutzer mit einer aktuellen Sitzung vom Webportal getrennt.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu bearbeiten.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollen aus.

3. Markieren Sie die Gruppe und wählen Sie Edit (Bearbeiten) aus.
4. Bearbeiten Sie die vorhandenen Regeln Quelle und Beschreibung (optional) oder fügen Sie zusätzliche Regeln hinzu.
5. Wählen Sie unter Tags aus, ob ein Schlüsselwertpaar für jede IP-Zugriffskontrollgruppe markiert werden soll.
6. Wenn Sie mit dem Hinzufügen von Regeln und Tags fertig sind, klicken Sie auf Speichern.
7. Wenn Sie eine vorhandene IP-Zugriffseinstellung aktualisiert haben, warten Sie bis zu 15 Minuten, bis die neue oder bearbeitete Regel wirksam wird.

Löschen einer IP-Zugriffskontrollgruppe im Amazon WorkSpaces Secure Browser

Sie können eine Regel für eine IP-Zugriffskontrollgruppe jederzeit löschen. Wenn Sie eine Regel entfernen, die verwendet wurde, um eine Verbindung mit einem Webportal zuzulassen, werden alle Benutzer mit einer aktuellen Sitzung vom Webportal getrennt.

Gehen Sie folgendermaßen vor, um eine IP-Zugriffskontrollgruppe zu löschen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im Navigationsbereich IP-Zugriffskontrollgruppen aus.
3. Wählen Sie die Gruppe aus und wählen Sie Löschen aus.

Verwaltung der Single Sign-On-Erweiterung im Amazon WorkSpaces Secure Browser

Sie können eine Erweiterung für Ihre Endbenutzer aktivieren, um die Portalanmeldung zu verbessern. Wenn Sie Okta beispielsweise als SAML-2.0-Identitätsanbieter (IDP) Ihres Portals und auch als Identitätsanbieter für die Websites verwenden, die Benutzer während einer Sitzung besuchen sollen, können Sie das Okta-Anmelde-Cookie mit der Erweiterung an die Sitzung übergeben. Wenn Benutzer anschließend eine Website besuchen, für die das Okta-Domain-Cookie erforderlich ist, können sie auf die Website zugreifen, ohne sich während der Sitzung anmelden zu müssen.

Die Erweiterung wird in den Browsern Chrome und Firefox unterstützt. Die Erweiterung ermöglicht die Cookie-Synchronisierung für die zulässigen Domains von der Benutzeranmeldung bis zur Sitzung.

Die Erweiterung erfordert nicht, dass sich der Benutzer anmeldet. Sie aktiviert im Hintergrund die Cookie-Synchronisierung, ohne dass der Benutzer nach der Installation irgendwelche Aktionen ausführen muss. Die Erweiterung speichert keine Daten.

Standardmäßig sind Erweiterungen in Chrome in Inkognito-Fenstern oder Firefox-Fenstern für privates Surfen nicht aktiviert. Benutzer können sie manuell aktivieren. Weitere Informationen zu Chrome finden Sie unter Erweiterungen im Inkognitomodus. Weitere Informationen zu Firefox finden Sie unter Erweiterungen im privaten Surfen.

Benutzer werden aufgefordert, die Erweiterung zu installieren, wenn sie sich bei einem Portal anmelden. Einzelheiten zum Benutzererlebnis mit der Erweiterung finden Sie unter the section called “Single-Sign-On-Erweiterung”.

Topics

- Identifizieren von Domains für die Single Sign-On-Erweiterung im Amazon WorkSpaces Secure Browser
- Hinzufügen der Single Sign-On-Erweiterung zu einem neuen Webportal im Amazon WorkSpaces Secure Browser
- Hinzufügen der Single Sign-On-Erweiterung zu einem vorhandenen Webportal im Amazon WorkSpaces Secure Browser
- Die Single Sign-On-Erweiterung im Amazon WorkSpaces Secure Browser bearbeiten oder entfernen

Identifizieren von Domains für die Single Sign-On-Erweiterung im Amazon WorkSpaces Secure Browser

Stellen Sie zunächst fest, welche Domains Sie für Ihren SAML-Identitätsanbieter und Ihre Websites benötigen. Sie können bis zu 10 Domains angeben.

Sie sind dafür verantwortlich, die entsprechende Domain für die zu synchronisierenden Cookies zu testen und zu identifizieren. Möglicherweise sind Änderungen auf der Ebene der Identitätsanbieter- oder Website-Authentifizierung erforderlich, um sicherzustellen, dass Single Sign-On erwartungsgemäß funktioniert.

In der folgenden Tabelle können Sie sehen, welche Domains für den gängigsten IdP verwendet werden sollten:

IdP und Domains

IdP	Domain
Okta	okta.com
ID eingeben	microsoftonline.com
AWS Identity Center	awsapps.com
Ein Login	onelogin.com
Duo	duosecurity.com

Hinzufügen der Single Sign-On-Erweiterung zu einem neuen Webportal im Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um die Erweiterung beim Erstellen eines neuen Webportals zuzulassen.

1. Folgen Sie den Anweisungen unter the section called “Erstellung eines Webportals”, bis Sie zu the section called “Benutzereinstellungen” gelangen.
2. Wählen Sie für Schritt 1 von the section called “Benutzereinstellungen” unter Benutzerberechtigungen die Option Zugelassen aus, um die Erweiterung für Ihr Webportal zu aktivieren.
3. Geben Sie die Domain für die Cookie-Synchronisierung ein und wählen Sie Neue Domain hinzufügen aus.
4. Führen Sie die Schritte unter the section called “Benutzereinstellungen” aus und schließen Sie die verbleibenden Abschnitte unter the section called “Erstellung eines Webportals” ab, um Ihr Webportal zu erstellen.

Hinzufügen der Single Sign-On-Erweiterung zu einem vorhandenen Webportal im Amazon WorkSpaces Secure Browser

Gehen Sie folgendermaßen vor, um die Erweiterung zu einem vorhandenen Webportal hinzuzufügen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole zu https://console.aws.amazon.com/workspaces-web/Hause.

2. Wählen Sie das zu bearbeitende Webportal aus.
3. Wählen Sie Benutzereinstellungen, Benutzerberechtigungen und Zugelassen aus, um die Erweiterung für Ihr Webportal zu aktivieren.
4. Geben Sie die Domain für die Cookie-Synchronisierung ein und wählen Sie Neue Domain hinzufügen aus.
5. Speichern Sie Ihre Portaländerungen. Die Portale fordern die Benutzer auf, die Erweiterung innerhalb von 15 Minuten zu installieren.

Die Single Sign-On-Erweiterung im Amazon WorkSpaces Secure Browser bearbeiten oder entfernen

Gehen Sie wie folgt vor, um Domains zu bearbeiten oder die Erweiterung zu entfernen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole zu https://console.aws.amazon.com/workspaces-web/Hause.
2. Wählen Sie das zu bearbeitende Webportal aus.
3. Wählen Sie Benutzereinstellungen, Benutzerberechtigungen und Nicht zugelassen aus, um die Erweiterung für Ihr Webportal zu entfernen.
4. Entfernen oder bearbeiten Sie einzelne Domains.
5. Nach dem Entfernen synchronisieren Sitzungen keine Cookies mehr, auch wenn der Benutzer die WorkSpaces Secure Browser-Erweiterung in seinem Browser installiert hat.

Filterung von Webinhalten im Amazon WorkSpaces Secure Browser

Die Web-Inhaltsfilterung ist eine Sicherheits- und Compliance-Funktion, mit der Ihr Unternehmen Richtlinien definieren und den Zugriff auf Inhalte im WorkSpaces Secure Browser regulieren kann. Mit der Web-Inhaltsfilterung können Sie festlegen, welche URLs Endbenutzer auf bestimmte Kategorien oder Domänenkategorien zugreifen URLs oder diese blockieren dürfen, um den Zugriff einzuschränken und so wichtige Sicherheits- und Compliance-Anforderungen zu erfüllen.

> **Note**
>
> Sie können zwar URL-Filterrichtlinien über Chrome-Richtlinien einrichten, um bestimmte Domains zu blockieren oder zuzulassen, wir empfehlen diesen Ansatz jedoch nicht, da

Aktionen aus Chrome-Richtlinien nicht im Rahmen der Dienstprotokollierungsfunktionen erfasst werden. Verwenden Sie die auf dieser Seite beschriebenen Richtlinien zur Filterung von Webinhalten, um umfassende Überwachungs- und Compliance-Berichte zu erhalten.

Topics

Beschränken Sie das Surfen auf bestimmte URLs

Sie können eine „Standardverweigerung“ -Richtlinie implementieren, nach der nur ausdrücklich genehmigte Websites zugänglich URLs sind. Sie eignet sich ideal für Hochsicherheitsumgebungen, in denen der Internetzugang streng kontrolliert werden muss und alle zugelassenen Websites auf ihre geschäftlichen Erfordernisse und die Einhaltung von Sicherheitsbestimmungen überprüft wurden.

Gehen Sie in der AWS Konsole unter URL-Filterung wie folgt vor:

- Navigieren Sie zur Blockliste und wählen Sie den Schalter Alle blockieren URLs
- Klicken Sie unter Zulassungsliste auf URL hinzufügen, um eine URL hinzuzufügen, die für Ihren Endbenutzer zugelassen wird. Fügen Sie einen Eintrag pro URL hinzu.
- Klicken Sie auf Speichern

Spezifisch blockieren URLs

Sie können Sicherheit und Produktivität in Einklang bringen, indem Sie einen offenen Internetzugang aufrechterhalten und gleichzeitig bekannte problematische Websites blockieren. Es eignet sich für Unternehmen, die ihren Benutzern vertrauen, aber den Zugriff auf bestimmte Bedrohungen oder unangemessene Inhalte verhindern möchten, ohne legitime Geschäftsaktivitäten übermäßig einzuschränken.

Gehen Sie in Ihrer AWS Konsole unter URL-Filterung wie folgt vor:

- Navigiere zu Blockiert URLs
- Wählen Sie URL hinzufügen und geben Sie die URL ein, die blockiert werden soll. Fügen Sie pro URL, die Sie blockieren möchten, einen Eintrag hinzu
- Klicken Sie auf Speichern

Kategorien blockieren

Sie können nicht nur bestimmte Gruppen blockieren URLs, sondern auch automatisch Gruppen blockieren, die auf Inhaltskategorien URLs basieren. Dies ist nützlich für Unternehmen, die einen umfassenden Schutz vor verschiedenen Arten von unangemessenen oder riskanten Inhalten benötigen, ohne einzelne Websites manuell identifizieren und blockieren zu müssen.

Gehen Sie in Ihrer AWS Konsole unter URL-Filterung wie folgt vor:

- Navigieren Sie zu Blockierte Kategorien und klicken Sie auf Kategorien hinzufügen
- Wählen Sie eine Kategorie aus, die Sie blockieren möchten
- Sie können Ausnahmen von diesen Kategorien festlegen, indem URLs Sie sie der Zulassungsliste hinzufügen. Klicken Sie dazu auf URL hinzufügen und geben Sie entry/ies die URL ein, die URLs Sie zulassen möchten. Auch wenn sie in den Kategorien enthalten sind, können Endbenutzer die besuchen URLs.
- Klicken Sie auf Speichern

Die folgenden Kategorien können ausgewählt werden. Sie können eine, mehrere oder alle Kategorien auswählen.

Verfügbare Filterkategorien

Thema	Kategorie	Description
Inhalte für Erwachsene und unangemessene Inhalte	Nacktheit	Websites mit nicht-sexuellen Aktbildern oder Kunstwerken.
Inhalte für Erwachsene und	Pornografie	Websites mit explizitem sexuellem Inhalt oder provokativem Nacktmaterial.

Thema	Kategorie	Description
unangemessene Inhalte		
Inhalte für Erwachsene und unangemessene Inhalte	Sexualerziehung	Altersgerechte, medizinisch geprüfte Ressourcen für Gesundheit und Sexualität.
Inhalte für Erwachsene und unangemessene Inhalte	Geschmacklos	Inhalte, die für Kinder ungeeignet sind, die nicht unter andere Kategorien fallen.
Kommunikation und Soziales	Chat	Plattformen für Gruppen- und Privatnachrichten in Echtzeit.
Kommunikation und Soziales	Sofortnachrichten	Private Messaging-Dienste.
Kommunikation und Soziales	Professionelles Netzwerk	Geschäftsorientierte Plattformen zum Aufbau von Beziehungen.
Kommunikation und Soziales	Soziale Netzwerke	Plattformen für Benutzerinteraktionen zum Teilen persönlicher Inhalte und Erfahrungen.
Kommunikation und Soziales	Webbasierte E-Mail	Über den Browser zugängliche Messaging-Dienste, einschließlich E-Cards und Begrüßungssysteme.
Unterhaltung	Games	Ressourcen für Freizeitspiele, einschließlich Videospiele, Puzzles und Aktivitäten, die nichts mit Glücksspielen zu tun haben.
Unterhaltung	Teilen von Bildern	Plattformen für visuelle Inhalte, die Funktionen zum Hosten, Suchen und Teilen bieten.
Unterhaltung	Gleichgesinnte	Anbieter von Filesharing-Anwendungen und zugehörige Softwaretools.

Thema	Kategorie	Description
Schädlicher und illegaler Inhalt	Kriminelle Aktivitäten	Anweisungen oder Materialien zur Förderung illegaler Handlungen.
Schädlicher und illegaler Inhalt	Hacken	Unbefugte Tools für den Systemzugriff und Ressourcen zur Netzwerkausnutzung.
Schädlicher und illegaler Inhalt	Illegale Droge	Inhalte, die den Konsum von Drogen oder Drogenmis sbrauch in der Freizeit fördern.
Schädliche und illegale Inhalte	Illegale Software	Unautorisierte Verbreitung von urheberrechtlich geschützt em Material und bösartiger Software.
Schädlicher und illegaler Inhalt	Gewalt	Inhalte, die körperliche Schäden fördern oder Bildmaterial zeigen.
Schädlicher und illegaler Inhalt	Waffen	Ressourcen zur legitimen Nutzung von Sport- und Freizeitwaffen.
Verhalten mit hohem Risiko	Kulte	Spirituelle und metaphysische Inhalte, die nicht zum Mainstream gehören.
Verhalten mit hohem Risiko	Glücksspiel	Aktivitäten und Informationen im Zusammenhang mit Wetten.
Verhalten mit hohem Risiko	Hass und Intoleranz	Inhalte, die Vorurteile gegenüber geschützten Merkmalen fördern.
Verhalten mit hohem Risiko	Betrug in der Schule	Unbefugte Dienste zur akademischen Unterstützung und Erledigung von Hausaufgaben.
Verhalten mit hohem Risiko	Selbstverletzung	Inhalte, die selbstzerstörerisches Verhalten fördern oder erörtern.
Technologie und KI	Websites herunterladen	Hosting-Plattformen für Software, Anwendungen und digitale Assets.
Technologie und KI	Generative KI	Technologieressourcen für KI und maschinelles Lernen.

Thema	Kategorie	Description
Technologie und KI	Geparkte Domains	Domains mit minimalem Inhalt, die für Werbung oder Domainverkäufe verwendet werden.
Technologie und KI	Streaming-Medien und Downloads	Plattformen für Audio-/Videoinhalte, darunter Musik, Videos und Internetradio.

Beispiel für URLs

Die folgenden Typen von URLs können im AllowedUrls oder angegeben werden BlockedUrls

Typ	Beispiel
Domain	example.com
Unterdomain	login.example.com
Pfad	example.com/myvideos
Abfrageparameter	example.com/? Parameter=123

Chrome-Richtlinien werden übertragen

Falls Sie bereits Chrome-Richtlinien eingerichtet haben, um bestimmte Domains zuzulassen oder zu blockieren, empfehlen wir Ihnen, diese auf die Funktion zur Filterung von Webinhalten zu übertragen.

Die Funktion zur Filterung von Webinhalten erkennt alle URLAllow URLBlock Richtlinien, die für eine WorkSpaces Secure Browser-Sitzung gelten, und meldet dies in der AWS Konsole.

So übertragen Sie die Chrome-Richtlinien für URLAllowlist und/oder URLBlocklist:

- Klicken Sie in Ihrer AWS Konsole unter URL-Filterung auf Chrome-Richtlinien überprüfen (wenn Sie die Schaltfläche Chrome-Richtlinien überprüfen nicht sehen, bedeutet das, dass derzeit keine Chrome-Richtlinien für URL-Zulassen gelten oder URLBlock)
- Lesen Sie unter dem Overlay die Chrome-Richtlinien
- Klicken Sie auf Transfer

Die Chrome-Richtlinien werden aus dem JSON-Editor unter Richtlinieneinstellungen entfernt und neue URLs werden automatisch zur Funktion zur Filterung von Webinhalten hinzugefügt.

Deeplinks im Amazon WorkSpaces Secure Browser

Wenn sich ein Benutzer bei WorkSpaces Secure Browser anmeldet, startet er die Sitzung auf einer vom Administrator festgelegten Startseite. Sie können Portalen auch ermöglichen, Deep-Links zu empfangen, die Benutzer während einer Sitzung mit einer bestimmten Website verbinden. Wenn ein Deep-Link ausgewählt ist, zeigt das Portal die im Deep-Link angegebene URL an. Der Link wird neben den Homepages angezeigt, die für den Sitzungsstart konfiguriert sind, oder eigenständig, falls bereits eine Sitzung läuft. Diese Funktion ermöglicht es Administratoren, dynamischere Benutzererlebnisse mit WorkSpaces Secure Browser zu schaffen.

Deep-Links öffnen Seiten in einer WorkSpaces Secure Browser-Sitzung. Wenn bereits eine Sitzung läuft, wird der Deep-Link in einer neuen Registerkarte geöffnet. Wenn noch keine Sitzung läuft, wird die Deep-Link-URL auf einer neuen Registerkarte und die Standardstartseite des Portals auf einer separaten Registerkarte geöffnet. Wenn ein Deep-Link mehr als eine URL enthält, wird die zuerst aufgeführte Deep-Link-URL im Fokus angezeigt, wobei jede nachfolgende URL (einschließlich der Standard-Homepage) in separaten Tabs geöffnet wird.

Topics

Deep-Links im Amazon WorkSpaces Secure Browser einrichten

Um die Erlaubnis für Deep-Links zuzulassen, wählen Sie bei der Erstellung von Benutzereinstellungen die Option Zulässig aus. Die Site, zu der Sie einen Deeplink erstellen möchten, muss URL-kodiert sein. Um beispielsweise einen Benutzer mit „/?“ zu verknüpfen https://www.example.com query=true“, aktualisieren Sie den Link auf %2F%3Fquery%3Dtrue. https%3A%2F%2Fwww.example.com

Ein Deeplink kann bis zu 10 enthalten, die durch ein Komma getrennt sind. URLs Beispiel:

<uuid>https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue, %2F%3Fquery%3Dtrue2, %2F%3Fquery%3Dtrue3, %2F%3Fquery%3Dtrue3, %2F%3Fquery%3Dtrue4. https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com

Weitere Hinweise zum Zulassen von Deep-Links finden Sie unter. the section called “Benutzereinstellungen”

Verwenden der URL-Filterung für Deep-Links im Amazon WorkSpaces Secure Browser

Jeder Benutzer, mit dem Sie diesen Portal-Link teilen, kann den Deep-Link-Wert manipulieren, um eine Website zu besuchen, sofern diese Domain vom Portal aus erreichbar ist und nicht auf der URL-Blockliste steht. Verwenden Sie die URL-Filterung, um eine restriktive Zulassungs- oder Sperrliste zu erstellen, um zu verhindern, dass Benutzer unbeabsichtigte Domains mit Ihrem Portal besuchen.

Die Zulassungs- und Sperrliste für ein Portal können mithilfe der URL-Filterung in den Browsereinstellungen Ihres Portals bearbeitet werden. <uuid>Fügen Sie dazu die URL im folgenden Format an eine Portal-URL auf der Zulassungsliste an, wobei UUID die Portal-ID ist: https://.workspaces-web.com/? deepLinks= %2F%3Fquery%3Dtrue https%3A%2F %2Fwww.example.com

Weitere Informationen the section called “Filterung von Webinhalten” finden Sie unter Zugriff auf Websites zulassen oder blockieren.

Verwenden des Sitzungsverwaltungs-Dashboards im Amazon WorkSpaces Secure Browser

Verwenden Sie das Sitzungsverwaltungs-Dashboard auf Ihrer WorkSpaces Secure Browser-Konsole, um aktive und abgeschlossene Sitzungen zu überwachen und zu verwalten.

Zugriff auf das Dashboard

Gehen Sie wie folgt vor, um auf das Dashboard zuzugreifen.

Um auf das Dashboard zuzugreifen

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale und wählen Sie Ihr Webportal aus.
3. Wählen Sie die Registerkarte „Sitzung“ oder „Sitzungen anzeigen“, um das Dashboard in einem geteilten Bereich darunter zu öffnen.

Dashboard-Filter

Im Sitzungsbereich können Sie Sitzungen nach den folgenden Eigenschaften oder Werten filtern:

- Status
  - Aktiv — Zeigt an, dass gerade eine Sitzung läuft. Informationen zum Beenden der Sitzung finden Sie weiter unten.
  - Beendet — Zeigt an, dass eine Sitzung nicht mehr aktiv ist.
- Sitzungs-ID
- Username
- Startzeit der Sitzung

Sitzungen beenden

Gehen Sie wie folgt vor, um eine Sitzung zu beenden.

Um eine Sitzung zu beenden

1. Wählen Sie im Sitzungs-Dashboard die Sitzung aus, die Sie beenden möchten.
2. Wähen Sie Beenden.
3. Getrennte Benutzer verlieren den gesamten Status der Sitzung. Alle geöffneten Tabs, der Browserverlauf und die in den sicheren Browser heruntergeladenen Dateien werden recycelt.

Verlauf der Sitzung

Das Dashboard enthält Sitzungen der letzten 35 Tage. Sie können die CLI verwenden, um Sitzungen mit oder ohne Filter aufzulisten. Der Sitzungsverlauf wird als JSON bereitgestellt, das Administratoren in einem separaten Repository verarbeiten, verwalten und speichern können.

Im Folgenden finden Sie CLI-Beispielbefehle für die Verwaltung von Sitzungen in der Region US-West-2 (Oregon).

Führen Sie den folgenden Befehl aus, um alle Sitzungen für ein Webportal aufzulisten:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>

Um alle Sitzungen für einen bestimmten Benutzer eines Webportals aufzulisten, führen Sie den folgenden Befehl aus:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>

Schutz von Daten während der Übertragung mit FIPS-Endpunkten und Amazon Secure Browser WorkSpaces

Wenn Sie als Administrator über die Konsole, die AWS Befehlszeilenschnittstelle (AWS CLI) oder ein AWS SDK oder während einer Benutzersitzung mit dem WorkSpaces Secure Browser Service kommunizieren, werden alle übertragenen Daten standardmäßig mit TLS 1.2 verschlüsselt.

Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Wenn Sie einen FIPS-Endpunkt verwenden, werden alle übertragenen Daten mithilfe kryptografischer Standards verschlüsselt, die dem Federal Information Processing Standard (FIPS) 140-3 entsprechen. Informationen zu FIPS-Endpunkten, einschließlich einer Liste von Secure Browser-Endpunkten, finden Sie unter. WorkSpaces https://aws.amazon.com/compliance/fips

Nachdem ein Portal mit FIPS-Endpunkten erstellt wurde, werden alle Benutzersitzungen und administrativen Änderungen automatisch mithilfe von FIPS 140-3-Endpunkten vorgenommen. Sie können die `AWS_USE_FIPS_ENDPOINT=true` Umgebungsvariable verwenden, um FIPS-Endpunkte zu finden und Anfragen mit dem SDK zu senden. Im Folgenden wird ein -Beispiel gezeigt.

