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 AppStream 2.0 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

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 serviceverknüpften Rollen”.
- Konsolen-URLs, die workspaces-web enthalten.
- Dokumentations-URLs, die workspaces-web enthalten. 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 bleiben die vorhandenen Portal-URLs unverändert. URLs für Portale, die vor dem 20. Mai 2024 erstellt wurden, verwendeten das Format <UUID>.workspaces-web.com. WorkSpaces Secure Browser-Portale verwenden weiterhin dieses Format und die Domäne workspaces-web.com.

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

Um Ihnen die ersten Schritte mit 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 Metadaten-Austauschdatei hochladen, die Sie von Ihrem IdP heruntergeladen haben.

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 aufgelisteten VPCs, 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 die PCAs in Ihrem Trust Store hinzufügen oder ändern. 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 Vertrauensspeicher hinzufügen, damit Ihr Benutzer im abgesicherten Browser auf diese Site zugreifen kann. WorkSpaces

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.

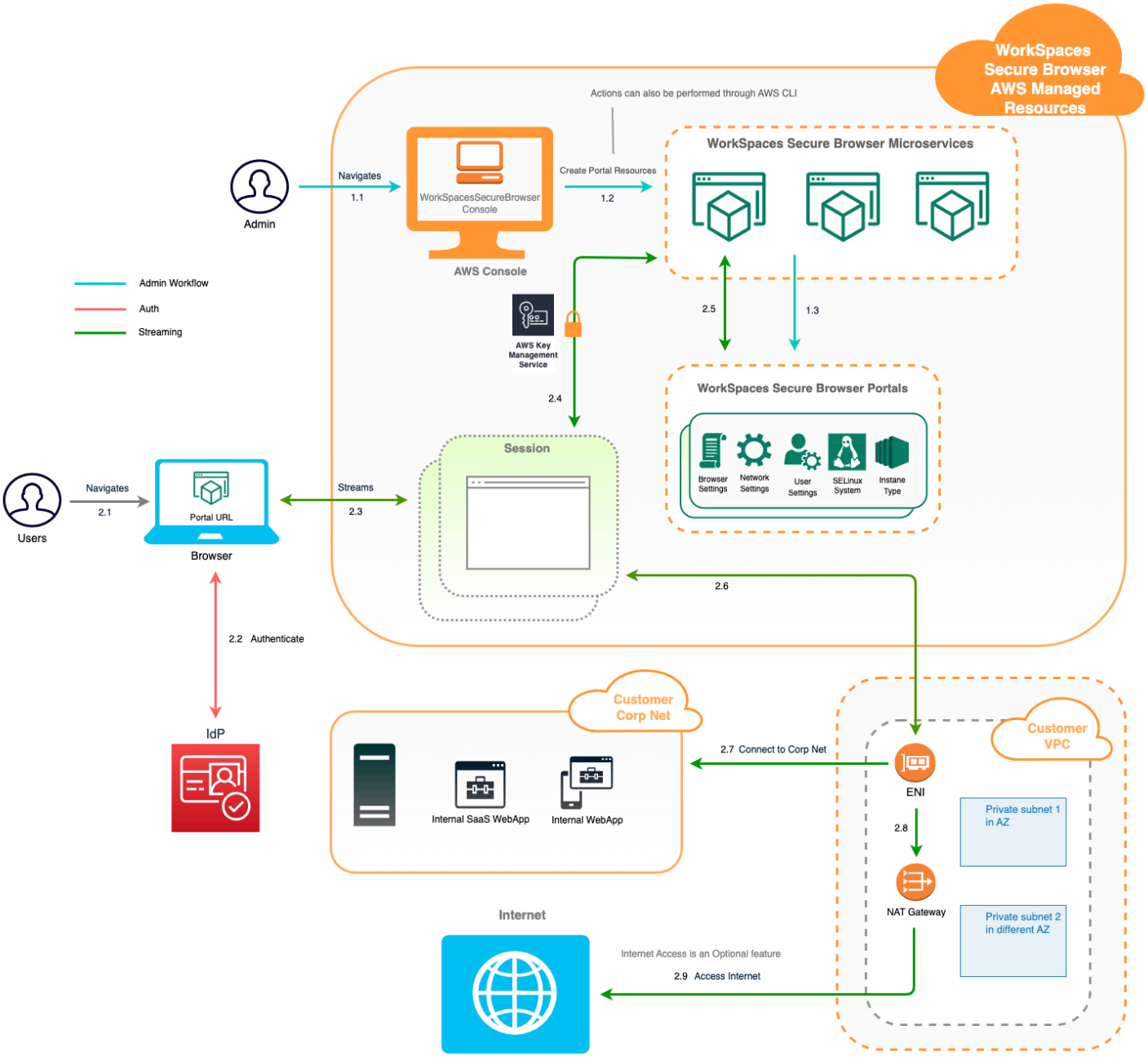
Der Endpunkt ist öffentlich im Internet verfügbar und kann in Ihr Netzwerk eingebettet werden.

Zugehörige Services

WorkSpaces Secure Browser ist eine Funktion von Amazon WorkSpaces im AWS-Endbenutzer-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

Das folgende Diagramm zeigt die Architektur von WorkSpaces Secure Browser.