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

Sie können die `–endpoint-url` Option auch verwenden, um Anfragen direkt an FIPS-Endpunkte zu senden. Im Folgenden finden Sie ein Beispiel für Anruflistenportale in der Region US-West-2 (Oregon):

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-west-2.amazonaws.com
```

Verwaltung der Datenschutzeinstellungen im Amazon WorkSpaces Secure Browser

Datenschutzeinstellungen werden verwendet, um zu verhindern, dass Daten während einer Sitzung geteilt werden. Einstellungen können erstellt und auf mehrere Portale angewendet werden.

Topics

Inline-Datenredaktion im Amazon WorkSpaces Secure Browser

Indem Sie einem Portal Inline-Datenschwärzung hinzufügen, können Sie bestimmte Daten anhand einer Textfolge, die auf Webseiten angezeigt wird, automatisch vorhersagen und unkenntlich machen. Sie können Richtlinien für die Schwärzung erstellen, indem Sie aus integrierten Mustern (wie Sozialversicherungsnummern oder Kreditkartennummern) wählen oder eigene benutzerdefinierte Datentypen mit regulären Ausdrücken und Schlüsselwörtern erstellen. Zu den Richtlinien gehören konfigurierbare Durchsetzungsebenen und Kontrollen für die Bereiche, URLs in denen die Schwärzung durchgesetzt werden soll.

Die folgenden Komponenten bestimmen, wann Daten geschwärzt werden:

- Datenschutzeinstellungen — Datenschutzeinstellungen ist der Name der Ressource, die Ihre Datentypen und Durchsetzungskriterien enthält. Um diese Ressource zu verwenden, erstellen Sie zunächst Ihre Einstellungen und ordnen Sie sie dann einem Portal zu. Wenn Benutzer eine Sitzung starten, werden Ihre Einstellungen während der Sitzung durchgesetzt.
- Browsererweiterung während der Sitzung — Wenn Sie Ihrem Portal Schwärzungseinstellungen zuordnen, wird der Sitzungsbrowser mit einer vom System erzwungenen Browsererweiterung gestartet, die Ihre Einstellungen durchsetzt. In den Datenschutzeinstellungen wird die

Schwärzung durch Musterabgleich (reguläre Ausdrücke) und Stichwortsuche entsprechend Ihrem Vertrauensniveau und der Konfiguration der URL-Durchsetzung erzwungen. Der Inhalt wird anhand von Textzeichenfolgen vorhergesagt und geschwärzt, bevor er auf dem Bildschirm angezeigt wird. Die Erweiterung legt auch zugehörige Browserrichtlinien fest, die die Fähigkeit der Benutzer regeln, Schwärzungen zu umgehen (z. B. deaktiviertes privates Surfen, Zugriff auf Entwicklertools und Netzwerkinspektion).

Die folgenden Änderungen der Chrome-Browserrichtlinie werden durch die Browsererweiterung während der Sitzung durchgesetzt. Weitere Informationen finden Sie in der Liste der Chrome-Unternehmensrichtlinien.

- Setzen Sie die Browserrichtlinie durch, um zu verhindern, dass Benutzer die Sitzung ohne Schwärzung ansehen:
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled= falsch
  - BrowserGuestModeEnabled= falsch
- Die Erweiterung verhindert außerdem, dass Benutzer HTML-Dateien herunterladen, die Datenschutzeinstellungen durchsetzen URLs , indem das Download-Ereignis abgebrochen wird.

Im Allgemeinen sollten Sie die Schwärzung bei privaten, strukturierten Websites (wie Ihren Kundenverwaltungstools, Ticketsystemen oder Wikis) und nicht bei unstrukturiertem öffentlichen Surfen (wie Facebook oder Google) verwenden. Sie können zwischen integrierten Datentypen wählen (die vollständige Liste finden Sie unten) oder benutzerdefinierte Datentypen mit Ihren eigenen Werten und Schlüsselwörtern für reguläre Ausdrücke definieren. Administratoren sind dafür verantwortlich, zu testen und zu überprüfen, ob die einzelnen Datentypen, die Vertrauensstufen und die URL-Durchsetzung erwartungsgemäß funktionieren. AWS kann die Kompatibilität mit benutzerdefinierten Websites oder Anwendungen, die von Drittanbietern bereitgestellt werden, nicht garantieren.

WorkSpaces Secure Browser unterstützt derzeit nicht die Schwärzung unterstützter oder benutzerdefinierter Datentypen in Nicht-Textformaten, einschließlich Text in den folgenden Formaten:

- Bilder wie JPEG, PNG oder GIF
- Webseiten, die es Benutzern ermöglichen, dynamische Textverarbeitung oder -bearbeitung zu verwenden, z. B. Google Docs oder Sheets

- Audio- oder Videostreams, auf die im Browser zugegriffen wird, z. B. YouTube Videos
- PDFs vom Chrome-Browser angesehen

Verwenden Sie die Schwärzung nicht für Inhalte in einem Format, das nicht unterstützt wird. Administratoren sind dafür verantwortlich, die Kompatibilität von Website und Inhalt zu überprüfen, bevor sie Benutzern Zugriff auf Inhalte gewähren, die sie redigieren möchten.

Standardkonfiguration für Schwärzung im Amazon WorkSpaces Secure Browser

Die Standardkonfiguration für Schwärzung wendet automatisch ein Konfidenzniveau und die URL-Durchsetzung für alle in den Datenschutzeinstellungen integrierten Datentypen an. Sie haben die Möglichkeit, die Standardkonfiguration zu überschreiben, wenn Sie einen integrierten Datentyp hinzufügen.

Mithilfe von Konfidenzstufen können Sie die Schwärzungslogik für integrierte Datentypen mithilfe einer Kombination aus Format, Schlüsselwörtern und unformatiertem Text feinabstimmen. Wählen Sie die Schärfegrad für die Schwärzung aus, z. B. Hoch, Mittel oder Niedrig. Der Standardwert gilt für alle Datentypen, es sei denn, auf Datentypebene wird eine Überschreibung vorgenommen. Im Allgemeinen sollten Sie mit einer Standardkonfiguration von Medium beginnen und diese verfeinern, indem Sie überprüfen, ob die Schwärzung auf Ihren Websites erwartungsgemäß durchgesetzt wird.

Konfidenzniveau	Description	Beispiel
Hoch	Erfordert eine Übereinst immung mit dem formatierten Textmuster, damit der Inhalt redigiert werden kann.	Die SSN 123-45-6798 würde redigiert werden, 123456789 nicht.
Mittel	Bei der Schwärzung werden sowohl formatierter als auch unformatierter Text berücksichtigt und der Logik ein Schlüsselwort zugeordnet.	Die SSN 123-45-6798 würde geschwärzt werden. 123456789 würde geschwärz t, wenn sie in der Nähe eines Schlüsselworts (z. B. „Sozialve rsicherungsnummer“) entdeckt würde.

Konfidenzniveau	Description	Beispiel
Niedrig	Die Schwärzung wurde sowohl für formatierte Muster als auch für unformatierte Muster ohne Schlüsselwort erzwungen.	SSN in beiden Formaten — 123-45-6798 und 123456789 — werden redigiert, ohne dass ein Schlüsselwort erforderlich ist.

Sie müssen die Standardkonfiguration für die Schwärzung für alle Datentypen festlegen. Sie können aus den folgenden Optionen wählen:

- Alle URLs
- Spezifisch URLs
- Erweiterte Konfiguration

Der Standardwert gilt für alle Datentypen, sofern keine Überschreibung auf Datentypebene angewendet wird. Die URL-Durchsetzung verwendet eine ähnliche Logik wie die Chrome-Richtlinie für die Verwaltung von Zulassungs- und Sperrlisten. Anleitungen zur Verwendung von Blockieren und Zulassen URLs finden Sie unter Zugriff auf Websites zulassen oder blockieren. Die besten Ergebnisse erzielen Sie, wenn Sie diese Listen URLs entsprechend dem Blocklisten-Filterformat von Chrome ergänzen. Weitere Informationen finden Sie unter URL-Sperrlisten-Filterformat.

Einfache Inline-Schwärzung im Amazon WorkSpaces Secure Browser

Die Inline-Datenschwärzung unterstützt integrierte Muster (wie Sozialversicherungsnummern und Kreditkartennummern), die Sie unter Inline-Schwärzung in der Basisversion finden. Wählen Sie die Datentypen aus dem Drop-down-Menü aus und geben Sie den Ersatzwert für jeden Datentyp an. Alle Datentypen folgen dem oben genannten Standardmuster zur Durchsetzung der Konfiguration. Sie können jedoch festlegen, dass das Konfidenzniveau außer Kraft gesetzt und das Muster für die Domänendurchsetzung für jeden Datentyp fein abgestimmt werden soll.

Um einen alternativen Wert aus der Standardkonfiguration einzugeben, wählen Sie Confidence Level Override. Wenn die Standardkonfiguration beispielsweise auf Mittel eingestellt ist, stellen Sie beim Testen möglicherweise fest, dass einer Ihrer Datentypen nicht zuverlässig geschwärzt wird. Sie können die Überschreibung auf Niedrig setzen, um die Wahrscheinlichkeit einer Schwärzung zu erhöhen, ohne die für Ihre anderen Datentypen verwendete Logik anzupassen.

Um die Art und Weise, wie Schwärzung angewendet wird, zu verfeinern, URLs ohne die Standardkonfiguration zu ändern, wenden Sie URL-Erzwingungsüberschreibungen an. Sie können beispielsweise festlegen, dass URL-Überschreibungen verwendet werden, um die Schwärzung von E-Mail-Adressen in Ihrem Kundenbeziehungsmanagementsystem zu erzwingen, ohne den Benutzerzugriff auf E-Mail-Adressen auf der Unternehmensverzeichnis-Website oder auf webbasierten E-Mails zu unterbrechen.

Im Folgenden finden Sie eine Liste der Datentypen und der entsprechenden integrierten Muster: IDs

builtInPatternId	Datentyp
awsAccessKey:	AWS-Zugriffsschlüssel
awsSecretKey:	AWS-Geheimschlüssel
Kartennummern:	Kreditkartennummern
Krypto:	Adressen für Kryptowährungen
Kissen Num:	CUSIP-Nummer
Datum:	Date
Dean um:	US-DEA-Nummern
Hund:	Geburtsdatum
Führerschein:	US-Führerscheine
E-Mail-Adresse:	Email Address
ein:	US-Arbeitgeber-Identifikationsnummer
Verfallsdatum:	Ablaufdatum der Kreditkarte
healthInsuranceNum:	Antragsnummer der Medicare-Krankenversicherung
HIPAA-Code:	HIPAA-ICD-10-Kode
indivTaxId:	Individuelle US-Steuernummer

builtInPatternId	Datentyp
iPadDR:	IP-Adresse
ist in:	Internationale Wertpapier-Identifikationsnummern
jwt:	JSON Web Token
Standort Coord:	Koordinaten des Standorts
MacAddr:	MAC-Adresse
medicareBeneficiaryId:	Nummer des Medicare-Begünstigten
npi:	Identifikationsnummer des nationalen Anbieters
ndc:	Nationale Arzneimittelcodes (NDC)
Nummer des Reisepasses:	US-Passnummer
Telefonnummer:	Telefonnummer
Routing-Nummer:	ABA-Routing-Nummer
ssn:	US-Sozialversicherungsnummer
SwiftCode:	SWIFT-Code
Zeit:	Zeit
vin:	US-Fahrzeugidentifikationsnummer

Benutzerdefinierte Inline-Schwärzung im Amazon WorkSpaces Secure Browser

Kunden können mithilfe regulärer Ausdrücke ihre eigenen Muster definieren, z. B. eine benutzerdefinierte interne Anwendung IDs. Gehen Sie wie folgt vor, um Ihr benutzerdefiniertes Inline-Schwärzmuster zu erstellen:

1. Gehen Sie zu Ihrer Datenschutzeinstellung.
2. Wählen Sie Benutzerdefinierte Inline-Schwärzung und fügen Sie hinzu.
3. Geben Sie einen Namen für den benutzerdefinierten Datentyp ein.
4. Geben Sie den Wert Ihres regulären Ausdrucks ein.
   - Die Werte regulärer Ausdrücke müssen der Literalsyntax JavaScript regulärer Ausdrücke entsprechen. Weitere Informationen finden Sie unter Reguläre Ausdrücke. Ein Beispiel für einen regulären Ausdruck ist`/ex[am]+ple/i`.
   - Stellen Sie sicher, dass Sie Ihre benutzerdefinierten Muster auf den Websites testen, die Sie unterstützen möchten. Wenn benutzerdefinierte Muster fehlerhaft geschrieben werden, können sie zu unbeabsichtigten Leistungseinbußen führen.
5. Geben Sie den Ersatzwert an.
6. Wählen Sie Weitere Optionen für weitere optionale Anpassungen, einschließlich der folgenden:
   - Fügen Sie Stichwörter hinzu, um die Redaktionslogik zu optimieren. Schlüsselwörter können die Genauigkeit der Durchsetzung erhöhen. Fügen Sie Schlüsselwörter in der Literalsyntax für reguläre Ausdrücke in Javascript hinzu. Weitere Informationen finden Sie unter Reguläre Ausdrücke.

     Wenn Sie beispielsweise ein benutzerdefiniertes Schwärzungsmuster für einen Client erstellen, der in einem internen System IDs verwendet wird, können Sie das Schlüsselwortfeld erweitern, `/client name/i` um die Scan- und Erkennungslogik zu beeinflussen.
   - Wenden Sie Überschreibungen zur URL-Durchsetzung an, um die Art und Weise, wie Schwärzung überall angewendet wird, zu optimieren URLs, ohne die Standardkonfiguration zu ändern.

     Sie können beispielsweise festlegen, dass URL-Überschreibungen verwendet werden, um die Schwärzung von E-Mail-Adressen in Ihrem Kundenbeziehungsmanagementsystem zu erzwingen, ohne den Benutzerzugriff auf E-Mail-Adressen auf der Unternehmensverzeichnis-Website oder in webbasierten E-Mails zu unterbrechen.
   - Geben Sie eine Beschreibung (optional) für den Datentyp ein.

Datenschutzeinstellungen im Amazon WorkSpaces Secure Browser erstellen

Sie können Datenschutzeinstellungen im WorkSpaces abgesicherten Browser erstellen.

Um Datenschutzeinstellungen zu erstellen

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im linken Navigationsbereich Datenschutzeinstellungen aus.
3. Wählen Sie Datenschutzeinstellungen erstellen.
4. Geben Sie einen Anzeigenamen (erforderlich) und eine Beschreibung (optional) für die Einstellung ein.
5. Wählen Sie die Standardeinstellungen für Inline-Schwärzung aus. Sie können Folgendes festlegen:
   - Der Grad der Strenge aller Datentypen
   - Die Domänen, für die die Schwärzung durchgesetzt werden sollte
6. Wählen Sie aus den unterstützten Typen Ihre Basisdatentypen für die Inline-Schwärzung aus, oder erstellen Sie einen benutzerdefinierten Datentyp. Sie können Überschreibungen für jeden Datentyp festlegen, einschließlich der Strenge und der Domain-Ausnahmen.
7. Fügen Sie beliebige Tags (optional) für die Berichterstattung hinzu.
8. Klicken Sie abschließend auf Save.

Datenschutzeinstellungen im Amazon WorkSpaces Secure Browser verknüpfen

Sie können Datenschutzeinstellungen im WorkSpaces abgesicherten Browser verknüpfen.

Um eine Datenschutzeinstellung einem vorhandenen Portal zuzuordnen

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie im linken Navigationsbereich Webportale aus.
3. Wählen Sie das Webportal aus und klicken Sie auf Bearbeiten.
4. Wählen Sie unter Datenschutzeinstellungen die Einstellung für Ihr Portal aus.
5. Wählen Sie Speichern.

Gehen Sie folgendermaßen vor, um beim Erstellen eines neuen Portals eine Datenschutzeinstellung zuzuordnen.

Um beim Erstellen eines neuen Portals eine Datenschutzeinstellung zuzuordnen

1. Folgen Sie den Anweisungen the section called “Erstellung eines Webportals” unter So erstellen Sie ein Portal, bis Sie zur Datenschutzeinstellung gelangen.
2. Wählen Sie Ihre Datenschutzeinstellung aus dem Drop-down-Menü aus.
3. Führen Sie die Schritte unter austhe section called “Erstellung eines Webportals”, um die Erstellung Ihres Portals abzuschließen.

Gehen Sie folgendermaßen vor, um beim Erstellen eines neuen Portals eine Datenschutzeinstellung zu erstellen.

Um beim Erstellen eines neuen Portals eine Datenschutzeinstellung zu erstellen

1. Folgen Sie den Anweisungen the section called “Erstellung eines Webportals” unter So erstellen Sie ein Portal, bis Sie zur Datenschutzeinstellung gelangen.
2. Wählen Sie Datenschutzeinstellungen aus dem Drop-down-Menü aus.
3. Geben Sie einen Anzeigenamen (erforderlich) und eine Beschreibung (optional) für die Einstellung ein.
4. Wählen Sie die Standardeinstellungen für Inline-Schwärzung aus. Sie können Folgendes festlegen:
   - Der Grad der Strenge aller Datentypen
   - Die Domänen, für die die Schwärzung durchgesetzt werden sollte
5. Wählen Sie aus den unterstützten Typen Ihre Basisdatentypen für die Inline-Schwärzung aus, oder erstellen Sie einen benutzerdefinierten Datentyp. Sie können Überschreibungen für jeden Datentyp festlegen, einschließlich der Strenge und der Domain-Ausnahmen.
6. Fügen Sie beliebige Tags (optional) für die Berichterstattung hinzu.
7. Klicken Sie abschließend auf Save.
8. Klicken Sie unter Datenschutzeinstellungen auf die Schaltfläche „Aktualisieren“ und wählen Sie dann Ihre Datenschutzeinstellung aus dem Drop-down-Menü aus.
9. Folgen Sie weiterhin den Anweisungen zum Erstellen eines Portals, um die Erstellung Ihres Portals abzuschließen.

Datenschutzeinstellungen im Amazon WorkSpaces Secure Browser bearbeiten

Sie können die Datenschutzeinstellungen im WorkSpaces abgesicherten Browser bearbeiten.

Um die Datenschutzeinstellungen zu bearbeiten

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie in der Listenansicht die Datenschutzeinstellungen und die Datenschutzeinstellung, die Sie bearbeiten möchten.
3. Sie können den Namen, die Beschreibung, die Standardeinstellungen und die Datentypen (unterstützt oder benutzerdefiniert) aktualisieren und die Vertrauensstufe oder die Domäne überschreiben.
4. Wählen Sie Speichern.

Datenschutzeinstellungen im Amazon WorkSpaces Secure Browser löschen

Sie können die Datenschutzeinstellungen im WorkSpaces abgesicherten Browser löschen.

Um Datenschutzeinstellungen zu löschen

1. Wenn Sie ein Portal mit einer Datenschutzeinstellung verknüpft haben, müssen Sie zuerst die Zuordnung entfernen, bevor Sie die Datenschutzeinstellung löschen.
2. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
3. Wählen Sie die Datenschutzeinstellungen und die Datenschutzeinstellung, die Sie löschen möchten, aus der Listenansicht aus.
4. Wählen Sie Löschen aus.

Anpassung des Brandings im Amazon WorkSpaces Secure Browser

Sie können die Anmelde- und Ladebildschirme, die Ihren Endbenutzern angezeigt werden, anpassen, indem Sie visuelle Elemente, Textinhalte und Nutzungsbedingungen ändern. Die Anpassung des Brandings trägt dazu bei, ein einheitliches Erlebnis zu schaffen, das der Identität Ihres Unternehmens entspricht.

Übersicht

Durch die Anpassung des Brandings können Sie die folgenden Aspekte der Benutzererfahrung personalisieren:

- Visuelle Elemente — Laden Sie Logo, Favicon und Hintergrundbild hoch und wählen Sie Farbthemen aus, die zu Ihrer Markenidentität passen.
- Textinhalt — Passen Sie Willkommensnachrichten, den Titel des Browser-Tabs und andere optionale Textfelder an, um Ihre Markensprache während des gesamten Anmeldevorgangs beizubehalten. Wenn Sie für bestimmte Felder keinen benutzerdefinierten Text angeben, wird Standardtext verwendet. Details hierzu finden Sie unter the section called “Richtlinien zur Anpassung”.
- Nutzungsbedingungen (optional) — Fügen Sie die Nutzungsbedingungen Ihrer Organisation hinzu, denen Benutzer zustimmen müssen, bevor sie eine Sitzung starten.

> **Note**
>
> Sie können auch den Domainnamen für Ihr Portal anpassen. Details hierzu finden Sie unter the section called “Benutzerdefinierte Domain”.

Topics

Konfiguration der Anpassung des Brandings für Ihr Portal

Funktionsweise

Wenn Sie die Anpassung des Brandings konfigurieren:

- Visuelle Elemente und Textelemente werden sowohl auf den Anmelde- als auch auf den Ladebildschirm angewendet.
- Auf der Browser-Registerkarte werden Ihr benutzerdefiniertes Favicon und Ihr benutzerdefinierter Titel angezeigt.
- Endbenutzer werden Ihre Anpassungsänderungen sehen, wenn sie eine neue Sitzung starten. In einigen Fällen kann es einige Minuten dauern, bis Ihre Änderungen sichtbar sind.
- Wenn die Nutzungsbedingungen konfiguriert sind, müssen Endbenutzer Ihre Nutzungsbedingungen akzeptieren, bevor sie ihre Streaming-Sitzung starten können. Beachten Sie, dass sie zu Beginn jeder Sitzung gefragt werden.

Voraussetzungen

Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Ändern der Portaleinstellungen verfügenthe section called “AWS verwaltete Richtlinien”. Weitere Informationen finden Sie unter.
- Bereiten Sie Ihre Branding-Assets (Logo, Favicon, Hintergrundbild) gemäß den Spezifikationen unter vorthe section called “Richtlinien zur Anpassung”.

Erste Schritte

Gehen Sie wie folgt vor, um die Anpassung des Brandings zu konfigurieren.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale und wählen Sie Ihr Webportal aus.
3. Wählen Sie Ihr Portal und dann die Registerkarte Benutzereinstellungen aus.
4. Wählen Sie im Bereich Branding-Anpassung die Option Bearbeiten aus.
5. Konfigurieren Sie die folgenden Abschnitte nach Bedarf:

- Im Inhaltseditor — Laden Sie alle visuellen Elemente (Ihr Firmenlogo, Ihr Favicon und ein optionales Hintergrundbild) hoch und wählen Sie das Farbdesign aus. Sie können die Dateien entweder von Ihrem lokalen Computer oder von einem S3-Bucket hochladen. Informationen zum Einrichten von S3-Bucket-Berechtigungen finden Sie unterthe section called “S3-Bucket-Berechtigungen einrichten”.
- Im Texteditor — Passen Sie den Text an, der auf dem Anmeldebildschirm angezeigt wird.
- Im Editor für Nutzungsbedingungen — Fügen Sie optional Bedingungen hinzu, die Benutzer bestätigen müssen.

6. Wählen Sie Änderungen speichern aus.

Detaillierte Anweisungen zu den einzelnen Anpassungsoptionen finden Sie unterthe section called “Richtlinien zur Anpassung”.

S3-Bucket-Berechtigungen einrichten

Sie können Branding-Dateien direkt von Ihrem Computer hochladen oder vorhandene Objekte aus Ihren S3-Buckets auswählen. Wenn Sie die Dateien für die visuellen Elemente (Ihr Firmenlogo, Ihr Favicon und ein Hintergrundbild) aus einem S3-Bucket hochladen möchten, stellen Sie sicher, dass Sie die richtigen Berechtigungen für den S3-Bucket einrichten.

Auswahl von S3-Objekten im selben Konto

Wenn Ihr IAM-Benutzer oder Ihre IAM-Rolle bereits über `s3:GetObject` Berechtigungen für den Bucket verfügt, der Ihre Branding-Assets enthält, ist keine zusätzliche Konfiguration erforderlich.

Auswahl von S3-Objekten in einem anderen Konto

Um einen S3-Bucket in einem anderen AWS Konto auszuwählen, müssen Sie sowohl die Bucket-Richtlinie im Quellkonto als auch die IAM-Richtlinie in Ihrem Administratorkonto konfigurieren.

Beispiel für eine Bucket-Richtlinie (im Quellkonto):

Wenden Sie diese Richtlinie auf den S3-Bucket im Quellkonto an. *123456789012*Ersetzen Sie sie durch Ihre Admin-Konto-ID und *source-account-bucket-name* durch Ihren tatsächlichen Bucket-Namen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

Beispiel für eine IAM-Richtlinie (in Ihrem Admin-Konto):

Fügen Sie diese Richtlinie dem IAM-Benutzer oder der IAM-Rolle in Ihrem Administratorkonto hinzu. *source-account-bucket-name*Ersetzen Sie es durch den tatsächlichen Bucket-Namen aus dem Quellkonto.

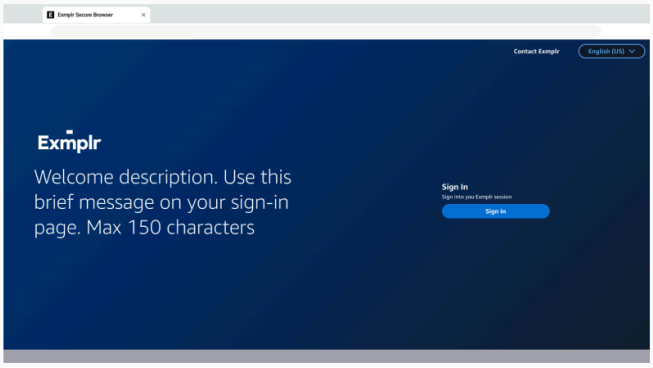
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
```

```
}
```

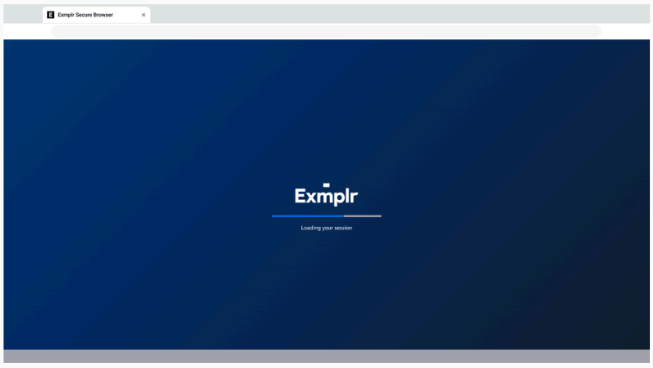
Ausführliche Informationen zum kontoübergreifenden Zugriff finden Sie unter S3 Access gewährt kontoübergreifenden Zugriff.

Richtlinien zur Anpassung

Passen Sie das Anmelde- und Ladeerlebnis für Ihre Endbenutzer an, indem Sie die Branding-Elemente und den Text auf den Anmelde- und Ladeseiten aktualisieren. Sie können visuelle Elemente wie Logos und Hintergrundbilder ändern, Textelemente wie Willkommensnachrichten und Kopfzeilen bearbeiten und optional eine Vereinbarung mit den Nutzungsbedingungen konfigurieren, die Benutzer akzeptieren müssen, bevor sie ihre Sitzung starten.



Sign in Page

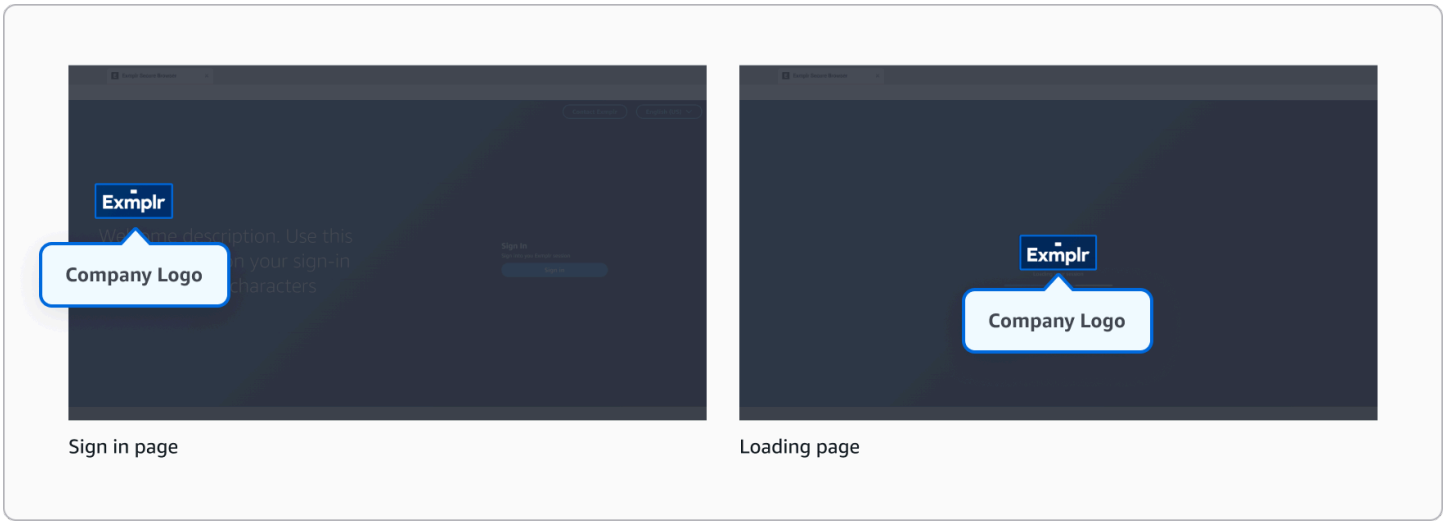


Loading Page

Inhaltseditor

Logo des Unternehmens

Das Logo erscheint auf dem Anmelde- und Ladebildschirm und sorgt so für ein einheitliches Branding in der gesamten Benutzerumgebung.

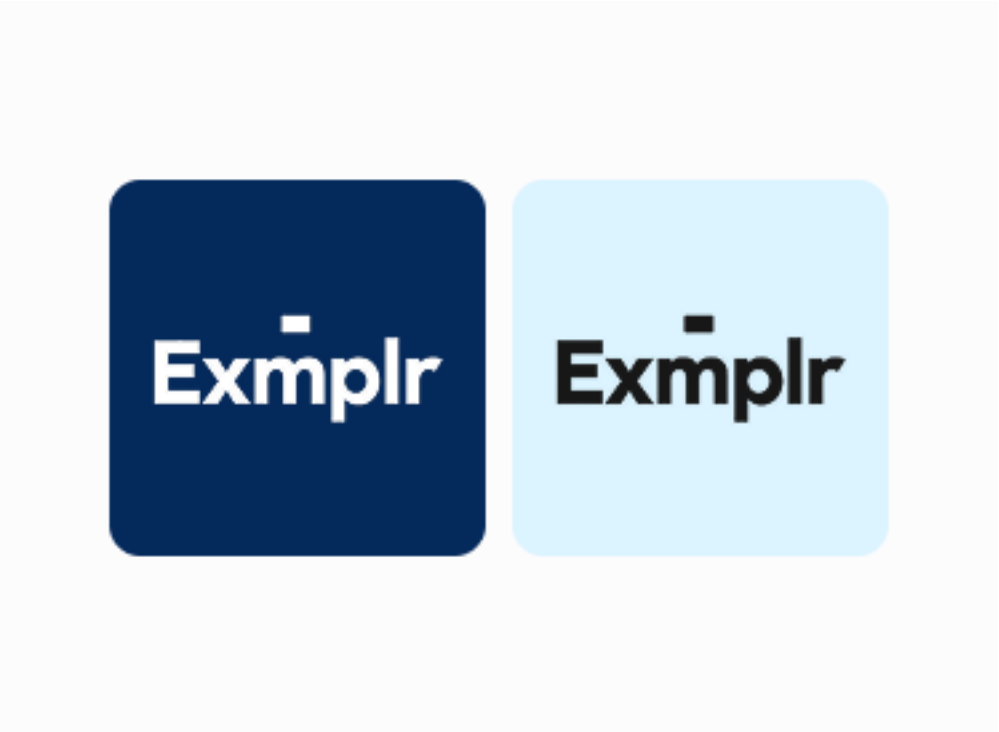


Sign in page

Loading page

- Unterstützte Formate: JPG oder ICO oder PNG
- Maximale Dateigröße: 100 KB

Tun



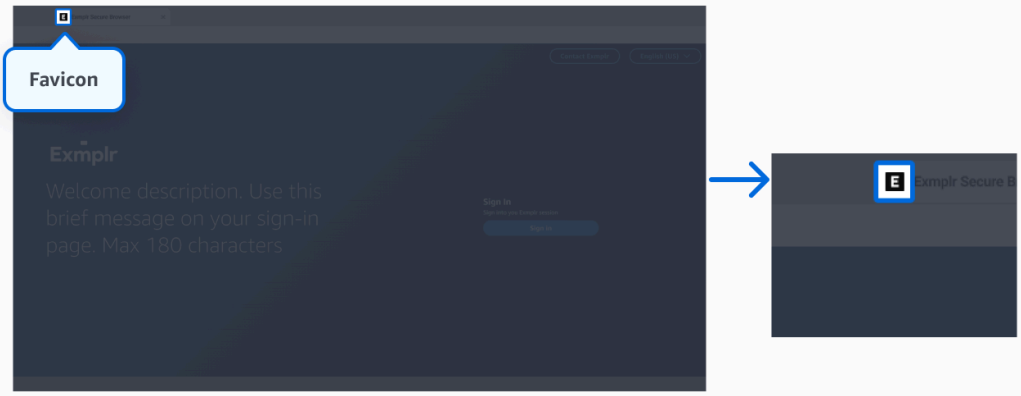
- Wenn Sie verschiedene Logo-Varianten haben (z. B. unterschiedliche Farben oder Stile), wählen Sie die, die den besten Kontrast zu Ihrem ausgewählten Hintergrundbild bietet.

Tun Sie das nicht

- Ignorieren Sie das Seitenverhältnis nicht, wenn Sie die Größe Ihres Logos ändern.
- Verwenden Sie keine Logos, die vorher nicht richtig dimensioniert wurden, da sie verzerrt aussehen könnten.

Favicon

Ein Favicon ist ein kleines Symbol, das in Browser-Tabs angezeigt wird und Benutzern hilft, Ihre Anwendung unter mehreren geöffneten Tabs zu identifizieren.



- Unterstützte Formate: JPG oder ICO oder PNG
- Maximale Dateigröße: 100 KB
- Empfohlenes Seitenverhältnis: 1:1

Hintergrundbild - optional

Das Hintergrundbild dient als Hintergrundbild auf allen Bildschirmen und sorgt so für ein einheitliches visuelles Erscheinungsbild. Wenn Sie kein benutzerdefiniertes Hintergrundbild hochladen, wird das unten abgebildete Standardhintergrundbild verwendet. Wählen Sie ein Bild, das zu Ihrem Branding passt, ohne die Lesbarkeit der Inhalte zu beeinträchtigen.

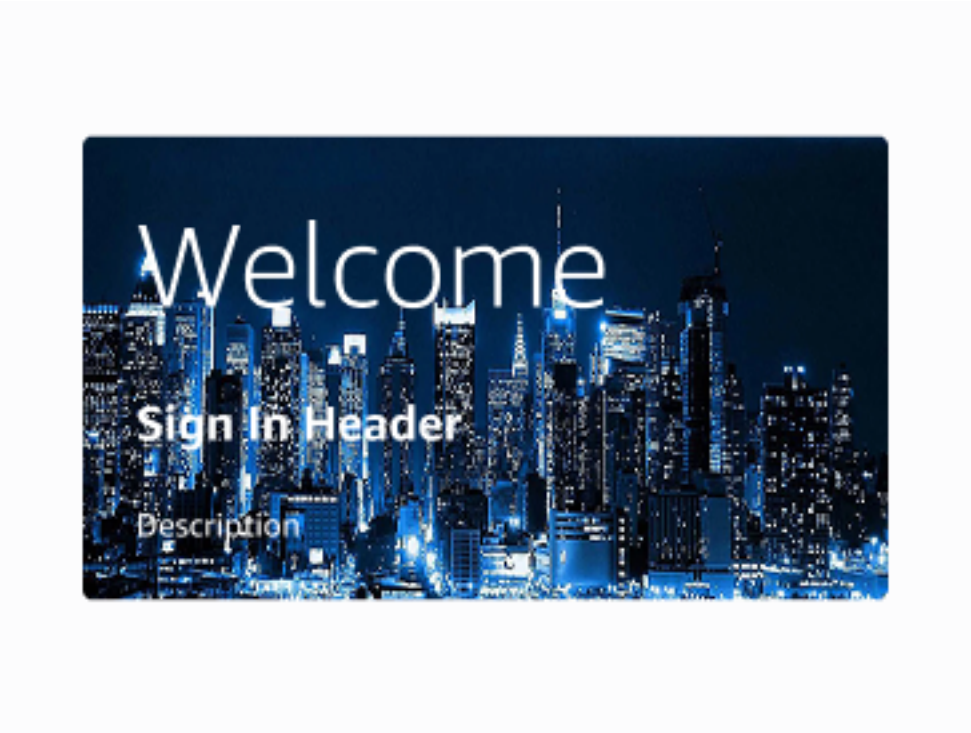
- Unterstützte Formate: JPEG oder PNG.
- Maximale Dateigröße: 5 MB

- Empfohlenes Seitenverhältnis: 16:9
- Empfohlene Mindestauflösung: 1920 x 1080

Tun

- Verwenden Sie dezente Hintergrundbilder mit geringem Kontrast oder verschwommene Bilder, die den Vordergrundinhalt nicht beeinträchtigen.
- Erwägen Sie eine voreingestellte Textplatzierung, um überfüllte Bereiche hinter dem Text zu vermeiden.
- Verwenden Sie Markenfarben und Überlagerungen, um den Kontrast und die Lesbarkeit zu verbessern.

Tun Sie das nicht



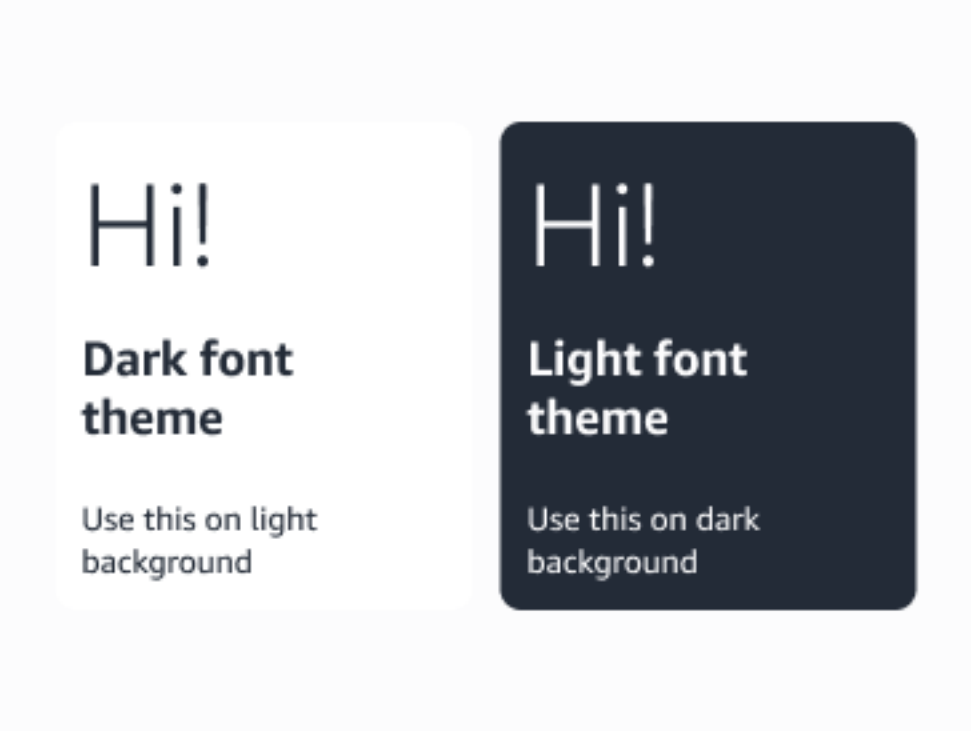
- Verwenden Sie keine stark frequentierten, gesättigten oder detailreichen Bilder direkt hinter wichtigem Text.
- Verwenden Sie keine visuell komplexen Bilder oder Bilder mit scharfen Übergängen, die zu Einschränkungen der Lesbarkeit an voreingestellten Textstellen führen könnten.
- Verlassen Sie sich nicht ausschließlich auf Farbe, um Text ohne ausreichenden Kontrast vom Hintergrund zu trennen.

Farbthema

Wählen Sie zwischen hellen und dunklen Themen, die sich auf Schriftarten, Schaltflächen und Modalitäten auswirken.

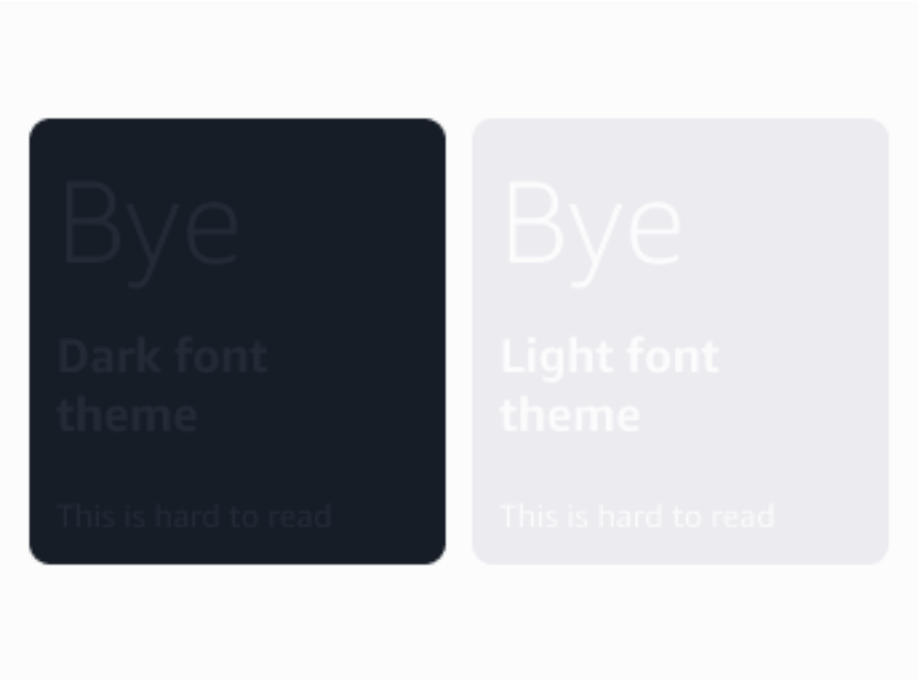
- Helles Design – Dieses Design eignet sich am besten für dunklere Hintergründe, sorgt für einen klaren Kontrast und reduziert die Belastung der Augen bei der Arbeit in Umgebungen mit wenig Licht.
- Dunkles Design – Optimal für helle Hintergründe, bietet eine komfortable Sicht und reduziert die Blendung in hellen Umgebungen.

Tun



- Achten Sie auf einen starken Kontrast zu Hintergrundelementen/Hintergrundbildern.
- Verwenden Sie ein dunkles Farbdesign auf hellem Hintergrund.
- Verwenden Sie ein helles Farbdesign auf dunklem Hintergrund.

Tun Sie das nicht



- Platzieren Sie keine hellen oder dunklen Schriften über Bildern oder komplexen Hintergrundbildern.

Text-Editor

Mit dem Text-Editor können Sie den Text anpassen, der auf dem Anmeldebildschirm Ihrer Endbenutzer angezeigt wird. Um die Anpassung des Brandings zu ermöglichen, müssen Sie mindestens eine Sprache hinzufügen.

Für neue Benutzer: Wir erkennen Ihre bevorzugte Browsersprache und zeigen die Portalseite in dieser Sprache an, wenn Sie sie in Ihren Branding-Sprachen konfiguriert haben. Wenn Ihre Browsersprache nicht in den von Ihnen konfigurierten Sprachen enthalten ist, verwenden wir standardmäßig Englisch (en-US), sofern verfügbar. Wenn Sie nicht Englisch konfiguriert haben, verwenden wir die erste Sprache in alphabetischer Reihenfolge aus Ihren konfigurierten Sprachen.

Für wiederkehrende Benutzer: Wir speichern Ihre Sprachpräferenz aus Ihrer vorherigen Sitzung in einem Browser-Cookie. Wenn diese Sprache in Ihren konfigurierten Branding-Sprachen enthalten ist, verwenden wir sie. Andernfalls folgen wir derselben Fallback-Logik: Englisch (en-US), falls verfügbar, oder die erste konfigurierte Sprache in alphabetischer Reihenfolge.

Die folgenden Gebietsschemata (Sprachcodes) werden unterstützt:

- Deutsch (de-DE)
- US-Englisch (en-US)

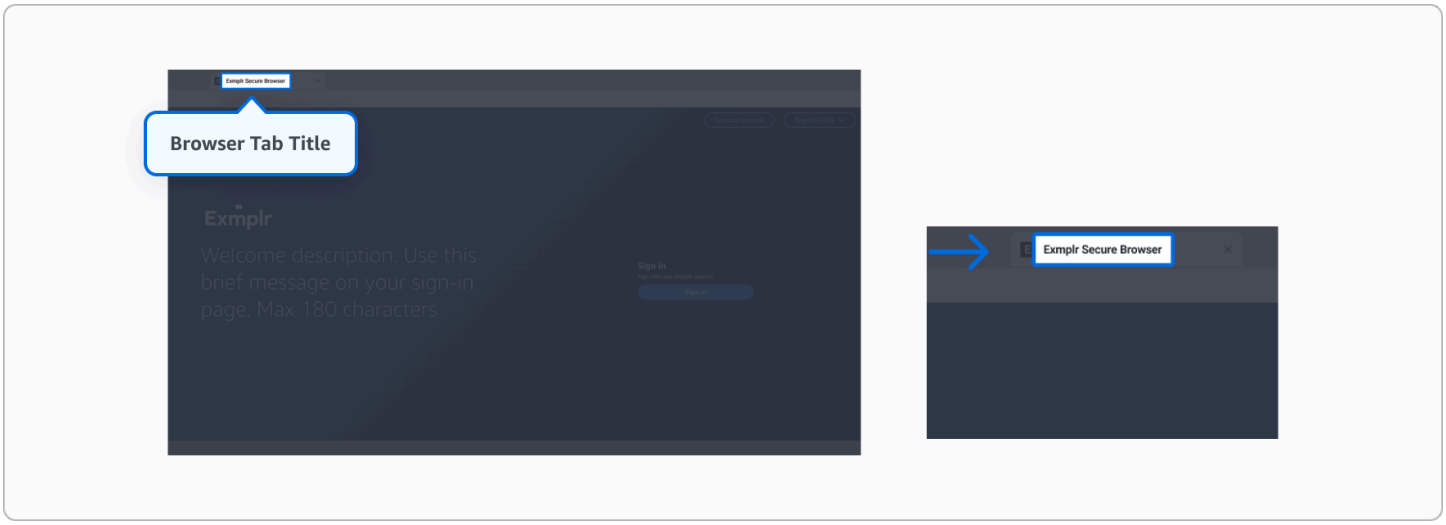
- Spanisch (es-ES)
- Französisch (fr-FR)
- Indonesisch (id-ID)
- Italienisch (it-IT)
- Japanisch (ja-JP)
- Koreanisch (ko-KR)
- Portugiesisch (pr-BR)
- Chinesisch – vereinfacht (zh-CN)
- Chinesisch – traditionell (zh-TW)

Aus Sicherheitsgründen sind die folgenden Zeichen in allen Textfeldern gesperrt:

- < (kleiner als)
- > (größer als)
- & (kaufmännisches Und)
- ' (gerader Apostroph)
- ` (Backtick/Gravis-Akzent)
- ~ (Tilde)
- \ (Umgekehrter Schrägstrich).

Titel des Browser-Tabs

Der Text, der auf der Browser-Registerkarte angezeigt wird. Maximal 25 Zeichen.

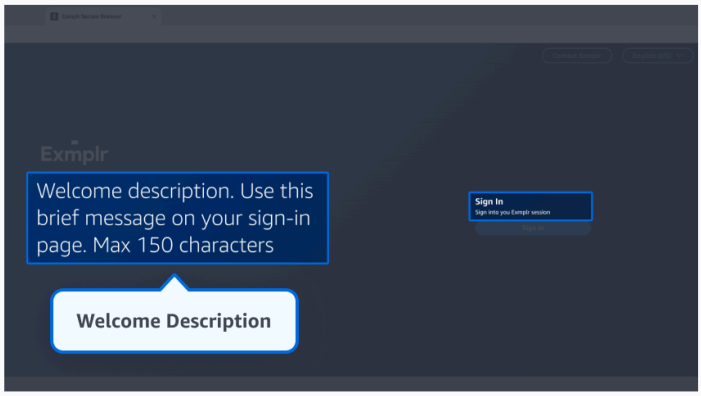


Empfehlung

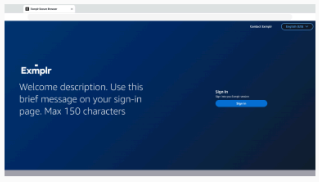
Erwägen Sie, kurze und klare Titel zu verwenden, damit sie auch dann lesbar bleiben, wenn mehrere Tabs geöffnet sind.

Willkommene Beschreibung

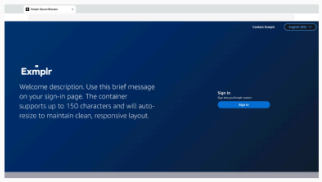
Eine kurze Beschreibung neben Ihrem Firmenlogo auf dem Anmeldebildschirm. Maximal 150 Zeichen.



Welcome description



Starting font sizing



Adapted sizing to Max characters

Empfehlung

Halten Sie den Text für eine bessere Lesbarkeit kurz. Beachten Sie, dass längerer Text automatisch auf eine kleinere Schriftgröße skaliert wird, während kürzere Nachrichten besser sichtbar angezeigt werden.

Bereich Kontakt

Kontaktschaltfläche – optional

Text der Kontaktschaltfläche auf dem Anmeldebildschirm. Wenn das Feld leer gelassen wird, wird „Kontaktieren Sie uns“ angezeigt. Maximal 30 Zeichen.

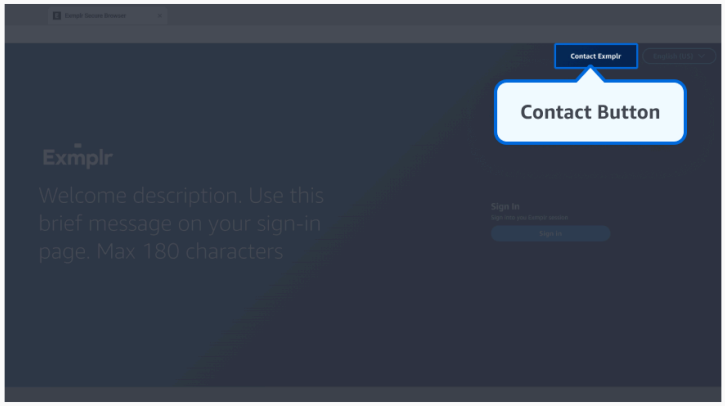
Kontaktlink – optional

Kontaktschaltflächenlink auf dem Anmeldebildschirm. Sie können Folgendes verwenden:

- Eine HTTPS-URL, um Benutzer zu einer Webseite weiterzuleiten

- Ein mailto:-Link zum Öffnen des E-Mail-Clients des Benutzers

Wenn das Feld leer gelassen wird, wird die Kontaktschaltfläche auf dem Bildschirm ausgeblendet.



Empfehlung

Halten Sie den Text kurz, idealerweise 2-3 Wörter.

Bereich „Anmelden“

Kopfzeile für die Anmeldung – optional

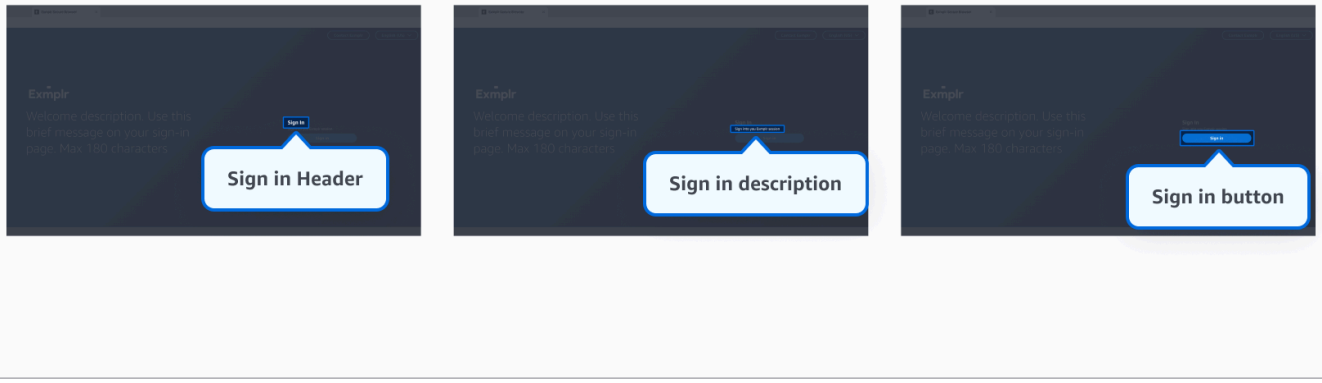
Kopfzeile für den Anmeldebereich der Anmeldeseite. Wenn das Feld leer gelassen wird, wird „Anmelden“ angezeigt. Maximal 100 Zeichen.

Beschreibung der Anmeldung – optional

Beschreibungstext für den Anmeldebereich. Wenn das Feld leer gelassen wird, wird „Melden Sie sich bei Ihrer WorkSpaces sicheren Browsersitzung an“ angezeigt. Maximal 250 Zeichen.

Schaltfläche „Anmelden“ – optional

Text, der auf der Anmeldeschaltfläche angezeigt wird. Wenn das Feld leer gelassen wird, wird „Anmelden“ angezeigt. Maximal 30 Zeichen.

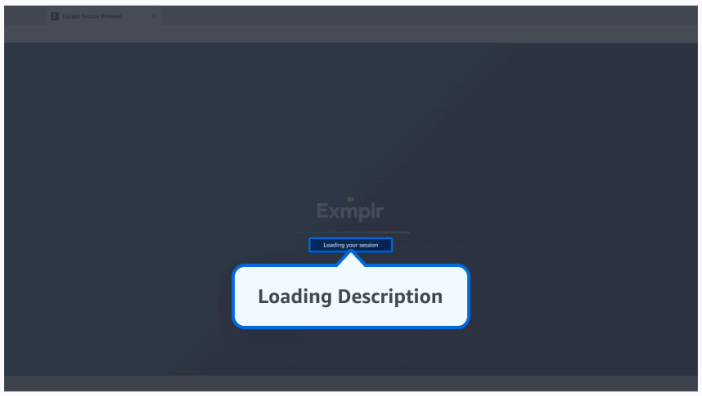


Empfehlungen

- Halten Sie den Text kurz.
- Bedenken Sie, dass die Anmeldeschaltfläche Benutzer zu dem für Ihr Portal konfigurierten Identitätsanbieter weiterleitet. Sie können den Schaltflächentext an Ihren spezifischen Identitätsanbieter anpassen.

Beschreibung wird geladen

Text, der während der Verbindung auf dem Ladebildschirm angezeigt wird. Wenn das Feld leer gelassen wird, wird „Verbindung wird hergestellt...“ angezeigt. Maximal 300 Zeichen.



Loading screen

Empfehlung

Diese Nachricht wird nur angezeigt, während die Sitzung geladen wird, sodass Endbenutzer möglicherweise keine Zeit haben, sie zu lesen. Vermeiden Sie es, es zu lang zu machen.

Servicebedingungen – optional

Sie können die Servicebedingungen so anpassen, dass Endbenutzer sie lesen und akzeptieren müssen, bevor sie eine Streaming-Sitzung starten. Dieser Inhalt kann entweder durch Hochladen einer Markdown-Datei oder mithilfe des integrierten Markdown-Editors hinzugefügt werden.

Den Benutzern werden nach erfolgreicher Anmeldung die Servicebedingungen angezeigt. Sie müssen das gesamte Dokument durchblättern und auf die Schaltfläche „Akzeptieren“ klicken, um mit ihrer Secure Browser-Sitzung fortzufahren. Wenn der Benutzer auf „Ablehnen“ klickt, wird er zurück zur Anmeldeseite weitergeleitet.

Beachten Sie, dass dies eine optionale Einstellung ist. Wenn Sie keine Servicebedingungen hinzufügen, werden Benutzer nach der Anmeldung direkt zu ihren Sitzungen weitergeleitet.

Unterstützte Formatierung:

- Grundlegende Textstile (fett, kursiv)
- Überschriften
- Geordnete und ungeordnete Listen
- Blockzitate
- Horizontale Linien
- Einfache Absätze und Zeilenumbrüche

Aus Sicherheitsgründen sind die folgenden Elemente blockiert:

- Skripts und Codeausführung
- Interaktive Elemente wie Formulare und Iframes
- Unsichere Protokolle und Dateipfade
- HTML-Attribute und Styling
- Externe Links und Tabellen

Beachten Sie, dass Ihre Datei mit den Servicebedingungen die Größe von 150 KB nicht überschreiten darf.

Aktivieren der WebAuthn Umleitungsunterstützung im Amazon WorkSpaces Secure Browser

> **Warning**
>
> WebAuthn Die Umleitung funktioniert nur in Browsersitzungen mit aktiviertem Internetzugang. Stellen Sie sicher, dass die Netzwerkeinstellungen Ihres Portals den Internetzugang zulassen, damit die WebAuthn Funktionen ordnungsgemäß funktionieren.

WorkSpaces Secure Browser unterstützt WebAuthn (Webauthentifizierung) für Websites, auf die innerhalb der Remote-Browsersitzung zugegriffen wird. Auf diese Weise können sich Benutzer mit ihren lokalen FIDO2 Sicherheitsschlüsseln, biometrischen Authentifikatoren und Plattformauthentifikatoren bei Websites authentifizieren, während sie in ihrer WorkSpaces Secure Browser-Sitzung surfen.

> **Note**
>
> WebAuthn Die Umleitung ist für Endnutzer verfügbar, die Google Chrome 136 (oder höher) oder Microsoft Edge 137 (oder höher) verwenden. Diese Funktion ist für Browser, die nicht zu Chromium gehören, wie Safari oder Firefox, nicht verfügbar.
> Um die WebAuthn Umleitungsfunktion zu aktivieren, müssen Administratoren beide konfigurieren:
>
> 1. Portalbenutzereinstellungen — Aktivieren Sie die WebAuthn Umleitung in den Portaleinstellungen
> 2. Lokale Browserrichtlinien für Endbenutzer — Konfigurieren Sie die WebAuthenticationRemoteDesktopAllowedOrigins Browserrichtlinie auf Benutzergeräten, um die Umleitung zu ermöglichen WebAuthn

Topics

Aktivierung der WebAuthn Umleitung in den Portaleinstellungen

Gehen Sie wie folgt vor, um die WebAuthn Umleitung für Websites zu aktivieren, auf die innerhalb der Remote-Browsersitzung zugegriffen wird.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unterhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Wählen Sie WorkSpaces Secure Browser, Webportale, wählen Sie Ihr Webportal aus und klicken Sie dann auf Bearbeiten.
3. Navigieren Sie zum Abschnitt Benutzereinstellungen.
4. Stellen Sie unter Benutzerberechtigungen die Option Benutzern erlauben, die lokale Authentifizierung in ihrer Portalsitzung zu verwenden, auf Zulässig ein.
5. Wählen Sie Speichern, um die Konfiguration anzuwenden.

Konfiguration der lokalen Browserrichtlinie für WebAuthn

Zusätzlich zur Aktivierung der WebAuthn Umleitung in Ihren Portaleinstellungen muss die lokale Browserrichtlinie so konfiguriert werden, dass sie die WebAuthn Umleitung zwischen dem lokalen Gerät des Benutzers und der Remote-Browsersitzung und umgekehrt ermöglicht. Diese Konfiguration wird in der Regel von IT-Administratoren für Unternehmensumgebungen oder von einzelnen Benutzern für BYOD-Szenarien verwaltet.

Die Browserrichtlinie muss die WorkSpaces Secure Browser-Inhaltsdomäne für Ihre Region enthalten. Fügen Sie der `WebAuthenticationRemoteDesktopAllowedOrigins` Richtlinie je nach Region den folgenden Ursprung hinzu:

`https://<region>.content.workspaces-web.com`

Zum Beispiel in us-west-2: `https://us-west-2.content.workspaces-web.com`

Die spezifische Konfigurationsmethode hängt davon ab, ob Sie Browser in einer Unternehmensumgebung verwalten oder einzelne Geräte für BYOD-Benutzer konfigurieren. Weitere Informationen zur Browserrichtlinie finden Sie in der Chrome Enterprise-Richtliniendokumentation und der Microsoft Edge-Richtliniendokumentation.

> **Note**
>
> Möglicherweise ist ein Neustart des Browsers erforderlich, damit die Richtlinie wirksam wird.

Verwendung der WebAuthn Umleitung in Remote-Browsersitzungen

Sobald die WebAuthn Umleitung in den Portaleinstellungen aktiviert und die lokale Browserrichtlinie konfiguriert ist, können Benutzer in ihren WorkSpaces Secure Browser-Remote-Browser-Sitzungen die WebAuthn Authentifizierung auf Websites verwenden.

Benutzer können sich auf Websites authentifizieren mit:

- FIDO2 Sicherheitsschlüssel, die mit ihrem lokalen Gerät verbunden sind
- Hauptschlüssel
- Plattformauthentifikatoren wie Windows Hello oder Touch ID

Der WebAuthn Authentifizierungsprozess wird nahtlos von der Remote-Browsersitzung an das lokale Gerät des Benutzers weitergeleitet, wodurch eine sichere kennwortlose Authentifizierung gewährleistet wird und gleichzeitig die Sicherheitsvorteile der Remote-Browsing-Umgebung erhalten bleiben.

Behebung von Problemen WebAuthn mit der Umleitung

Wenn Benutzer in ihren Remote-Browsersitzungen Probleme mit der WebAuthn Umleitung haben, verwenden Sie die folgenden Schritte zur Problembehandlung, um häufig auftretende Probleme zu identifizieren und zu lösen.

Topics

WebAuthn Die Umleitung funktioniert nicht

Wenn WebAuthn Authentifizierungsaufforderungen nicht angezeigt werden oder nicht funktionieren:

1. Verify WebAuthn ist in den Portaleinstellungen unter Benutzerberechtigungen aktiviert.
2. Überprüfen Sie, ob die lokale Browserrichtlinie korrekt konfiguriert ist, indem Sie zu `chrome://policy` oder navigieren `edge://policy` und bestätigen, dass die Inhalts-URL Ihrer Region `WebAuthenticationRemoteDesktopAllowedOrigins` enthalten ist.
3. Stellen Sie sicher, dass die Browserversion die Anforderungen erfüllt: Chrome 136+ oder Edge 137+.

4. Testen Sie mit einem anderen Authentifikator (Sicherheitsschlüssel oder Plattformauthentifikator).

Häufige Fehlermeldungen

Im Folgenden sind häufig auftretende Fehlermeldungen und ihre Lösungen aufgeführt:

WebAuthn Fehlermeldungen und Lösungen

Fehlermeldung	Auflösung
Die Amazon WebAuthn DCV-Umleitung konnte die Registrierungsanfrage nicht abschließen: Die Webauthn-Umleitung wird vom Client nicht unterstützt	Vergewissern Sie sich, dass Sie einen unterstützten Browser und eine unterstützte Version (Chrome 136+ oder Edge 137+) verwenden.
Die Aufforderung wird angezeigt, aber es kann nicht mit den lokalen Authentifikatoren interagiert werden	Vergewissern Sie sich, dass die Amazon WebAuthn DCV-Umleitungserweiterung in Ihrem Remote-Browser installiert und aktiviert ist.
Die Amazon WebAuthn DCV-Umleitung konnte die Registrierungsanfrage nicht abschließen: Die ID der vertrauenden Partei ist weder ein registrierbares Domain-Suffix von noch entspricht sie der aktuellen Domain. Anschließend schlug der Versuch fehl, die Ressource .well-known/webauthn der beanspruchten RP-ID abzurufen.	Dies bedeutet, dass die lokale Browserrichtlinie nicht angewendet wird. WebAuthenticationRemoteDesktopAllowedOrigins Überprüfen Sie die Richtlinie und aktualisieren Sie sie, um die Inhaltsdomäne zuzulassen. Stellen Sie sicher, dass der Browser neu gestartet wurde. Möglicherweise müssen Sie eine neue Sitzung starten, damit die Änderungen wirksam werden.
Der Vorgang hat entweder das Zeitlimit überschritten oder war nicht zulässig. Weitere Informationen finden Sie unter: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client.	Dieser Fehler kann auftreten, wenn: (1) Die WebAuthn DCV-Umleitungserweiterung nicht installiert oder aktiviert ist, (2) der Benutzer die Authentifizierungsaufforderung abbricht, (3) der Benutzer eine falsche PIN für seinen Sicherheitsschlüssel eingibt oder (4) der Benutzer die Eingabeaufforderung nicht befolgt und das Zeitlimit für die Anfrage überschritten wird.

Verwaltung der Toolbar-Steuerelemente im Amazon WorkSpaces Secure Browser

Mit den Steuerelementen in der Werkzeugleiste können Sie die Darstellung der Werkzeugleiste für Endbenutzersitzungen konfigurieren, einschließlich der folgenden Optionen:

- Funktionen
  - Zwischenablage: Wenn diese Option aktiviert ist, können copy/paste detaillierte Steuerelemente verwendet werden (nur Kopieren, nur Einfügen oder beides). Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet und die Verwendung in der Werkzeugleiste verhindert.
  - Dateiübertragung: Wenn diese Option aktiviert ist, sind Dateioperationen mit detaillierter Steuerung möglich (nur Upload, nur Herunterladen oder beides). Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet und Übertragungen werden verhindert.
  - Mikrofon: Wenn diese Option aktiviert ist, wird die Verwendung des Mikrofons ermöglicht. Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet.
  - Webcam: Wenn diese Option aktiviert ist, kann die Kamera verwendet werden. Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet.
  - Zwei Monitore: Wenn diese Option aktiviert ist, können zwei Monitore verwendet werden. Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet.
  - Vollbild: Wenn diese Option aktiviert ist, wird der Vollbildmodus aktiviert. Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet.
  - Windows: Wenn diese Option aktiviert ist, können Sie zwischen Fenstern wechseln. Wenn diese Option deaktiviert ist, wird das Symbol ausgeblendet.
- Einstellungen
  - Design der Werkzeugleiste: Steuert die Anzeige im Hell- oder Dunkelmodus. Durch die Konfiguration wird die Steuerung des Themes durch den Endbenutzer entfernt.
  - Status der Werkzeugleiste: Legt fest, ob die Werkzeugleiste angedockt oder getrennt ist. Durch die Konfiguration wird dem Endbenutzer die Kontrolle über den Status der Werkzeugleiste entzogen.
  - Max. Auflösung: Definiert die höchste zulässige Bildschirmauflösung. Benutzer können nur Auflösungen bis zu diesem definierten Limit auswählen.

Konfiguration einer benutzerdefinierten Domain für Ihr Portal

Sie können eine benutzerdefinierte Domain für ein WorkSpaces Secure Browser-Portal konfigurieren, um den Zugriff über Ihren eigenen Domainnamen statt über die Standard-Portal-URL zu ermöglichen. Mit dieser Funktion können Sie Benutzern mithilfe einer Domain, die dem Branding Ihres Unternehmens entspricht, ein stärker integriertes Erlebnis bieten.

Übersicht

Mit der benutzerdefinierten Domain können Sie die folgenden Aspekte der Benutzererfahrung personalisieren:

- Zugriff auf Ihr Markenportal — Benutzer greifen über die Domain Ihres Unternehmens auf Ihr Portal zu, anstatt über den standardmäßigen AWS-Endpunkt.
- Konsistentes Benutzererlebnis — Sorgen Sie für Markenkonsistenz, indem Sie vertraute Domainnamen verwenden, die zu Ihrem Unternehmen passen.

> **Note**
>
> Informationen zur Anpassung des visuellen Erscheinungsbilds und der Branding-Elemente Ihres Portals finden Sie unterthe section called “Anpassung des Brandings”.

Topics

Konfiguration einer benutzerdefinierten Domain für Ihr Portal

Funktionsweise

Wenn Sie eine benutzerdefinierte Domain konfigurieren:

- Sie erstellen und konfigurieren einen Reverse-Proxy mit Ihrer benutzerdefinierten Domain, um den Datenverkehr zum Portal-Endpunkt weiterzuleiten.
- Benutzer greifen über Ihre benutzerdefinierte Domain statt über den Standardportal-Endpunkt auf Ihr Portal zu.

- SSL-Zertifikate sorgen für sichere Verbindungen während des gesamten Prozesses.

Voraussetzungen

Bevor Sie benutzerdefinierte Domains einrichten, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein Domainname, den Sie über einen DNS-Dienstanbieter wie Amazon Route53 verwalten.
- Ein WorkSpaces sicheres Browser-Portal. Weitere Informationen zum Erstellen eines Portals finden Sie unterthe section called “Erstellung eines Webportals”.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für die Verwaltung von AWS Certificate Manager CloudFront - und DNS-Konfigurationen verfügen.

Important

Benutzer müssen Drittanbieter-Cookies für die benutzerdefinierte Domain in ihren Browsern aktivieren, um die ordnungsgemäße Portalfunktionalität sicherzustellen.
Stellen Sie sicher, dass Sie Eigentümer der benutzerdefinierten Domain und ihrer DNS-Einträge sind und diese ordnungsgemäß verwalten, um die Sicherheit und Funktionalität Ihres Portals zu gewährleisten.

Note

Um die Single Sign-On-Erweiterung für benutzerdefinierte Domains zu aktivieren, müssen Benutzer die Erweiterung in ihrem Browser mit einer späteren Version als 1.0.2505.6608 installieren.
Benutzer werden aufgefordert, die Erweiterung zu installieren, wenn sie sich bei einem Portal anmelden. Einzelheiten zum Benutzererlebnis mit der Erweiterung finden Sie unter the section called “Single-Sign-On-Erweiterung”.

Erste Schritte

Sie können Ihre benutzerdefinierte Domäne entweder beim Erstellen eines neuen Portals oder beim Bearbeiten eines vorhandenen Portals als Attribut für Portaleinstellungen konfigurieren. Dies kann mit den Befehlen AWS Console, SDK CloudFormation oder AWS CLI erfolgen.

Wir empfehlen, eine CloudFront Amazon-Distribution als Reverse-Proxy einzurichten, der den Datenverkehr von Ihrer benutzerdefinierten Domain zum Endpunkt des WorkSpaces Secure Browser-Portals weiterleitet.

> **Note**
>
> Obwohl Amazon als Reverse-Proxy-Lösung empfohlen CloudFront wird, können Sie alternative Reverse-Proxy-Konfigurationen verwenden. Stellen Sie sicher, dass Sie die erforderlichen Origin- und Cache-Konfigurationseinstellungen erfüllen, wie in den CloudFront Amazon-Einrichtungsschritten beschrieben.

Einrichtung CloudFront als Reverse-Proxy

Um die Einrichtung eines Reverse-Proxys abzuschließen, benötigen Sie:

- Ein SSL-Zertifikat über AWS Certificate Manager (ACM)
- Eine CloudFront Amazon-Distribution
- DNS-Einträge
- Mit Ihrer benutzerdefinierten Domain konfiguriertes Portal

SSL Certificate (SSL-Zertifikat)

Wenn Sie noch keine haben, gehen Sie wie folgt vor, um eine über ACM anzufordern:

1. Navigieren Sie zur ACM-Konsole unter. https://console.aws.amazon.com/acm

   > **Important**
   >
   > Verwenden Sie die Region USA Ost (Nord-Virginia), da Zertifikate dort gespeichert werden CloudFront müssen.

2. Fordern Sie ein Zertifikat an:

   - Für neue ACM-Benutzer: Wählen Sie unter Zertifikate bereitstellen die Option Erste Schritte
   - Für bestehende ACM-Benutzer: Wählen Sie Zertifikat anfordern

3. Wählen Sie Öffentliches Zertifikat anfordern und anschließend Zertifikat anfordern aus.

> **Note**
>
> Sie können auch ein vorhandenes Zertifikat importieren. Weitere Informationen finden Sie unter Importieren von Zertifikaten in ACM im ACM-Benutzerhandbuch.

4. Geben Sie Ihren primären Domainnamen ein (z. B.**`myportal.example.com`**).
5. Wählen Sie eine Validierungsmethode:
   - DNS-Validierung (empfohlen für Route 53 53-Benutzer) — Ermöglicht die automatische Erstellung von Datensätzen in Ihrer Hosting-Zone. Weitere Informationen finden Sie unter DNS-Validierung im ACM-Benutzerhandbuch.
   - E-Mail-Validierung — Weitere Informationen finden Sie unter E-Mail-Validierung im ACM-Benutzerhandbuch.
6. Überprüfen Sie Ihre Einstellungen und wählen Sie Bestätigen und anfordern.

CloudFront Verteilung

Erstellen Sie eine CloudFront Verteilung, um Anfragen von Ihrer benutzerdefinierten Domain an den Portal-Endpunkt weiterzuleiten.

1. Navigieren Sie zur CloudFront Konsole unterhttps://console.aws.amazon.com/cloudfront.
2. Wählen Sie Create Distribution (Distribution erstellen).
   - Distributionsname: Geben Sie einen Namen für die Distribution ein
   - Vertriebstyp: Einzelne Website oder App

> **Note**
>
> Wenn Ihre benutzerdefinierte Domain in Route 53 im selben AWS-Konto verwaltet wird, CloudFront kann Ihr DNS automatisch für Sie verwaltet werden. Geben Sie Ihre benutzerdefinierte Domain ein und klicken Sie auf „Domain prüfen“. Wenn Sie eine Domain von einem anderen DNS-Anbieter haben, überspringen Sie diesen Schritt und konfigurieren Sie Ihre Domain später.

3. Konfigurieren Sie die Ursprungseinstellungen:

- Ursprungs-Typ: Andere
- Benutzerdefinierter Ursprung: Geben Sie den Portal-Endpunkt *<portalId>* .workspaces-web.com ein
- Origin-Pfad: Leer lassen (Standard)

4. Origin-Einstellungen anpassen:

   - Benutzerdefinierten Header hinzufügen

     > **Important**
     >
     > Der Portalzugriff über eine benutzerdefinierte Domain funktioniert nur, wenn dieser Header in Proxyanfragen vorhanden ist. Stellen Sie sicher, dass der Name und der Wert des Headers genau wie angegeben angegeben angegeben sind.

     - Name der Kopfzeile: workspacessecurebrowser-custom-domain
     - Wert: Ihre benutzerdefinierte Domain (zum Beispiel**`myportal.example.com`**)
   - Protokoll: Nur HTTPS
   - HTTPS-Port: 443 (Standard beibehalten)
   - Minimales ursprüngliches SSL-Protokoll: TLSv1 .2 (Standard)
   - Origin-IP-Adresstyp: IPv4 nur (Amazon WorkSpaces Secure Browser unterstützt IPv6 zum Zeitpunkt der Erstellung dieses Administratorhandbuchs nicht.)

5. Passen Sie die Cache-Einstellungen an:

   - Viewer-Protokollrichtlinie: HTTP zu HTTPS umleiten
   - Zulässige HTTP-Methoden: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Cache-Richtlinie: CachingDisabled
   - Richtlinie für Origin-Anfragen: AllViewerExceptHostHeader

     > **Important**
     >
     > Der Portalzugriff über eine benutzerdefinierte Domain funktioniert nur, wenn die Richtlinie für Ursprungsanfragen auf eingestellt ist AllViewerExceptHostHeader. Wie der Name schon sagt, filtert diese Richtlinie nur den Host-Header aus den

Anforderungsheadern heraus und leitet alle verbleibenden Header an den Ursprung weiter.

6. Sie können WAF konfigurieren, wenn Sie möchten, dies ist jedoch für dieses Setup nicht erforderlich.
7. Wählen Sie unter TLS-Zertifikat abrufen das in Schritt 1 erstellte TLS-Zertifikat aus.
8. Überprüfen Sie die Einstellungen und wählen Sie Create Distribution aus.

DNS-Einträge

Cloudfront kann Ihre DNS-Einträge in Route 53 aktualisieren, um den Datenverkehr von den angegebenen Domains an die in Schritt 2 erstellte Verteilung weiterzuleiten, sofern sich Ihre gehostete Zone im selben AWS-Konto befindet.

1. Navigieren Sie zu den Einstellungen CloudFront
2. Klicken Sie auf „Domains weiterleiten an CloudFront“
3. Klicken Sie auf „Routing automatisch einrichten“

Wenn Sie DNS für die benutzerdefinierte Domain in einem anderen Service Provider oder einem anderen AWS-Konto konfiguriert haben, konfigurieren Sie Ihren DNS-Anbieter so, dass der Datenverkehr für Ihre Domain an die Distribution weitergeleitet wird. In den folgenden Schritten wird beschrieben, wie Sie dies mithilfe von Route 53 tun können.

1. Öffnen Sie die Amazon Route 53 53-Konsole unterhttps://console.aws.amazon.com/route53.
2. Greifen Sie auf die DNS-Verwaltung zu:
   - Wenn Sie Route 53 noch nicht mit diesem AWS Konto verwenden, wird die Übersichtsseite von Amazon Route 53 geöffnet. Wählen Sie unter DNS-Verwaltung die Option Jetzt starten aus.
   - Wenn Sie Route 53 bereits mit diesem AWS Konto verwendet haben, fahren Sie mit dem nächsten Schritt fort.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Erstellen Sie eine gehostete Zone, falls Sie noch keine haben:
   - Informationen zur Weiterleitung des Internetverkehrs zu Ihren Ressourcen finden Sie unter Creating a Public Hosted Zone im Amazon Route 53 53-Entwicklerhandbuch.

- Informationen zur Weiterleitung von Traffic in Ihrer VPC finden Sie unter Creating a Private Hosted Zone im Amazon Route 53 Developer Guide.

5. Wählen Sie auf der Seite Hosted Zones den Namen der Hosting-Zone aus, die Sie verwalten möchten.
6. Wählen Sie Create Record Set (Datensatz erstellen).
7. Erstellen Sie einen Eintrag für Ihre Domain (z. B.**`myportal.example.com`**):

   - Typ: A — IPv4 Adresse
   - Alias: Ja
   - Alias-Ziel: CloudFront Vertriebs-URL

   Behalten Sie die Standardwerte für alle anderen Einstellungen bei.

> **Note**
>
> Wenn Sie Route 53 nicht verwenden, um DNS für Ihre Domain zu verwalten, verwenden Sie Ihren DNS-Dienstanbieter und fügen Sie der URL Ihrer CloudFront Distribution DNS-Einträge hinzu, die auf Ihre Domain verweisen.

Alternativ können Sie die folgende CloudFormation Vorlage verwenden, um Ihre CloudFront Distribution zu erstellen:

Diese CloudFormation Vorlage erstellt automatisch die CloudFront Verteilung, konfiguriert die Reverse-Proxyeinstellungen und erstellt optional Route53-DNS-Einträge:

Example workspaces-web-custom-domain-template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'CloudFront Distribution for custom domain configuration with existing AWS
 WorkSpaces Secure Browser Portal'

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
```

```
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'

  CustomDomainName:
    Type: String
    Description: 'Custom domain name for the portal (e.g., myportal.example.com)'
    AllowedPattern: '^([a-zA-Z0-9]?((?!-)([A-Za-z0-9-]*[A-Za-z0-9])\.)+[a-zA-Z0-9]+)$'
    ConstraintDescription: 'Must be a valid domain name'

  CertificateArn:
    Type: String
    Description: 'ARN of the validated SSL certificate in ACM (must be in us-east-1
 region for CloudFront)'
    AllowedPattern: 'arn:aws:acm:us-east-1:[0-9]{12}:certificate/[a-f0-9]{8}-[a-f0-9]
{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}'
    ConstraintDescription: 'Must be a valid ACM certificate ARN in us-east-1 region'

  CreateRoute53Record:
    Type: String
    Description: 'Create Route53 record for custom domain (requires existing hosted
 zone)'
    Default: 'No'
    AllowedValues:
      - 'Yes'
      - 'No'

  HostedZoneId:
    Type: String
    Description: 'Route53 Hosted Zone ID for the custom domain (required if creating
 Route53 record)'
    Default: ''

Conditions:
  ShouldCreateRoute53Record: !And
    - !Equals [!Ref CreateRoute53Record, 'Yes']
    - !Not [!Equals [!Ref HostedZoneId, '']]

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
```

```
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
${CustomDomainName}'
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

        # Origin Configuration
        Origins:
          - Id: WorkSpacesWebOrigin
            DomainName: !Ref PortalEndpoint
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
              - HeaderName: workspacessecurebrowser-custom-domain
                HeaderValue: !Ref CustomDomainName

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
```

```
          MinimumProtocolVersion: TLSv1.2_2021

      Tags:
        - Key: Name
          Value: !Sub '${AWS::StackName}-cloudfront'

  # Route 53 Record (optional - requires hosted zone to exist)
  Route53Record:
    Type: AWS::Route53::RecordSet
    Condition: ShouldCreateRoute53Record
    Properties:
      HostedZoneId: !Ref HostedZoneId
      Name: !Ref CustomDomainName
      Type: A
      AliasTarget:
        DNSName: !GetAtt CloudFrontDistribution.DomainName
        HostedZoneId: Z2FDTNDATAQYW2  # CloudFront Hosted Zone ID
        EvaluateTargetHealth: false

Outputs:
  PortalEndpoint:
    Description: 'WorkSpaces Web Portal endpoint used as origin'
    Value: !Ref PortalEndpoint
    Export:
      Name: !Sub '${AWS::StackName}-PortalEndpoint'

  CustomDomainEndpoint:
    Description: 'Custom domain endpoint for the portal'
    Value: !Sub 'https://${CustomDomainName}'
    Export:
      Name: !Sub '${AWS::StackName}-CustomDomainEndpoint'

  CloudFrontDistributionId:
    Description: 'CloudFront Distribution ID'
    Value: !Ref CloudFrontDistribution
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDistributionId'

  CloudFrontDomainName:
    Description: 'CloudFront Distribution Domain Name'
    Value: !GetAtt CloudFrontDistribution.DomainName
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDomainName'
```

```
  CertificateArn:
    Description: 'SSL Certificate ARN used by CloudFront'
    Value: !Ref CertificateArn
    Export:
      Name: !Sub '${AWS::StackName}-CertificateArn'

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: "Existing Portal Configuration"
        Parameters:
          - PortalEndpoint
      - Label:
          default: "Custom Domain Configuration"
        Parameters:
          - CustomDomainName
          - CertificateArn
          - CreateRoute53Record
          - HostedZoneId
    ParameterLabels:
      PortalEndpoint:
        default: "Portal Endpoint"
      CustomDomainName:
        default: "Custom Domain Name"
      CertificateArn:
        default: "SSL Certificate ARN"
      CreateRoute53Record:
        default: "Create Route53 Record"
      HostedZoneId:
        default: "Hosted Zone ID"
```

Um diese Vorlage zu verwenden:

1. Speichern Sie die obige Vorlage als `workspaces-web-custom-domain-template.yaml`
2. Bereitstellen mithilfe der AWS Konsole, der AWS CLI oder des AWS SDK mit Ihren spezifischen Parameterwerten
3. Nach der Bereitstellung konfigurieren Sie Ihr Portal mit der benutzerdefinierten Domain, wie in Schritt 4 unten beschrieben

Konfiguration des Portals

Registrieren Sie Ihre benutzerdefinierte Domain mit der AWS Konsole, der UpdatePortal API oder dem AWS CLI-Befehl update-portal als Attribut für Portaleinstellungen.

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unter. https://console.aws.amazon.com/workspaces-web/home
2. Wählen Sie im linken Navigationsbereich die Option Webportale aus.
3. Wählen Sie das Webportal aus, das Sie konfigurieren möchten, und klicken Sie auf Bearbeiten.
4. Fügen Sie in den Portaleinstellungen Ihre benutzerdefinierte Domain hinzu.
5. Speichern Sie die Portalkonfiguration.

Testen Sie Ihre Konfiguration

Gehen Sie wie folgt vor, um Ihre Konfiguration zu testen:

1. Öffnen Sie einen Webbrowser und navigieren Sie zur URL für Ihre benutzerdefinierte Domain (z. B.**`https://myportal.example.com`**).
2. Wenn alles korrekt eingerichtet ist, sollte die Anmeldeseite für Ihr Portal angezeigt werden.
3. Geben Sie anschließend die Portal-URL in Ihren Browser ein. Sie sollten nach der Anmeldung bei Ihrem IdP zur benutzerdefinierten Domain weitergeleitet werden.
4. Melden Sie sich abschließend bei Ihrem IdP an und klicken Sie auf die Anwendungskachel für Ihr Portal. Sie sollten zur benutzerdefinierten Domain weitergeleitet werden.

Behebung von Problemen mit benutzerdefinierten Domains

Wenn Benutzer in ihren Remote-Browsersitzungen Probleme mit dem Portalzugriff über eine benutzerdefinierte Domäne haben, verwenden Sie die folgenden Schritte zur Fehlerbehebung, um häufig auftretende Probleme zu identifizieren und zu lösen.

Topics

Häufige Fehlermeldungen

Im Folgenden finden Sie häufig auftretende Fehlermeldungen und deren Lösungen bei der Einrichtung benutzerdefinierter Domänen:

Ungültiger CSRF-Token-Fehler

Dieser Fehler tritt auf, wenn Secure Browser Ihre Anfrage über das CloudFront Setup nicht ordnungsgemäß empfängt.

So beheben Sie dieses Problem

- Überprüfen Sie die benutzerdefinierten Origin-Einstellungen in Ihrer CloudFront Distribution.
- Stellen Sie sicher, dass der Name des benutzerdefinierten Headers genau `workspacessecurebrowser-custom-domain` und der Wert genau mit Ihrer benutzerdefinierten Domain übereinstimmt (ohne https://oder irgendwelche Abfrageparameter).
- Leeren Sie den Cache in Ihrem lokalen Browser.
- Machen Sie den Cache ungültig auf. CloudFront

502 Bad Gateway-Fehler

Dieser Fehler weist normalerweise auf Probleme mit der Cache-Konfiguration hin.

So beheben Sie dieses Problem

- Überprüfen Sie die Cache-Einstellungen auf Ihrer CloudFront Distribution.
- Stellen Sie sicher, dass die Cache-Richtlinie auf eingestellt ist`CachingDisabled`.
- Vergewissern Sie sich, dass die Origin-Anforderungsrichtlinie auf eingestellt ist`AllViewerExceptHostHeader`.
- Leeren Sie den Cache in Ihrem lokalen Browser.
- Machen Sie den Cache ungültig auf. CloudFront

Fehler „Zugriff verweigert“

Dieser Fehler kann auftreten, wenn Ihre benutzerdefinierte Domain falsch konfiguriert ist.

So beheben Sie dieses Problem

- Überprüfen Sie die Ursprungseinstellungen Ihrer CloudFront Distribution.
- Vergewissern Sie sich, dass für Origin die richtige Portal-URL festgelegt ist.
- Stellen Sie sicher, dass das Portal mit der richtigen benutzerdefinierten Domain konfiguriert ist.
- Leeren Sie den Cache in Ihrem lokalen Browser.
- Machen Sie den Cache ungültig auf. CloudFront

Sicherheit im Amazon WorkSpaces Secure Browser

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon WorkSpaces Secure Browser gelten, finden Sie unter AWS-Services in Umfang nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und alle geltenden Gesetze und Vorschriften, die für Ihre Daten gelten.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon WorkSpaces Secure Browser anwenden können. Es zeigt Ihnen, wie Sie Amazon WorkSpaces Secure Browser konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Amazon Secure Browser-Ressourcen überwachen und WorkSpaces sichern können.

Inhalt

- Zugriff APIs über eine Schnittstelle VPC-Endpunkt ()AWS PrivateLink
- Bewährte Sicherheitsmethoden für Amazon WorkSpaces Secure Browser

Datenschutz im Amazon WorkSpaces Secure Browser

Das AWS Modell der mit gilt für den Datenschutz im Amazon WorkSpaces Secure Browser. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit WorkSpaces Secure Browser oder anderen Geräten arbeiten und die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Topics

Datenverschlüsselung im Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser sammelt Portalanpassungsdaten wie Browsereinstellungen, Benutzereinstellungen, Netzwerkeinstellungen, Identitätsanbieterinformationen, Trust Store-Daten und Trust Store-Zertifikatsdaten. WorkSpaces Secure Browser sammelt auch Browserrichtliniendaten, Benutzereinstellungen (für Browsereinstellungen) und Sitzungsprotokolle. Die gesammelten Daten werden in Amazon DynamoDB und Amazon S3 gespeichert. WorkSpaces Secure Browser verwendet AWS Key Management Service für die Verschlüsselung.

Befolgen Sie die folgenden Richtlinien, um deine Inhalte zu schützen:

- Implementieren Sie den Zugriff mit den geringsten Rechten und erstellen Sie spezielle Rollen, die für WorkSpaces Secure Browser-Aktionen verwendet werden. Verwenden Sie IAM-Vorlagen, um eine Rolle mit Vollzugriff oder Schreibschutz zu erstellen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für WorkSpaces Secure Browser.
- Schützen Sie Daten durchgängig, indem Sie einen vom Kunden verwalteten Schlüssel bereitstellen, sodass WorkSpaces Secure Browser Ihre gespeicherten Daten mit den von Ihnen bereitgestellten Schlüsseln verschlüsseln kann.
- Seien Sie vorsichtig, wenn Sie Portal-Domains und Benutzeranmeldedaten teilen:
  - Administratoren müssen sich bei der WorkSpaces Amazon-Konsole anmelden, und Benutzer müssen sich beim WorkSpaces Secure Browser-Portal anmelden.

- Jeder Benutzer im Internet kann auf das Webportal zugreifen, aber er kann keine Sitzung starten, wenn er nicht über die gültigen Benutzeranmeldedaten für das Portal verfügt.
- Benutzer können ihre Sitzungen explizit beenden, indem sie Sitzung beenden auswählen. Dadurch wird die Instance, die die Browsersitzung hostet, verworfen und der Browser wird isoliert.

WorkSpaces Secure Browser schützt Inhalte und Metadaten standardmäßig, indem er alle sensiblen Daten mit verschlüsselt. AWS KMS Es erfasst Browserrichtlinien und Benutzereinstellungen, um Richtlinien und Einstellungen während WorkSpaces Secure Browser-Sitzungen durchzusetzen. Wenn beim Anwenden vorhandener Einstellungen ein Fehler auftritt, kann ein Benutzer weder auf neue Sitzungen noch auch auf die internen Websites und SaaS-Anwendungen des Unternehmens zugreifen.

Verschlüsselung im Ruhezustand für Amazon WorkSpaces Secure Browser

Die Verschlüsselung im Ruhezustand ist standardmäßig konfiguriert und alle im WorkSpaces Secure Browser verwendeten Kundendaten (z. B. Browserrichtlinien, Benutzernamen, Protokollierung oder IP-Adressen) werden mit AWS KMS verschlüsselt. Standardmäßig aktiviert WorkSpaces Secure Browser die Verschlüsselung mit einem AWS eigenen Schlüssel. Sie können auch einen vom Kunden verwalteten Schlüssel (CMK) verwenden, indem Sie Ihren CMK bei der Ressourcenerstellung angeben. Dies wird derzeit nur über die CLI unterstützt.

Wenn Sie sich dafür entscheiden, einen CMK zu übergeben, muss es sich bei dem bereitgestellten Schlüssel um einen symmetrischen AWS KMS Verschlüsselungsschlüssel handeln, und Sie als Administrator müssen über die folgenden Berechtigungen verfügen:

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Wenn Sie einen CMK verwenden, müssen Sie den externen Dienstprinzipal von WorkSpaces Secure Browser für den Zugriff auf den Schlüssel zulassen.

Weitere Informationen finden Sie unter Beispiel für eine CMK-Schlüsselrichtlinie mit Geltungsbereich mit aws: SourceAccount

Wann immer möglich, verwendet WorkSpaces Secure Browser die Anmeldeinformationen für Forward Access Sessions (FAS), um auf Ihren Schlüssel zuzugreifen. Weitere Informationen zu FAS finden Sie unter Forward Access Sessions.
Es gibt Fälle, in denen WorkSpaces Secure Browser möglicherweise asynchron auf Ihren Schlüssel zugreifen muss. Wenn Sie den externen Dienstprinzipal von WorkSpaces Secure Browser in Ihrer Schlüsselrichtlinie zulassen, kann WorkSpaces Secure Browser die auf der Zulassungsliste aufgeführten kryptografischen Operationen mit Ihrem Schlüssel ausführen.

Nachdem eine Ressource erstellt wurde, kann der Schlüssel nicht mehr entfernt oder geändert werden. Wenn Sie ein CMK verwendet haben, müssen Sie als Administrator, der auf die Ressource zugreift, über die folgenden Berechtigungen verfügen:

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Wenn bei der Verwendung der Konsole der Fehler Zugriff verweigert angezeigt wird, verfügt der Benutzer, der auf die Konsole zugreift, wahrscheinlich nicht über die erforderlichen Berechtigungen, um den CMK für den verwendeten Schlüssel zu verwenden.

Beispiele für wichtige Richtlinien und Geltungsbereiche für Secure Browser WorkSpaces

CMKs erfordern die folgende wichtige Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
```

```
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      }
    ]
}
```

Die folgenden Berechtigungen sind für WorkSpaces Secure Browser erforderlich:

- `kms:DescribeKey`— Überprüft, ob der angegebene AWS KMS Schlüssel korrekt konfiguriert ist.
- `kms:GenerateDataKeyWithoutPlaintext`und `kms:GenerateDataKey` — Anforderung des AWS KMS Schlüssels zur Erstellung von Datenschlüsseln, die zur Verschlüsselung von Objekten verwendet werden.
- `kms:Decrypt`— Fordert den AWS KMS Schlüssel zur Entschlüsselung der verschlüsselten Datenschlüssel an. Diese Datenschlüssel werden verwendet, um Ihre Daten zu verschlüsseln.
- `kms:ReEncryptTo`und `kms:ReEncryptFrom` — Anforderung des AWS KMS Schlüssels, um eine erneute Verschlüsselung von oder zu einem KMS-Schlüssel zu ermöglichen.

Festlegung des Gültigkeitsbereichs der WorkSpaces Secure Browser-Berechtigungen für Ihren Schlüssel AWS KMS

Wenn es sich bei dem Prinzipal in einer wichtigen Richtlinienerklärung um einen AWS Dienstprinzipal handelt, empfehlen wir dringend, zusätzlich zum Verschlüsselungskontext die SourceAccount globalen Bedingungsschlüssel aws: SourceArn oder aws: zu verwenden.

Der für eine Ressource verwendete Verschlüsselungskontext enthält immer einen Eintrag im Format `aws:workspaces-web:RESOURCE_TYPE:id` und die entsprechende Ressourcen-ID.

Die Werte des Quell-ARN und des Quellkontos sind nur dann im Autorisierungskontext enthalten, wenn eine Anfrage AWS KMS von einem anderen AWS Dienst eingeht. Diese Kombination von Bedingungen implementiert die geringsten Berechtigungen und verhindert ein potenzielles Szenario des verwirrten Stellvertreters. Weitere Informationen finden Sie unter Berechtigungen für AWS-Services in den wichtigsten Richtlinien.

```
   "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "AccountId",
          "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
          ]
        },
      }
```

> **Note**
>
> Vor der Erstellung der Ressource sollte die Schlüsselrichtlinie nur die `aws:SourceAccount` Bedingung verwenden, da der vollständige Ressourcen-ARN noch nicht vorhanden sein wird. Nach der Erstellung der Ressource kann die Schlüsselrichtlinie so aktualisiert werden, dass sie die `kms:EncryptionContext` Bedingungen `aws:SourceArn` und enthält.

Beispiel für eine CMK-Schlüsselrichtlinie mit Geltungsbereich **`aws:SourceAccount`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

Beispiel für eine CMK-Schlüsselrichtlinie mit Gültigkeitsbereich und Ressourcen-Platzhalter **`aws:SourceArn`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

Beispiel für eine CMK-Schlüsselrichtlinie mit Geltungsbereich **`aws:SourceArn`**

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

```
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> Nachdem Sie die Ressource erstellt haben, können Sie den Platzhalter dafür aktualisieren. `SourceArn` Wenn Sie WorkSpaces Secure Browser verwenden, um eine neue Ressource zu erstellen, für die CMK-Zugriff erforderlich ist, stellen Sie sicher, dass Sie die zugehörige Schlüsselrichtlinie entsprechend aktualisieren.

Beispiel für eine bereichsbezogene CMK-Schlüsselrichtlinie mit und ressourcenspezifischer **`aws:SourceArn`** **`EncryptionContext`**

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

```
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
"<userSetttingsId>"
```

```
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
"<browserSettingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
```

```
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
 "<ipAccessSettingsId>"
        }
      }
    },
  ]
}
```

> **Note**
>
> Stellen Sie sicher, dass Sie separate Anweisungen erstellen, wenn Sie eine Ressource einbeziehen, die sich `EncryptionContext` auf dieselbe Schlüsselrichtlinie bezieht. Weitere Informationen finden Sie im Abschnitt Verwenden mehrerer Verschlüsselungskontextpaare unter kms:EncryptionContext: Kontextschlüssel.

Verschlüsselung bei der Übertragung für Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser verschlüsselt Daten während der Übertragung über HTTPS und TLS 1.2. Sie können eine Anfrage über die WorkSpaces Konsole oder direkte API-Aufrufe an senden. Die übertragenen Anforderungsdaten werden verschlüsselt, indem alles über eine HTTPS- oder TLS-Verbindung gesendet wird. Anforderungsdaten können von der AWS Konsole oder dem AWS SDK an den WorkSpaces Secure Browser übertragen werden. AWS Command Line Interface

Sowohl die Verschlüsselung während der Übertragung als auch sichere Verbindungen (HTTPS, TLS) sind standardmäßig konfiguriert.

Schlüsselverwaltung für Amazon WorkSpaces Secure Browser

Sie können Ihren eigenen vom Kunden verwalteten AWS KMS Schlüssel angeben, um Ihre Kundeninformationen zu verschlüsseln. Wenn Sie keinen angeben, verwendet WorkSpaces Secure Browser einen AWS eigenen Schlüssel. Sie können Ihren Schlüssel mithilfe des AWS -SDK festlegen.

Datenschutz im Netzwerkverkehr im Amazon WorkSpaces Secure Browser

Um Verbindungen zwischen WorkSpaces Secure Browser und lokalen Anwendungen zu sichern, verwenden Sie WorkSpaces Secure Browser, um Browsersitzungen in Ihrer eigenen VPC zu starten. Die Verbindung zu lokalen Anwendungen ist in Ihrer eigenen VPC konfiguriert und wird nicht vom WorkSpaces Secure Browser gesteuert.

Um Verbindungen zwischen Konten zu WorkSpaces sichern, verwendet Secure Browser eine dienstbezogene Rolle, um eine sichere Verbindung zu Kundenkonten herzustellen und Vorgänge im Namen des Kunden auszuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon WorkSpaces Secure Browser.

Protokollierung des Benutzerzugriffs im Amazon WorkSpaces Secure Browser

Administratoren können WorkSpaces Secure Browser-Sitzungsereignisse wie Start- und Stopp- und URL-Besuche aufzeichnen. Diese Protokolle werden verschlüsselt und sicher über einen Amazon-Kinesis-Datenstrom an Kunden übermittelt. Browserinformationen aus der Benutzerzugriffsprotokollierung werden nicht in Sitzungen gespeichert und sind auch nicht in Sitzungen verfügbar AWS, für die keine Protokollierung konfiguriert ist. URL-Besuche im Inkognitomodus oder URLs aus dem Browserverlauf gelöschte URLs werden nicht in der Benutzerzugriffsprotokollierung aufgezeichnet.

Identity and Access Management für Amazon WorkSpaces Secure Browser

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um WorkSpaces Secure Browser-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Verwenden von serviceverknüpften Rollen für Amazon WorkSpaces Secure Browser

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Secure Browser).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Amazon WorkSpaces Secure Browser mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Amazon WorkSpaces Secure Browser mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf WorkSpaces Secure Browser zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit WorkSpaces Secure Browser verwendet werden können.

IAM-Funktionen, die Sie mit Amazon WorkSpaces Secure Browser verwenden können

IAM-Feature	WorkSpaces Unterstützung für sicheren Browser
Identitätsbasierte Richtlinien	Ja

IAM-Feature	WorkSpaces Unterstützung für sicheren Browser
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie WorkSpaces Secure Browser und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Topics

- Identitätsbasierte Richtlinien für Secure Browser WorkSpaces
- Ressourcenbasierte Richtlinien in Secure Browser WorkSpaces
- Richtlinienaktionen für Secure Browser WorkSpaces
- Richtlinienressourcen für Secure Browser WorkSpaces
- Bedingungsschlüssel für Richtlinien für Secure Browser WorkSpaces
- Zugriffskontrolllisten (ACLs) im Secure Browser WorkSpaces
- Attributbasierte Zugriffskontrolle (ABAC) mit Secure Browser WorkSpaces
- Temporäre Anmeldeinformationen mit WorkSpaces Secure Browser verwenden
- Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Secure Browser

- Servicerollen für WorkSpaces Secure Browser
- Dienstbezogene Rollen für WorkSpaces Secure Browser

Identitätsbasierte Richtlinien für Secure Browser WorkSpaces

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Secure Browser WorkSpaces

Beispiele für identitätsbasierte Richtlinien von WorkSpaces Secure Browser finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Ressourcenbasierte Richtlinien in Secure Browser WorkSpaces

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Secure Browser WorkSpaces

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der WorkSpaces Secure Browser-Aktionen finden Sie unter Von Amazon WorkSpaces Secure Browser definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen im WorkSpaces Secure Browser verwenden vor der Aktion das folgende Präfix:

```
workspaces-web
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

Beispiele für identitätsbasierte Richtlinien von WorkSpaces Secure Browser finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Richtlinienressourcen für Secure Browser WorkSpaces

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der WorkSpaces Secure Browser-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon WorkSpaces Secure Browser definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon WorkSpaces Secure Browser definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für WorkSpaces Secure Browser finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Bedingungsschlüssel für Richtlinien für Secure Browser WorkSpaces

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für WorkSpaces Secure Browser finden Sie unter Bedingungsschlüssel für Amazon WorkSpaces Secure Browser in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon WorkSpaces Secure Browser definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für WorkSpaces Secure Browser finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Zugriffskontrolllisten (ACLs) im Secure Browser WorkSpaces

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Secure Browser WorkSpaces

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit WorkSpaces Secure Browser verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu

verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Secure Browser

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für WorkSpaces Secure Browser

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von WorkSpaces Secure Browser beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn WorkSpaces Secure Browser Sie dazu anleitet.

Dienstbezogene Rollen für WorkSpaces Secure Browser

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Standardmäßig sind Benutzer und Rollen nicht berechtigt, WorkSpaces Secure Browser-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von WorkSpaces Secure Browser definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Secure Browser in der Service Authorization Reference.

Themen

Bewährte Methoden für identitätsbasierte Richtlinien für Amazon Secure Browser WorkSpaces

Identitätsbasierte Richtlinien legen fest, ob jemand WorkSpaces Secure Browser-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen

finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon WorkSpaces Secure Browser-Konsole

Um auf die Amazon WorkSpaces Secure Browser-Konsole zugreifen zu können, müssen Sie über Mindestberechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu

den WorkSpaces Secure Browser-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die WorkSpaces Secure Browser-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den WorkSpaces Secure Browser `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Benutzern ermöglichen, ihre eigenen Berechtigungen für Amazon WorkSpaces Secure Browser einzusehen

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für WorkSpaces Secure Browser

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste können einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzufügen, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue

Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Topics

- AWS verwaltete Richtlinie: AmazonWorkSpacesWebServiceRolePolicy
- AWS verwaltete Richtlinie: AmazonWorkSpacesSecureBrowserReadOnly
- AWS verwaltete Richtlinie: AmazonWorkSpacesWebReadOnly
- WorkSpaces Secure Browser-Updates für AWS verwaltete Richtlinien

AWS verwaltete Richtlinie: AmazonWorkSpacesWebServiceRolePolicy

Sie können die `AmazonWorkSpacesWebServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es WorkSpaces Secure Browser ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter the section called “Verwenden von servicegebundenen Rollen”.

Diese Richtlinie gewährt Administratorberechtigungen, die den Zugriff auf AWS Dienste und Ressourcen ermöglichen, die von WorkSpaces Secure Browser verwendet oder verwaltet werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `workspaces-web`— Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die von WorkSpaces Secure Browser verwendet oder verwaltet werden.
- `ec2`— Ermöglicht es Prinzipalen VPCs, Subnetze und Verfügbarkeitszonen zu beschreiben, Netzwerkschnittstellen zu erstellen, zu kennzeichnen, zu beschreiben und zu löschen, eine Adresse zuzuordnen oder zu trennen und Routentabellen, Sicherheitsgruppen und VPC-Endpunkte zu beschreiben.

- `CloudWatch` – ermöglicht es Prinzipalen, Metrikdaten einzugeben.
- `Kinesis` – ermöglicht es Prinzipalen, eine Zusammenfassung der Kinesis-Datenströme zu beschreiben und Datensätze zur Protokollierung von Benutzerzugriffen in Kinesis-Datenströmen abzulegen. Weitere Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
```

```
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonWorkSpacesSecureBrowserReadOnly

Sie können die `AmazonWorkSpacesSecureBrowserReadOnly`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die den Zugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten über die AWS Management Console, das SDK und die CLI ermöglichen. Diese Richtlinie beinhaltet keine Berechtigungen, die für die Interaktion mit Portalen erforderlich sind, bei denen `IAM_Identity_Center` als Authentifizierungstyp verwendet wird. Wenn Sie diese Berechtigungen erhalten möchten, kombinieren Sie diese Richtlinie mit `AWSSSOReadOnly`.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `workspaces-web`— Bietet über die AWS Management Console, das SDK und die CLI schreibgeschützten Zugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten.
- `ec2`— Ermöglicht Prinzipalen die Beschreibung von Subnetzen VPCs und Sicherheitsgruppen. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet VPCs, um Ihnen Ihre Subnetze und Sicherheitsgruppen anzuzeigen, die für die Verwendung mit dem Dienst verfügbar sind.

- `Kinesis` – ermöglicht Prinzipalen das Aufführen von Amazon-Kinesis-Datenströmen. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet, um Ihnen Kinesis-Datenstreams anzuzeigen, die für die Verwendung mit dem Service verfügbar sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS verwaltete Richtlinie: AmazonWorkSpacesWebReadOnly

Sie können die `AmazonWorkSpacesWebReadOnly`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die den Zugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten über die AWS Management Console, das SDK und die CLI ermöglichen. Diese Richtlinie beinhaltet keine Berechtigungen, die für die Interaktion mit Portalen erforderlich sind, bei denen `IAM_Identity_Center` als Authentifizierungstyp verwendet wird. Wenn Sie diese Berechtigungen erhalten möchten, kombinieren Sie diese Richtlinie mit `AWSSSOReadOnly`.

> **Note**
>
> Wenn Sie diese Richtlinie derzeit verwenden, wechseln Sie zu der neuen `AmazonWorkSpacesSecureBrowserReadOnly` Richtlinie.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `workspaces-web`— Bietet über die AWS Management Console, das SDK und die CLI schreibgeschützten Zugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten.
- `ec2`— Ermöglicht Prinzipalen die Beschreibung von Subnetzen VPCs und Sicherheitsgruppen. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet VPCs, um Ihnen Ihre Subnetze und Sicherheitsgruppen anzuzeigen, die für die Verwendung mit dem Dienst verfügbar sind.
- `Kinesis` – ermöglicht Prinzipalen das Aufführen von Amazon-Kinesis-Datenströmen. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet, um Ihnen Kinesis-Datenstreams anzuzeigen, die für die Verwendung mit dem Service verfügbar sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces Secure Browser-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für WorkSpaces Secure Browser an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

Änderungen	Beschreibung	Date
AmazonWorkSpacesSecureBrowserReadOnly – Neue Richtlinie	WorkSpaces Secure Browser hat eine neue Richtlinie hinzugefügt, die Lesezugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten über die AWS-Managementkonsole, das SDK und die CLI ermöglicht.	24. Juni 2024
AmazonWorkSpacesWebServiceRolePolicy – Richtlinie aktualisieren	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, sodass nur noch CreateNetworkInterface Tags mit aws:RequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged: true verwendet werden dürfen.	15. Dezember 2022
AmazonWorkSpacesWebReadOnly – Richtlinie aktualisieren	WorkSpaces Secure Browser hat die Richtlinie um Leseberechtigungen für die Protokollierung von Benutzerzugriffen und die Auflistung von Kinesis-Datenströmen erweitert. Weitere	02. November 2022

Änderungen	Beschreibung	Date
	Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”.	
AmazonWorkSpacesWebServiceRolePolicy – Richtlinie aktualisieren	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, um eine Zusammenfassung der Kinesis-Datenströme zu beschreiben und Datensätze für die Benutzerzugriffsprotokollierung in Kinesis-Datenströmen abzulegen. Weitere Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”.	17. Oktober 2022
AmazonWorkSpacesWebServiceRolePolicy – Richtlinie aktualisieren	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, sodass bei der ENI-Erstellung Tags erstellt werden.	6. September 2022
AmazonWorkSpacesWebServiceRolePolicy – Richtlinie aktualisieren	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, um den AWS/Usage Namespace zu den PutMetricData API-Berechtigungen hinzuzufügen.	6. April 2022

Änderungen	Beschreibung	Date
AmazonWorkSpacesWebReadOnly – Neue Richtlinie	WorkSpaces Secure Browser hat eine neue Richtlinie hinzugefügt, die Lesezugriff auf WorkSpaces Secure Browser und seine Abhängigkeiten über die AWS-Managementkonsole, das SDK und die CLI ermöglicht.	30. November 2021
AmazonWorkSpacesWebServiceRolePolicy – Neue Richtlinie	WorkSpaces Secure Browser hat eine neue Richtlinie hinzugefügt, die den Zugriff auf AWS-Services und -Ressourcen ermöglicht, die von WorkSpaces Secure Browser verwendet oder verwaltet werden.	30. November 2021
WorkSpaces Secure Browser hat begonnen, Änderungen zu verfolgen	WorkSpaces Secure Browser begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	30. November 2021

Fehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Secure Browser

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit WorkSpaces Secure Browser und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion im WorkSpaces Secure Browser durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkSpaces Secure Browser-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion im WorkSpaces Secure Browser durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `workspaces-web:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `workspaces-web:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an WorkSpaces Secure Browser übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion im WorkSpaces Secure Browser auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkSpaces Secure Browser-Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob WorkSpaces Secure Browser diese Funktionen unterstützt, finden Sie unter. So funktioniert Amazon WorkSpaces Secure Browser mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Secure Browser verknüpft ist. WorkSpaces Dienstbezogene Rollen sind von WorkSpaces Secure Browser vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstverknüpfte Rolle erleichtert die Einrichtung von WorkSpaces Secure Browser, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. WorkSpaces Secure Browser definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur WorkSpaces Secure Browser seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinien. Die Berechtigungsrichtlinie kann mit keiner anderen IAM-Entität verknüpft werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre WorkSpaces Secure Browser-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Topics

Mit dem Dienst verknüpfte Rollenberechtigungen für Secure Browser WorkSpaces

WorkSpaces Secure Browser verwendet die serviceverknüpfte Rolle mit dem Namen `AWSServiceRoleForAmazonWorkSpacesWeb` — WorkSpaces Secure Browser verwendet diese serviceverknüpfte Rolle, um auf Amazon EC2 EC2-Ressourcen von Kundenkonten für Streaming-Instances und Metriken zuzugreifen. CloudWatch

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonWorkSpacesWeb` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `workspaces-web.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen `AmazonWorkSpacesWebServiceRolePolicy` ermöglicht es WorkSpaces Secure Browser, die folgenden Aktionen an den angegebenen

Ressourcen durchzuführen. Weitere Informationen finden Sie unter the section called “AmazonWorkSpacesWebServiceRolePolicy”.

- Aktion: `ec2:DescribeVpcs` für `all AWS resources`
- Aktion: `ec2:DescribeSubnets` für `all AWS resources`
- Aktion: `ec2:DescribeAvailabilityZones` für `all AWS resources`
- Aktion: `ec2:CreateNetworkInterface` mit `aws:RequestTag/WorkSpacesWebManaged: true` in Subnetz- und Sicherheitsgruppenressourcen
- Aktion: `ec2:DescribeNetworkInterfaces` für `all AWS resources`
- Aktion: `ec2:DeleteNetworkInterface` in Netzwerkschnittstellen mit `aws:ResourceTag/WorkSpacesWebManaged: true`
- Aktion: `ec2:DescribeSubnets` für `all AWS resources`
- Aktion: `ec2:AssociateAddress` für `all AWS resources`
- Aktion: `ec2:DisassociateAddress` für `all AWS resources`
- Aktion: `ec2:DescribeRouteTables` für `all AWS resources`
- Aktion: `ec2:DescribeSecurityGroups` für `all AWS resources`
- Aktion: `ec2:DescribeVpcEndpoints` für `all AWS resources`
- Aktion: `ec2:CreateTags` in `ec2:CreateNetworkInterface`-Betrieb mit `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Aktion: `cloudwatch:PutMetricData` für `all AWS resources`
- Aktion: `kinesis:PutRecord` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen
- Aktion: `kinesis:PutRecords` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen
- Aktion: `kinesis:DescribeStreamSummary` in Kinesis-Datenströmen mit Namen, die mit `amazon-workspaces-web-` beginnen

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Eine dienstbezogene Rolle für WorkSpaces Secure Browser erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Ihr erstes Portal in der AWS-Managementkonsole, der oder der AWS API erstellen AWS CLI, erstellt WorkSpaces Secure Browser die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet.

Wenn Sie diese serviceverknüpfte Rolle löschen und später erneut erstellen müssen, können Sie die Rolle in Ihrem Konto auf dieselbe Weise neu erstellen. Wenn Sie Ihr erstes Portal erstellen, erstellt WorkSpaces Secure Browser die serviceverknüpfte Rolle erneut für Sie.

Sie können die IAM-Konsole auch verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall WorkSpaces Secure Browser zu erstellen. Erstellen Sie in der AWS CLI oder der AWS API eine dienstverknüpfte Rolle mit dem `workspaces-web.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpfte Rolle im IAM-Leitfaden. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Eine dienstverknüpfte Rolle für WorkSpaces Secure Browser bearbeiten

WorkSpaces Der sichere Browser erlaubt es Ihnen nicht, die `AWSServiceRoleForAmazonWorkSpacesWeb` dienstverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstverknüpften Rolle für Secure Browser WorkSpaces

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der WorkSpaces Secure Browser-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um WorkSpaces Secure Browser-Ressourcen zu löschen, die von AWSService RoleForAmazonWorkSpacesWeb

- Wählen Sie eine der folgenden Optionen aus:
  - Wenn Sie die Konsole verwenden, löschen Sie alle Ihre Portale auf der Konsole.
  - Wenn Sie die CLI oder API verwenden, trennen Sie alle Ihre Ressourcen (einschließlich Browsereinstellungen, Netzwerkeinstellungen, Benutzereinstellungen, Trust Stores und Einstellungen für die Benutzerzugriffsprotokollierung) aus Ihren Portalen. Löschen Sie diese Ressourcen und löschen Sie dann die Portale.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForAmazonWorkSpacesWeb serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für dienstverknüpfte WorkSpaces Secure Browser-Rollen

WorkSpaces Secure Browser unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS Regionen und Endpunkte.

Reaktion auf Vorfälle im Amazon WorkSpaces Secure Browser

Sie können Vorfälle erkennen, indem Sie die `SessionFailure` CloudWatch Amazon-Metrik überwachen. Um Warnmeldungen für Vorfälle zu erhalten, verwenden Sie einen CloudWatch Alarm für die `SessionFailure` Metrik. Weitere Informationen finden Sie unter Überwachung des Amazon WorkSpaces Secure Browsers mit Amazon CloudWatch.

Konformitätsprüfung für Amazon WorkSpaces Secure Browser

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz im Amazon WorkSpaces Secure Browser

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Folgendes wird derzeit von WorkSpaces Secure Browser nicht unterstützt:

- Inhalte regionsübergreifend AZs sichern
- Verschlüsselte Sicherungen
- Verschlüsselung von Inhalten, die während der Übertragung zwischen oder Regionen übertragen AZs werden
- Standard-Sicherungen oder automatische Sicherungen

Wenn Sie eine hohe Internetverfügbarkeit konfigurieren möchten, können Sie Ihre VPC-Konfiguration optimieren. Für eine hohe API-Verfügbarkeit können Sie die richtige Menge an TPS anfordern.

Infrastruktursicherheit im Amazon WorkSpaces Secure Browser

Als verwalteter Service ist Amazon WorkSpaces Secure Browser durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon WorkSpaces Secure Browser zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

WorkSpaces Secure Browser isoliert den Dienstverkehr, indem er die AWS Standard-SigV4-Authentifizierung und -Autorisierung auf alle Dienste anwendet. Der Endpunkt der Kundenressource (oder der Endpunkt des Webportals) wird durch Ihren Identitätsanbieter geschützt. Sie können den Datenverkehr weiter isolieren, indem Sie die Multi-Faktor-Autorisierung und andere Sicherheitsmechanismen in Ihrem Identitätsanbieter (IDP) verwenden.

Der gesamte Internetzugriff kann durch die Konfiguration von Netzwerkeinstellungen wie VPC, Subnetz oder Sicherheitsgruppe gesteuert werden. Mehrmandantenfähigkeit und VPC-Endpunkte (PrivateLink) werden derzeit nicht unterstützt.

Konfiguration und Schwachstellenanalyse im Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser aktualisiert und patcht Anwendungen und Plattformen nach Bedarf in Ihrem Namen, einschließlich Chrome und Linux. Sie müssen keine Patches oder Neuerstellungen durchführen. Es liegt jedoch in Ihrer Verantwortung, WorkSpaces Secure Browser gemäß den Spezifikationen und Richtlinien zu konfigurieren und die Nutzung des WorkSpaces Secure Browsers durch Ihre Benutzer zu überwachen. Alle dienstbezogenen Konfigurationen und Schwachstellenanalysen liegen in der Verantwortung von WorkSpaces Secure Browser.

Sie können eine Erhöhung des Limits für WorkSpaces Secure Browser-Ressourcen beantragen, z. B. für die Anzahl der Webportale und die Anzahl der Benutzer. WorkSpaces Secure Browser stellt die Verfügbarkeit des Dienstes und des SLA sicher.

Zugriff APIs über eine Schnittstelle VPC-Endpunkt ()AWS PrivateLink

Sie können den Amazon WorkSpaces Secure Browser API-Endpunkt direkt von einer privaten Cloud (VPC) aus aufrufen, anstatt eine Verbindung über das Internet herzustellen. Sie können dies ohne die Verwendung eines Internet-Gateways, eines NAT-Geräts, einer VPN-Verbindung oder einer Direct Connect Verbindung tun.

Sie stellen diese private Verbindung her, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen, der mit Strom versorgt wird AWS PrivateLink. Für jedes Subnetz, das Sie von Ihrer VPC aus angeben, erstellen wir eine Endpunkt-Netzwerkschnittstelle im Subnetz. Eine Endpunkt-Netzwerkschnittstelle ist eine vom Anforderer verwaltete Netzwerkschnittstelle, die als Einstiegspunkt für den Amazon WorkSpaces Secure Browser API-Verkehr dient.

Weitere Informationen finden Sie unter Access AWS Services bis. AWS PrivateLink

Topics

- Überlegungen zu Amazon WorkSpaces Secure Browser
- Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon WorkSpaces Secure Browser
- Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-VPC-Endpunkt
- Fehlerbehebung

Überlegungen zu Amazon WorkSpaces Secure Browser

Bevor Sie einen VPC-Schnittstellen-Endpunkt für Amazon WorkSpaces Secure Browser einrichten APIs, stellen Sie sicher, dass Sie die „Voraussetzungen“ unter Access AWS Services bis AWS PrivateLink lesen. Amazon WorkSpaces Secure Browser unterstützt Aufrufe all seiner API-Aktionen über den VPC-Endpunkt der Schnittstelle.

Standardmäßig ist der vollständige Zugriff auf Amazon WorkSpaces Secure Browser über den Endpunkt zulässig. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon WorkSpaces Secure Browser

Sie können einen VPC-Schnittstellen-Endpunkt für den Amazon WorkSpaces Secure Browser Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Schnittstellen-Endpunkt für Amazon WorkSpaces Secure Browser mit dem folgenden Servicenamen:

- com.amazonaws. *region*.workspaces-web

Erstellen Sie für FIPS-unterstützte Regionen einen VPC-Schnittstellen-Endpunkt für Amazon WorkSpaces Secure Browser mit dem folgenden Servicenamen:

- com.amazonaws. *region*. workspaces-web-fips

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-VPC-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-VPC-Endpunkt anhängen können. Die Standard-Endpunktrichtlinie gewährt Ihnen vollen Zugriff auf Amazon WorkSpaces Secure Browser APIs über den VPC-Endpunkt der Schnittstelle. Um den Zugriff zu kontrollieren, der Amazon WorkSpaces Secure Browser von Ihrer VPC aus gewährt wird, fügen Sie dem VPC-Endpunkt der Schnittstelle eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Amazon WorkSpaces Secure Browser-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellen-VPC-Endpunkt anhängen, gewährt sie allen Principals auf allen Ressourcen Zugriff auf die aufgelisteten Amazon WorkSpaces Secure Browser-Aktionen.

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

Fehlerbehebung

Wenn Ihre Aufrufe an den Amazon WorkSpaces Secure Browser APIs hängen bleiben, liegt wahrscheinlich eine Fehlkonfiguration in Ihrer VPC Endpoint Service-Sicherheitsgruppe oder Ihrer IAM-Rollenkonfiguration vor. Versuchen Sie Folgendes, um dieses Problem zu beheben:

- Beim Erstellen Ihres Schnittstellen-VPC-Endpunkts wurde dieser möglicherweise automatisch an Ihre AWS-Konto Standardsicherheitsgruppe angehängt. Versuchen Sie, eine andere Sicherheitsgruppe zu verwenden, und stellen Sie sicher, dass die eingehenden und ausgehenden Berechtigungen es Ihnen ermöglichen, Ihre Daten ordnungsgemäß zu übertragen.
- Stellen Sie sicher, dass Sie eine IAM-Rolle verwenden, mit der Sie Amazon WorkSpaces Secure Browser APIs aufrufen können.

Weitere Informationen finden Sie unter Was ist AWS PrivateLink? im Amazon VPC-Benutzerhandbuch.

Bewährte Sicherheitsmethoden für Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien verwenden können. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung.

Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Zu den bewährten Methoden für Amazon WorkSpaces Secure Browser gehören die folgenden:

- Um potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Nutzung des WorkSpaces Secure Browsers zu erkennen, verwenden Sie AWS CloudTrail Amazon, CloudWatch um den Zugriffsverlauf zu erkennen und nachzuverfolgen und Protokolle zu verarbeiten. Weitere Informationen erhalten Sie unter Überwachung des Amazon WorkSpaces Secure Browsers mit Amazon CloudWatch und Protokollieren von WorkSpaces Secure Browser API-Aufrufen mit AWS CloudTrail.
- Verwenden Sie CloudTrail Protokolle und Metriken, um detektive Kontrollen zu implementieren und CloudWatch Anomalien zu identifizieren. Weitere Informationen erhalten Sie unter Überwachung des Amazon WorkSpaces Secure Browsers mit Amazon CloudWatch und Protokollieren von WorkSpaces Secure Browser API-Aufrufen mit AWS CloudTrail.
- Sie können die Benutzerzugriffsprotokollierung einrichten, um Benutzerereignisse aufzuzeichnen. Weitere Informationen finden Sie unter the section called “Protokollierung von Benutzeraktivitäten einrichten”.

Um potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Verwendung von WorkSpaces Secure Browser zu verhindern, befolgen Sie diese bewährten Methoden:

- Implementieren Sie den Zugriff mit den geringsten Rechten und erstellen Sie spezielle Rollen, die für WorkSpaces Secure Browser-Aktionen verwendet werden. Verwenden Sie IAM-Vorlagen, um eine Rolle mit Vollzugriff oder Schreibschutz zu erstellen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für WorkSpaces Secure Browser.
- Seien Sie vorsichtig, wenn Sie Portal-Domains und Benutzeranmeldedaten teilen. Jeder Benutzer im Internet kann auf das Webportal zugreifen, aber er kann keine Sitzung starten, wenn er nicht über die gültigen Benutzeranmeldeinformationen für das Portal verfügt. Seien Sie vorsichtig dabei, wie, wann und an wen Sie die Anmeldeinformationen für das Webportal weitergeben.

Überwachung des Amazon WorkSpaces Secure Browsers

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon WorkSpaces Secure Browser und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie Ihre WorkSpaces Secure Browser-Portale und deren Ressourcen überwachen, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen bestimmten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen für Ihre EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von EC2 Amazon-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

Überwachung des Amazon WorkSpaces Secure Browsers mit Amazon CloudWatch

Sie können Amazon WorkSpaces Secure Browser mithilfe von Amazon überwachen CloudWatch, der Rohdaten sammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Der `AWS/WorkSpacesWeb`-Namespace enthält die folgenden Metriken.

CloudWatch Metriken für Amazon WorkSpaces Secure Browser

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
`SessionAttempt`	Die Anzahl der Amazon WorkSpaces Secure Browser-Sitzungsversuche.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionSuccess`	Die Anzahl der erfolgreichen Amazon WorkSpaces Secure Browser-Sitzungsstarts.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionFailure`	Die Anzahl der fehlgeschlagenen Amazon WorkSpaces Secure Browser-Sitzungsstarts.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
SessionIdleDisconnect	Die Anzahl der Verbindungen, die aufgrund von Benutzeraktivität geschlossen wurden.	[PortalId]	Durchschnitt	Anzahl
ActiveSession	Die Anzahl der aktiven Sitzungen auf einem Portal.	[PortalId]	Durchschnitt	Anzahl
GlobalCpuPercent	Die CPU-Auslastung der Amazon WorkSpaces Secure Browser-Sitzungsinstanz.	[PortalId] [PortalId, UserName]	Durchschnitt, Summe, Maximum, Minimum	Prozent
GlobalMemoryPercent	Die Speichernutzung (RAM) der Amazon WorkSpaces Secure Browser-Sitzungsinstanz.	[PortalId] [PortalId, UserName]	Durchschnitt, Summe, Maximum, Minimum	Prozent
DisplayLatency	Die durchschnittliche Zeit in Millisekunden zwischen Frame-Erfassung und Präsentation.	[PortalId] [PortalId, UserName]	Durchschnitt, Maximum, Minimum	Millisekunden

Metrik	Beschreibung	Dimensionen	Statistiken	Einheiten
`InputLatency`	Die Eingangslatenz zwischen Client und Server. Zum Beispiel die Latenz zwischen dem Mausklick des Clients und dem Mausklick des Servers.	`[PortalId]` `[PortalId, UserName]`	Durchschnitt, Maximum, Minimum	Millisekunden
`SessionLoggerEventDelivered`	Die Anzahl der Ereignisse, die jede übermittelte Session Logger-Datei hat.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionLoggerTargetNotFoundError`	Die Anzahl der Protokolldateizustellungen, die dazu geführt haben, dass der Bucket nicht gefunden wurde.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl
`SessionLoggerAccessDeniedError`	Die Anzahl der Protokolldateizustellungen, die dazu führten, dass Berechtigungen verweigert wurden.	`[PortalId]`	Durchschnitt, Summe, Maximum, Minimum	Anzahl

> **Note**
>
> Die metrischen Datenpunkte werden von jeder Sitzung einmal pro Minute erfasst und alle 5 Minuten veröffentlicht. CloudWatch Session Logger-Metriken werden sofort für jede Protokolldateizustellung ausgegeben.

Dimensionen für Amazon WorkSpaces Secure Browser-Metriken

Dimension	Beschreibung
PortalId	Filtert die Metrikdaten für Amazon WorkSpaces Secure Browser für ein bestimmtes Portal.
UserName	Filtert die Metrikdaten für Amazon WorkSpace s Secure Browser für ein bestimmtes Portal und einen bestimmten Benutzer.

Sie können die SessionLoggerEventDeliveredMetrik verwenden, um die Gesamtzahl der Ereignisse in Ihrem Portal zu überwachen oder die Anzahl der übermittelten Protokolldateien zu ermitteln, indem Sie die Anzahl der Datenpunkte zählen, anstatt Werte zu summieren. Wir empfehlen, Alarme für die SessionLoggerAccessDeniedErrorMetriken SessionLoggerTargetNotFoundErrorund zu konfigurieren, um das versehentliche Löschen von Ressourcen oder Berechtigungen zu erkennen.

Protokollieren von WorkSpaces Secure Browser API-Aufrufen mit AWS CloudTrail

WorkSpaces Secure Browser ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Amazon WorkSpaces Secure Browser bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon WorkSpaces Secure Browser als Ereignisse. Dazu gehören Aufrufe von der Amazon WorkSpaces Secure Browser-Konsole und Codeaufrufen für Amazon WorkSpaces Secure Browser API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon WorkSpaces Secure Browser. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon WorkSpaces Secure Browser gestellt wurde, die IP-Adresse,

von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, sowie weitere Details identifizieren.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Themen

- WorkSpaces Informationen zum sicheren Browser in CloudTrail
- Grundlegendes zu den Einträgen in WorkSpaces Secure Browser-Protokolldateien

WorkSpaces Informationen zum sicheren Browser in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität im Amazon WorkSpaces Secure Browser auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Im Ereignisverlauf können Sie aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Amazon WorkSpaces Secure Browser, können Sie einen Trail erstellen. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Amazon WorkSpaces Secure Browser-Aktionen werden von der Amazon WorkSpaces API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von `DeleteUserSettings` und `ListBrowserSettings` Aktionen Einträge in den CloudTrail Protokolldateien. `CreatePortal`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in WorkSpaces Secure Browser-Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter und andere Details. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListBrowserSettings` Aktion demonstriert.


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
```

```
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
        "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    },
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
```

```
        "eventCategory": "Management"
    }]
}
```

Protokollierung von Benutzeraktivitäten im Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser ermöglicht es Kunden, Sitzungsereignisse im Zusammenhang mit Benutzeraktivitäten in den Secure Browser-Sitzungen zu protokollieren.

WorkSpaces Secure Browser bietet zwei Optionen für die Protokollierung von Benutzeraktivitäten und sicherheitsrelevanten Ereignissen:

- Session Logger erfasst eine Vielzahl von Sitzungsereignissen. Diese Protokolle werden an einen Amazon S3 S3-Bucket in Ihrem Konto übermittelt, was eine einfache Integration mit Ihrer bevorzugten SIEM-Plattform ermöglicht.
- Die Benutzerzugriffsprotokollierung erfasst die kritischsten Sitzungsereignisse. Diese Protokolle werden zur Verarbeitung und Analyse in Echtzeit in einen Amazon Kinesis Kinesis-Stream gestreamt.

Weitere Informationen zur Einrichtung dieser Optionen finden Sie unter the section called “Session Logger einrichten” und. the section called “Protokollierung des Benutzerzugriffs einrichten”

Themen

- Sitzungsereignisse im Session Logger für Amazon WorkSpaces Secure Browser
- Sitzungsereignisse in der Benutzerzugriffsprotokollierung für Amazon WorkSpaces Secure Browser

Sitzungsereignisse im Session Logger für Amazon WorkSpaces Secure Browser

Der Sitzungslogger erfasst verschiedene sitzungsbezogene Ereignisse zu Überwachungs- und Prüfungszwecken.

Sie können Session Logger so konfigurieren, dass alle Sitzungsereignisse oder eine ausgewählte Teilmenge erfasst werden, je nach den Anforderungen des WorkSpaces Secure Browser-Portals.

Weitere Informationen zur Konfiguration finden Sie unterthe section called “Session Logger einrichten”.

Um die Privatsphäre der Benutzer zu wahren, zeichnet Session Logger keine vertraulichen Inhalte auf, wie z. B. Daten aus der Zwischenablage oder Inhalte von hoch- oder heruntergeladenen Dateien.

Die folgenden Felder sind in allen Ereignissen enthalten:

- Time (Zeit)
- Username
- Portal-ID
- Portal-IP
- Client-IP
- Sitzungs-ID

Name	Beschreibung	Zusätzliche Felder, die in der Veranstaltung enthalten sind
SessionStart	Eine sichere Browsersitzung wurde gestartet, aber der Benutzer hat noch keine Verbindung hergestellt.	
SessionConnect	Der Benutzer ist mit der sicheren Browsersitzung verbunden.	
TabOpen	In seiner sicheren Browsersitzung hat der Benutzer eine neue Registerkarte geöffnet, oder er hat einen Link in einer neuen Registerkarte geöffnet.	Hostname, Pfad, URL (wenn der Benutzer einen Link in einer neuen Registerkarte öffnet), keine (wenn der Benutzer eine neue Registerkarte öffnet)
UrlVisit	In seiner Browsersitzung navigierte der Benutzer zu einer URL.	Hostname, Pfad, URL

Name	Beschreibung	Zusätzliche Felder, die in der Veranstaltung enthalten sind
WebsiteInteract	Der Benutzer hat ein Standard-HTML-Element auf einer Website geändert (z. B. klickt er auf ein Kontrollk ästchen, ein Optionsfeld oder eine Schaltfläche oder wählt ein Element in der Drop-down-Liste aus).	Hostname, Pfad, URL
TabClose	In seiner Browsersitzung hat der Benutzer einen Tab geschlossen.	Hostname, Pfad, URL (wenn der Benutzer einen Tab schließt, zu dem er navigiert hat), keine (wenn der Benutzer einen neuen Tab schließt)
ContentTransferFro mLocalToRemoteClipboard	Der Benutzer hat die Zwischenablage im sicheren Browser mithilfe von Inhalten aus seinem lokalen Browser (außerhalb der sicheren Umgebung) aktualisiert. Dieses Update kann entweder durch Kopieren von Inhalten über die Sitzungs-Symbollei ste oder durch Übertragung von Daten über Tastenkom binationen (Strg+C/Strg+V) erfolgen.	

Name	Beschreibung	Zusätzliche Felder, die in der Veranstaltung enthalten sind
ContentCopyFromWebsite	Der Benutzer hat die Zwischenablage im sicheren Browser mithilfe von Inhalten aus dem sicheren Browser (in der sicheren Umgebung) aktualisiert.	Hostname, Pfad, URL
ContentPasteToWebsite	Der Inhalt der Zwischenablage wurde in eine Webseite im Browser eingefügt. (Dieses Ereignis erfasst keine Fälle, in denen Inhalt der Zwischena blage in die URL-Leiste des Browsers eingefügt wird.)	Hostname, Pfad, URL
PrintJobSubmit	Der Benutzer hat einen Anforderungsauftrag an den virtuellen Drucker des Browsers („DCV-Drucker“) gesendet. Der Inhalt wird als PDF auf dem lokalen Computer des Benutzers gespeichert.	Dateiname, Größe, Erweiteru ng
FileDownloadFromSe cureBrowserToRemoteDisk	Eine Datei wurde aus der Sitzung auf der lokalen Festplatte der Remote-Instanz gespeichert.	Hostname, Pfad URLfilename, Größe, Erweiterung
FileTransferFromRe moteToLocalDisk	Eine Datei wurde von der Festplatte der Remote-In stanz auf das lokale Gerät des Benutzers heruntergeladen.	Dateiname, Größe, Erweiteru ng

Name	Beschreibung	Zusätzliche Felder, die in der Veranstaltung enthalten sind
FileUploadFromRemoteDiskToSecureBrowser	Eine auf der lokalen Festplatte der Remote-Instanz gespeicherte Datei wurde über die Browsersitzung auf eine Filesharing-SaaS-Plattform (z. B. Google Drive, Box oder File.io) hochgeladen.	
FileTransferFromLocalToRemoteDisk	Eine Datei wurde vom Benutzergerät in die sichere Browsersitzung hochgeladen.	Dateiname, Größe und Erweiterung
SessionDisconnection	Der Benutzer wird von der sicheren Browsersitzung getrennt.	
SessionEnd	Die sichere Browsersitzung wurde beendet. Die Kündigung kann auf drei Arten erfolgen: Der Administrator beendet die Sitzung über den Benutzersitzungsmanager in der Konsole, der Benutzer beendet die Sitzung manuell mithilfe der Option Sitzung beenden in der Werkzeugleiste, oder die Sitzung läuft ab, nachdem eine vom Administrator festgelegte Dauer überschritten wurde.	

Jedes Ereignis folgt dem OCSF-Standard und umfasst eine Liste von Attributen, die allen Ereignissen gemeinsam sind:

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
    activity_id : Integer | OCSF standard value 99 for 'others'
    category_name : "WorkSpacesSecureBrowser" | The category name where the event
 belongs to.
    category_id : 2 | Numerical identifier for category,
    metadata : link | Required {
        product : link {
            vendor_name : "wsb",
            name : "WorkSpacesSecureBrowser"
        }
        version : String | Version of the schema | eg. 1.0.0
    },
    severity_id : 1 | The severity of the event. All events will have a severity of 1,
 meaning 'Informational',
    type_id : class_uid * 100 + activity_id
    time : The time the event happened (RFC3339 format),
    observables : link [
        {
            name : "session_detail.portal_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.session_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.client_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.portal_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.username",
            type_id : 10 //Resource UID
            value : //Generated value
```

```
        }
    ],

    // New Events
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
        username : String | The logged-in username | eg. bobross
    }
}
```

Im Folgenden finden Sie ein Beispiel für das URLVisit Ereignis:

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

Im Folgenden finden Sie ein Beispiel für die PrintJobSubmit Veranstaltung:

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
}
```

Session Logger-Metriken für Amazon WorkSpaces Secure Browser

Session Logger gibt die folgenden Amazon CloudWatch Metriken aus.

Sie können die SessionLoggerEventDeliveredMetrik verwenden, um die Gesamtzahl der Ereignisse in Ihrem Portal zu überwachen oder die Anzahl der übermittelten Protokolldateien zu ermitteln, indem Sie die Anzahl der Datenpunkte zählen, anstatt Werte zu summieren. Wir empfehlen, Alarme für die SessionLoggerAccessDeniedErrorMetriken SessionLoggerTargetNotFoundErrorund zu konfigurieren, um das versehentliche Löschen von Ressourcen oder Berechtigungen zu erkennen.

> **Note**
>
> Metrische Datenpunkte werden von jeder Sitzung einmal pro Minute erfasst und alle 5 Minuten veröffentlicht. Amazon CloudWatch Session Logger-Metriken werden sofort für jede Protokolldateizustellung ausgegeben.

Session Logger-Metriken

Metrik	Beschreibung	Dimension	Statistiken	Einheit
SessionLoggerEventDelivered	Die Anzahl der Ereignisse, die jede übermittelte Session-Logger-Datei hat.	[PortalId]	Durchschnitt, Summe, Maximum, Minimum	Anzahl
SessionLoggerTargetNotFoundError	Die Anzahl der Protokolldateizustellungen, die dazu geführt haben, dass der Bucket nicht gefunden wurde.	[PortalId]	Durchschnitt, Summe, Maximum, Minimum	Anzahl
SessionLoggerAccessDeniedError	Die Anzahl der Protokolldateizustellungen, die dazu führten, dass Berechtigungen verweigert wurden.	[PortalId]	Durchschnitt, Summe, Maximum, Minimum	Anzahl

Sitzungsereignisse in der Benutzerzugriffsprotokollierung für Amazon WorkSpaces Secure Browser

Die folgenden Sitzungsereignisse sind für die Benutzerzugriffsprotokollierung verfügbar:

- Validierung: Das Ereignis wurde erfolgreich in den Kinesis-Datenstrom übertragen.
- StartSession: Der Benutzer hat eine Sitzung gestartet und ist mit der sicheren Browsersitzung verbunden.
- VisitPage: Der Benutzer besucht eine Seite in der Sitzung.

- EndSession: Der Benutzer hat die Sitzung beendet.

URL-Navigationsprotokolle werden aus dem Browserverlauf aufgezeichnet. URLs nicht im Browserverlauf aufgezeichnet (entweder im Inkognitomodus besucht oder aus dem Browserverlauf gelöscht) werden nicht in Protokollen aufgezeichnet. Es liegt an den Kunden, anhand ihrer Browserrichtlinie zu entscheiden, ob sie den Inkognitomodus oder das Löschen des Verlaufs deaktivieren möchten.

Im Folgenden finden Sie ein Beispiel für jedes verfügbare Ereignis. Die folgenden Felder sind immer für jedes Ereignis enthalten:

- timestamp ist als Epochenzeit in Millisekunden enthalten.
- EventType ist als Zeichenfolge enthalten.
- details ist als weiteres JSON-Objekt enthalten.
- portalArn und userName sind für jedes Ereignis mit Ausnahme von Validation enthalten.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
```

```
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

Anleitung für Benutzer von Amazon WorkSpaces Secure Browser

Administratoren verwenden WorkSpaces Secure Browser, um Webportale zu erstellen, die eine Verbindung zu Unternehmenswebsites herstellen, z. B. zu internen Websites, software-as-a-service (SAAS) -Webanwendungen oder dem Internet. Endbenutzer greifen über ihre vorhandenen Webbrowser auf diese Webportale zu, um eine Sitzung zu starten und auf Inhalte zuzugreifen.

Der folgende Inhalt hilft Endbenutzern, die mehr über den Zugriff auf WorkSpaces Secure Browser, das Starten und Konfigurieren einer Sitzung sowie die Verwendung der Werkzeugleiste und des Webbrowsers erfahren möchten.

Topics

Browser- und Gerätekompatibilität für Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser wird vom Amazon DCV-Webbrowser-Client unterstützt, der in einem Webbrowser ausgeführt wird, sodass keine Installation erforderlich ist. Der Webbrowser-Client wird von gängigen Webbrowsern wie Chrome und Firefox sowie von den wichtigsten Desktop-Betriebssystemen wie Windows, macOS und Linux unterstützt.

Die meisten up-to-date Informationen zur Unterstützung von Webbrowser-Clients finden Sie unter Webbrowser-Client.

> **Note**
>
> Webcam-Unterstützung ist derzeit nur in Chromium-basierten Browsern wie Google Chrome und Microsoft Edge verfügbar. Derzeit unterstützen Apple Safari und Mozilla FireFox keine Webcam.

Zugriff auf das Webportal für Amazon WorkSpaces Secure Browser

Ihr Administrator kann den Zugriff auf Ihr Webportal mit den folgenden Optionen gewähren:

- Sie können einen Link aus einer E-Mail oder Website auswählen und sich dann mit Ihren SAML-Identitätsdaten anmelden.
- Sie können sich bei Ihrem SAML-Identitätsanbieter (wie Okta, Ping oder Azure) anmelden und mit einem Klick von der Anwendungsstartseite Ihres SAML-Anbieters aus eine Sitzung starten (z. B. das Okta-Endbenutzer-Dashboard oder das Azure-Myapps-Portal).

Sitzungsanleitung für Amazon WorkSpaces Secure Browser

Nachdem Sie sich beim Webportal angemeldet haben, können Sie eine Sitzung starten und während Ihrer Sitzung verschiedene Aktionen ausführen.

Topics

Eine Sitzung im Amazon WorkSpaces Secure Browser starten

Nachdem Sie sich angemeldet haben, um eine Sitzung zu starten, werden die Meldung Sitzung wird gestartet und der Fortschrittsbalken angezeigt. Dies bedeutet, dass Amazon WorkSpaces Secure Browser eine Sitzung für Sie erstellt. Hinter den Kulissen erstellt Amazon WorkSpaces Secure Browser die Instance, startet den verwalteten Webbrowser und wendet Administratoreinstellungen und Browserrichtlinien an.

Wenn Sie sich zum ersten Mal in Ihrem Webportal anmelden, werden blaue Plus-Symbole in der Symbolleiste angezeigt. Dieses Symbol weist darauf hin, dass eine Anleitung verfügbar ist, das Sie durch die in der Symbolleiste verfügbaren Features führt. Mithilfe dieser Symbole können Sie lernen, wie Folgendes tun:

- Erlauben Sie Browserberechtigungen für das Mikrofon, die Webcam und die Zwischenablage, indem Sie das Schlosssymbol neben Ihrem lokalen Browser auswählen und den Schalter neben der Zwischenablage, dem Mikrofon und der Kamera auf Ein umstellen.

  > **Note**
  >
  > Wenn Sie zu Beginn Ihrer ersten Sitzung die Webcam-Berechtigungen aktivieren, wird die Webcam kurzzeitig aktiviert und eine LED auf Ihrem Computer blinkt. Dadurch wird der lokale Browserzugriff auf Ihre Webcam gewährt.

- Aktivieren Sie Amazon WorkSpaces Secure Browser, um zusätzliche Monitorfenster zu öffnen, indem Sie das Schlosssymbol in Ihrem Browser und die Einstellung Popups immer zulassen auswählen.

Wenn Sie eine Anleitung erneut starten möchten, können Sie in der Symbolleiste Profil, Hilfe und Anleitung starten auswählen.

Verwenden der Werkzeugleiste im Amazon WorkSpaces Secure Browser

Gehen Sie wie folgt vor, um zu erfahren, wie Sie die Werkzeugleiste verwenden.

Wenn Sie die Symbolleiste verschieben möchten, wählen Sie die hellere Leiste im oberen Bereich der Symbolleiste aus, ziehen Sie sie an die gewünschte Position und lassen Sie sie dann los, um sie abzulegen.

Um die Werkzeugleiste zu reduzieren, bewegen Sie den Mauszeiger darüber und wählen Sie die Schaltfläche mit dem Aufwärtspfeil aus, oder doppelklicken Sie auf die hellere Leiste im oberen Bereich. In der minimierten Ansicht haben Sie mehr Platz auf dem Bildschirm und können mit einem Klick auf die am häufigsten verwendeten Symbole zugreifen.

Um die Anzeige zu vergrößern, wählen Sie das Browserfenster aus und vergrößern Sie die Ansicht. Um die Anzeige der Symbole und des Texts in der Werkzeugleiste zu vergrößern, wählen Sie die Werkzeugleiste aus und vergrößern Sie sie.

Gehen Sie wie folgt vor, um auf einem Windows-Gerät die Ansicht zu vergrößern oder zu verkleinern:

1. Wählen Sie die Werkzeugleiste oder den Webinhalt aus.
2. Drücken Sie Strg + +, um die Ansicht zu vergrößern, oder drücken Sie Strg + -, um die Ansicht zu verkleinern.

Gehen Sie wie folgt vor, um auf einem Mac-Gerät die Ansicht zu vergrößern oder zu verkleinern:

1. Wählen Sie die Werkzeugleiste oder den Webinhalt aus.
2. Drücken Sie Cmd + +, um die Ansicht zu vergrößern, oder drücken Sie Cmd + -, um die Ansicht zu verkleinern.

Um die Werkzeugleiste am oberen Bildschirmrand anzudocken, wählen Sie unter Werkzeugleistenmodus Einstellungen, Allgemein und Angedockt aus.

Die folgende Tabelle enthält eine Beschreibung aller verfügbaren Symbole in der Symbolleiste:

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> Die Symbole für „Zwischenablage“ und „Dateien“ sind standardmäßig ausgeblendet, sofern Ihr Administrator diese Berechtigungen nicht erteilt. Nur Administratoren können die Zwischenablage und Dateien in einem Webportal aktivieren oder deaktivieren. Wenn diese Symbole ausgeblendet sind und Sie darauf zugreifen müssen, wenden Sie sich an Ihren Administrator.

Den Browser im Amazon WorkSpaces Secure Browser verwenden

Wenn Sie Ihre Sitzung starten, zeigt der Browser die Startup-URL an. Dabei handelt es sich um eine URL, die von Ihrem Administrator ausgewählt wurde. Wenn der Administrator keine Startup-URL ausgewählt hat, wird Ihnen die Standardumgebung mit neuen Registerkarten von Google Chrome angezeigt.

Im Browser können Sie Registerkarten öffnen, zusätzliche Browserfenster starten (über das Windows-Symbolleistensymbol oder das Dreipunktmenü des Browsers), eine URL eingeben bzw. in der URL-Leiste suchen oder über verwaltete Lesezeichen zu Websites wechseln. Wenn Sie auf Lesezeichen für das Webportal zugreifen möchten, öffnen Sie den Ordner Verwaltete Lesezeichen in der Lesezeichenleiste (unter der URL-Leiste) oder öffnen Sie den Lesezeichen-Manager über das Dreipunktmenü auf der rechten Seite der URL-Leiste.

Wenn Sie die Größe des Browserfensters ändern oder das Fenster verschieben möchten, ziehen Sie die Leiste mit den Registerkarten von Chrome nach unten. Dadurch steht während der Sitzung auf dem Bildschirm mehr Platz für mehrere Browserfenster zur Verfügung.

> **Note**
>
> Browser-Features wie der Inkognitomodus sind während Ihrer Sitzung möglicherweise nicht verfügbar, wenn Ihr Administrator sie deaktiviert hat.

Eine Sitzung im Amazon WorkSpaces Secure Browser beenden

Wenn Sie eine Sitzung beenden möchten, wählen Sie Profil und Sitzung beenden aus. Nach dem Ende einer Sitzung löscht Amazon WorkSpaces Secure Browser alle Daten aus der Sitzung. Nach

dem Ende einer Sitzung sind keine Browserdaten wie geöffnete Websites, Verlauf, Dateien oder Daten aus dem Datei-Explorer verfügbar.

Wenn Sie während einer aktiven Sitzung eine Registerkarte schließen, endet die Sitzung nach einem von Ihrem Administrator festgelegten Zeitraum. Wenn Sie die Registerkarte schließen und das Webportal vor dieser Zeitüberschreitung erneut aufrufen, können Sie der aktuellen Sitzung beitreten und alle Ihre vorherigen Sitzungsdaten anzeigen, z. B. geöffnete Websites und Dateien.

Behebung von Benutzerproblemen im Amazon WorkSpaces Secure Browser

Wenn Sie bei der Verwendung von WorkSpaces Secure Browser auf eines der folgenden Probleme stoßen, versuchen Sie es mit den folgenden Lösungen.

Mein Amazon WorkSpaces Secure Browser-Portal lässt mich nicht anmelden. Ich habe die Fehlermeldung „Ihr Webportal ist noch nicht eingerichtet“ erhalten. Wenden Sie sich an Ihren IT-Administrator, um Hilfe zu erhalten“.

Ihr Administrator muss die Portalerstellung mit einem SAML-2.0-Identitätsanbieter abschließen, damit Sie sich anmelden können. Wenden Sie sich an Ihren Administrator, um Hilfe zu erhalten.

Mein Portal startet keine Sitzung. Ich habe die Fehlermeldung „Sitzung konnte nicht reserviert werden“ erhalten. Es ist ein interner Fehler aufgetreten. Bitte versuchen Sie es erneut.“

Beim Start Ihrer Webportal-Sitzung ist ein Problem aufgetreten. Versuchen Sie erneut, die Sitzung zu starten. Wenn das Problem weiterhin besteht, bitten Sie Ihren Administrator um Hilfe.

Ich kann die Zwischenablage, das Mikrofon oder die Webcam nicht verwenden.

Wenn Sie Browserberechtigungen zulassen möchten, klicken Sie auf das Schlosssymbol neben der URL und schalten Sie den blauen Schalter neben Zwischenablage, Mikrofon, Kamera und Pop-ups und Weiterleitungen um, damit dieses Feature aktiviert wird.

> **Note**
>
> Wenn Ihr Webbrowser die Video- oder Audioeingabe nicht unterstützt, werden diese Optionen nicht in der Symbolleiste angezeigt.

Amazon WorkSpaces Secure Browser Echtzeit-Audiovideo (AV) leitet Ihr lokales Webcam-Video und Ihren Mikrofon-Audioeingang an die Browser-Streaming-Sitzung weiter. Auf diese Weise können Sie innerhalb Ihrer Streaming-Sitzung mit Chromium-basierten Webbrowsern wie Google Chrome oder Microsoft Edge Ihre lokalen Geräte für Video- und Audiokonferenzen verwenden. Webcam wird derzeit in Browsern, die nicht Chromium-basiert sind, nicht unterstützt.

Informationen zur Konfiguration von Google Chrome finden Sie unter Kamera und Mikrofon verwenden in Chrome.

Mein Webportal öffnet kein zusätzliches Monitorfenster.

Wenn Sie versuchen, zwei Monitore zu starten und am Ende der Adressleiste im oberen Browser ein Symbol für Pop-ups blockiert angezeigt wird, wählen Sie das Symbol und das Optionsfeld neben Pop-ups und Weiterleitungen immer zulassen aus. Wenn Pop-ups zulässig sind, wählen Sie in der Symbolleiste das Symbol für zwei Monitore aus, um ein neues Fenster zu öffnen. Positionieren Sie das Fenster auf Ihrem Monitor neu und ziehen Sie eine Browser-Registerkarte in das Fenster.

Wenn ich versuche, Dateien aus dem Dateibereich herunterzuladen, passiert nichts.

Wenn Sie versuchen, Dateien aus dem Bereich Dateien herunterzuladen und am Ende der Adressleiste im oberen Browser ein Symbol für Pop-ups blockiert angezeigt wird, wählen Sie das Symbol und das Optionsfeld neben Pop-ups und Weiterleitungen immer zulassen aus. Wenn Pop-ups zulässig sind, versuchen Sie erneut, die Dateien herunterzuladen.

Woran erkenne ich, welche and/or Mikrofon-Webcam verwendet wird, und wie kann ich sie ändern?

Klicken Sie auf den Abwärtspfeil neben dem Mikrofon oder der Kamera. Im Menü werden verfügbare Geräte angezeigt, wobei ein Häkchen Ihr aktuelles Gerät anzeigt. Wählen Sie ein anderes Gerät aus, um das Gerät zu ändern, das Sie für Ihre Sitzung verwenden möchten.

Mein Webportal wird nicht gestartet, wenn es direkt über die benutzerdefinierte Domain des Unternehmens aufgerufen wird

Wenn Sie versuchen, eine Sitzung mit einem Domainnamen wie workspaces-web.com zu start`enacme.secureportal.mycompany.com`, stellen Sie sicher, dass in Ihrem Browser Drittanbieter-Cookies für die Unternehmensdomain aktiviert sind, auf die Sie zugreifen.

Single Sign-On-Erweiterung für Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser bietet eine Erweiterung für Single Sign-On mit Chrome- und Firefox-Browsern auf Desktop-Computern. Wenn Ihr Administrator die Erweiterung aktiviert hat, werden Sie vom Webportal bei der Anmeldung aufgefordert, die Erweiterung zu installieren.

Amazon WorkSpaces Secure Browser hat die Erweiterung entwickelt, um Single Sign-On auf Websites während Ihrer Sitzung zu ermöglichen. Wenn Sie sich beispielsweise mit einem SAML-2.0-Identitätsanbieter (wie Okta oder Ping) bei Ihrem Webportal anmelden und während Ihrer Sitzung eine Website besuchen, die denselben Identitätsanbieter verwendet, kann die Erweiterung den Zugriff auf die Website erleichtern, indem zusätzliche Anmeldeaufforderungen entfernt werden.

Sie müssen die Erweiterung nicht installieren, um auf Ihr Webportal zugreifen zu können, aber sie kann Ihr Erlebnis verbessern, da Sie weniger oft aufgefordert werden, Ihren Benutzernamen und Ihr Passwort einzugeben.

Wenn Sie sich anmelden, sucht die Erweiterung nach den Cookies, die Ihr Administrator für Ihre Sitzung angegeben hat. Alle von der Erweiterung gefundenen Daten, werden im Ruhezustand und während der Übertragung verschlüsselt. Keine dieser Daten wird in Ihrem lokalen Browser gespeichert. Wenn Sie Ihre Sitzung beenden, werden alle Ihre Sitzungsdaten (z. B. geöffnete Registerkarten, heruntergeladene Dateien und Cookies, die an die Sitzung gesendet oder während der Sitzung erstellt wurden) gelöscht.

Topics

Kompatibilität der Single Sign-On-Erweiterung für Amazon WorkSpaces Secure Browser

Die Single Sign-On-Erweiterung funktioniert mit den folgenden Geräten und Browsern:

- Geräte
  - Laptops

  - Desktop-Computer
- Browser
  - Google Chrome
  - Mozilla Firefox

Installation der Single Sign-On-Erweiterung für Amazon WorkSpaces Secure Browser

Gehen Sie folgendermaßen vor, um die Single Sign-On-Erweiterung zu installieren.

Wenn Sie sich im Portal anmelden, folgen Sie der Aufforderung, die Erweiterung für Ihren Chrome- oder Firefox-Browser zu installieren. Sie müssen dies für jeden Webbrowser nur einmal tun.

Wenn Sie das Gerät wechseln, auf demselben Gerät zu einem anderen Browser wechseln oder die Erweiterung aus Ihrem lokalen Browser löschen, werden Sie beim Start Ihrer nächsten Sitzung aufgefordert, die Erweiterung zu installieren.

Um sicherzustellen, dass die Erweiterung wie erwartet funktioniert, verwenden Sie die Erweiterung in einem normalen Browserfenster und nicht in Inkognito (Chrome) oder Privates Surfen (Firefox).

Fehlerbehebung bei der Single Sign-On-Erweiterung für Amazon WorkSpaces Secure Browser

Bei der Verwendung der Single Sign-On-Erweiterung kann das folgende Problem auftreten.

Wenn Sie die Erweiterung installiert haben, Sie aber während Ihrer Sitzung immer noch zur Anmeldung aufgefordert werden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie die Amazon WorkSpaces Secure Browser-Erweiterung in Ihrem Browser installiert haben. Falls Sie Ihre Browserdaten gelöscht haben sollten, haben Sie die Erweiterung möglicherweise versehentlich entfernt.
2. Stellen Sie sicher, dass Sie nicht im Inkognito-Modus (Chrome) oder im privaten Modus (Firefox) surfen. Diese Modi können zu Problemen mit Erweiterungen führen.
3. Wenn das Problem weiterhin besteht, bitten Sie Ihren Portaladministrator um weitere Hilfe.

Dokumentenverlauf für das Amazon WorkSpaces Secure Browser Administration Guide

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon WorkSpaces Secure Browser beschrieben.

Änderung	Beschreibung	Datum
Sitzungsprotokollierung	Richten Sie den Sitzungslogger ein, um eine Vielzahl von Sitzungsereignissen zu erfassen.	1. August 2025
CloudWatch Metriken	Aktualisierte CloudWatch Metriken.	21. Juli 2025
Steuerelemente in der Symbolleiste	Mit den Steuerelementen in der Werkzeugleiste können Sie die Darstellung der Werkzeugleiste für Endbenutzersitzungen konfigurieren.	21. Februar 2025
Zugriff APIs über eine Schnittstelle VPC-Endpunkt ()AWS PrivateLink	Rufen Sie den Amazon WorkSpaces Secure Browser API-Endpunkt direkt von einer privaten Cloud (VPC) aus auf, anstatt eine Verbindung über das Internet herzustellen.	10. Januar 2025
Datenschutzeinstellungen	Fügen Sie Datenschutzeinstellungen hinzu, um zu verhindern, dass Daten während einer Sitzung geteilt werden.	20. November 2024
FIPS-Endpunkte	Schützen Sie Daten während der Übertragung mit FIPS-Endpunkten.	7. Oktober 2024

Dashboard für die Sitzungsverwaltung	Verwenden Sie das Sitzungsverwaltungs-Dashboard, um aktive und abgeschlossene Sitzungen zu überwachen und zu verwalten.	19. September 2024
Deep-Links zulassen	Erlauben Sie Portalen den Empfang von Deep-Links, die Benutzer während einer Sitzung mit einer bestimmten Website verbinden.	25. Juni 2024
Aktualisierung der verwalteten Richtlinien	AmazonWorkSpacesSecureBrowserReadOnly Verwaltete Richtlinie hinzugefügt	24. Juni 2024
Verwenden Sie die Werkzeugleiste zum Zoomen	Mit der Werkzeugleiste können Sie das Display, die Symbole und den Text vergrößern.	1. Mai 2024
Neue Einstellungen für das Webportal	Sie können jetzt den Instanztyp und die maximale Anzahl gleichzeitiger Benutzer für Ihr Webportal angeben.	22. April 2024
CloudWatch Metriken	Hinzugefügt GlobalCpuPercent und GlobalMemoryPercent Metriken.	26. Februar 2024
Richten Sie die URL-Filterung ein	Mithilfe der Chrome-Richtlinie können Sie filtern, auf welche URLs Nutzer von ihrem Remote-Browser aus zugreifen können.	21. Februar 2024

IdP-Authentifizierungstypen	Sie können entweder den Standard- oder den IAM Identity Center-Authentifiz ierungstyp wählen.	5. Februar 2024
Erweiterung für Single-Sign-On aktivieren	Sie können eine Erweiterung für Ihre Endbenutzer aktiviere n, um die Portalanmeldung zu verbessern.	28. August 2023
Benutzeranleitung für Amazon WorkSpaces Secure Browser	Es wurden Inhalte hinzugefü gt, die Endbenutzern helfen, die mehr über den Zugriff auf Amazon WorkSpaces Secure Browser, das Starten und Konfigurieren einer Sitzung sowie die Verwendun g der Werkzeugleiste und des Webbrowsers erfahren möchten.	17. Juli 2023
IP-Zugriffskontrollen	WorkSpaces Mit Secure Browser können Sie steuern, von welchen IP-Adressen aus auf Ihr Webportal zugegriffen werden kann.	31. Mai 2023
Aktualisierung der verwalteten Richtlinien	Die AmazonWorkSpacesWe bReadOnly verwaltete Richtlini e wurde aktualisiert	15. Mai 2023
Identitätsanbieteraktualisi erung konfigurieren	WorkSpaces Secure Browser bietet zwei Authentifizierungs typen: Standard und AWS IAM Identity Center	15. März 2023

Aktualisierung der Browser-Richtlinie	Der Abschnitt mit den Browser-Richtlinien wurde aktualisiert und neu strukturiert.	31. Januar 2023
Aktualisierung der verwalteten Richtlinien	Die AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie wurde aktualisiert	15. Dezember 2022
Zulassungsliste und Sperrliste	Geben Sie die Zulassungsliste und die Sperrliste an, um eine Liste von Domains anzugeben, auf die Ihre Benutzer zugreifen können oder nicht.	14. November 2022
Aktualisierung der verwalteten Richtlinien	Die AmazonWorkSpacesWebReadOnly verwaltete Richtlinie wurde aktualisiert	02. November 2022
Aktualisierung der verwalteten Richtlinien	Die AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie wurde aktualisiert	24. Oktober 2022
Benutzerzugriffsprotokollierung	Die Benutzerzugriffsprotokollierung zum Aufnehmen von Benutzerereignissen wurde eingerichtet.	17. Oktober 2022
Netzwerkaktualisierungen	Es wurden verschiedene Aktualisierungen im Abschnitt „Netzwerk und Zugriff“ vorgenommen.	22. September 2022
Aktualisierung der verwalteten Richtlinien	Die AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie wurde aktualisiert	6. September 2022

Benutzersitzungen konfigurieren	Den Eingabemethoden-Editor (IME) und die sitzungsinterne Lokalisierung konfigurieren	28. Juli 2022
Netzwerkaktualisierungen	Es wurden verschiedene Aktualisierungen im Abschnitt „Netzwerk und Zugriff“ vorgenommen.	7. Juli 2022
Zeitüberschreitungswerte	Geben Sie das Zeitübers chreitung beim Trennen der Verbindung in Minuten und das Zeitüberschreitung beim Trennen der Verbindung bei Nichtbenutzung in Minuten an.	16. Mai 2022
Verwaltete Richtlinie aktualisiert	Die AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie wurde aktualisiert, um den AWS/Usage Namespace zu den PutMetricData API-Berechtigungen hinzuzufügen	6. April 2022
Serviceverknüpfte Rolle	Neue AWSService RoleForAmazonWorkSpacesWeb serviceverknüpfte Rolle	30. November 2021
Verwaltete Richtlinie	Neue AmazonWorkSpacesWebReadOnly verwaltete Richtlinie	30. November 2021
Verwaltete Richtlinie	Neue AmazonWorkSpacesWebServiceRolePolicy verwaltete Richtlinie	30. November 2021

Erstversion	Erste Version des WorkSpaces Secure Browser Administration Guide	30. November 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.