Zugreifen auf WorkSpaces Secure Browser

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.

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.

Themen

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/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und 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. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer 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 Management Consoleals 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 Sie einen Benutzer 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 Benutzer in IAM Identity Center Administratorzugriff.

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

Melden Sie sich als Benutzer mit Administratorzugriff an

- 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 Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

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

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console 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
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisung en für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benut zeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldein formationen im Referenzh andbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltun g von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benut zerhandbuch.

Netzwerk und Zugriff

In den folgenden Themen wird erklärt, wie Sie WorkSpaces Secure Browser-Streaming-Instanzen 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.

Themen

VPC-Anforderungen

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 die Subnetze müssen die folgenden Anforderungen erfüllen:

- Die VPC muss über Standard-Tenancy verfügen. VPCs mit dedizierter Mandantenfähigkeit 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 erstellen und konfigurieren.
- 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 erstellen und konfigurieren.

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. Aktivieren Sie uneingeschränktes Surfen im Internet (empfohlen)

Eine neue VPC erstellen und konfigurieren

In dieser Sitzung wird beschrieben, wie Sie mit dem VPC-Assistenten eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz erstellen. Im Rahmen dieses Prozesses erstellt der Assistent ein Internet-Gateway und ein NAT-Gateway. Es wird auch eine benutzerdefinierte Routing-Tabelle erstellt, die dem öffentlichen Subnetz zugeordnet ist. Dann wird die Haupt-Routing-Tabelle aktualisiert, die dem privaten Subnetz zugeordnet ist. Das NAT-Gateway wird automatisch im Subnetz Ihrer VPC erstellt.

Nachdem Sie den Assistenten zum Erstellen einer VPC-Konfiguration verwendet haben, fügen Sie ein zweites privates Subnetz hinzu. Weitere Informationen zu dieser Konfiguration finden Sie unter VPC mit öffentlichen und privaten Subnetzen (NAT).

Schritt 1: Eine Elastic IP-Adresse zuweisen

Bevor Sie Ihre VPC erstellen, müssen Sie eine Elastic IP-Adresse in Ihrer WorkSpaces Secure Browser-Region zuweisen. Nach der Zuweisung können Sie die Elastic IP-Adresse mit Ihrem NAT-Gateway verknüpfen. Mit einer Elastic IP-Adresse können Sie einen Ausfall bei Streaming-Instances maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrer VPC neu zu. Weitere Informationen finden Sie unter Elastic IP-Adressen.

> **Note**
>
> Für Elastic IP-Adressen, die Sie verwenden, fallen möglicherweise Gebühren an. Weitere Informationen finden Sie unter Seite mit Preisen für Elastic-IP-Adressen.

Wenn Sie noch keine Elastic IP-Adresse haben, führen Sie die folgenden Schritte aus. Wenn Sie eine vorhandene Elastic IP-Adresse verwenden möchten, müssen Sie zunächst sicherstellen, dass sie derzeit nicht einer anderen Instance oder einer Netzwerkschnittstelle zugeordnet ist.

So weisen Sie eine Elastic IP-Adresse zu

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security die Option Elastic IPs aus.
3. Wählen Sie Allocate new address (Neue Adresse zuordnen) und anschließend Yes, Allocate (Ja, zuordnen) aus.
4. Notieren Sie sich die Elastic IP-Adresse, die auf der Konsole angezeigt wird.
5. Klicken Sie in die im Bereich Elastic IPs in der Ecke oben rechts auf das x-Symbol, um den Bereich zu schließen.

Schritt 2: Eine neuen VPC erstellen

Führen Sie die folgenden Schritte aus, um eine neue VPC mit einem öffentlichen Subnetz und einem privaten Subnetz zu erstellen.

So erstellen Sie eine neue VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich VPC Dashboard (VPC-Dashboard) aus.
3. Wählen Sie VPC Wizard starten.
4. Wählen Sie unter Step 1: Select a VPC Configuration (Schritt 1: Auswählen einer VPC-Konfiguration) die Option VPC with Public and Private Subnets (VPC mit öffentlichen und privaten Subnetzen) und anschließend Select (Auswählen) aus.
5. Konfigurieren Sie unter Step 2: VPC with Public and Private Subnets (Schritt 2: VPC mit öffentlichen und privaten Subnetzen) die VPC wie folgt:
   - Geben Sie für IPv4 CIDR Block (IPv4-CIDR-Block) einen IPv4-CIDR-Block für die VPC ein.
   - Behalten Sie unter IPv6 CIDR Block (IPv6-CIDR-Block) den Standardwert No IPv6 CIDR Block (Kein IPv6-CIDR-Block) bei.
   - Geben Sie unter VPC-Name einen eindeutigen Namen für die VPC ein.
   - Konfigurieren Sie das öffentliche Subnetz wie folgt:
     - Legen Sie unter Public subnet's IPv4 CIDR (IPv4-CIDR für öffentliches Subnetz) den CIDR-Block für das Subnetz ein.
     - Behalten Sie unter Availability Zone den Standardwert No Preference (Keine Einstellung) bei.

  - Geben Sie unter Name für öffentliches Subnetz einen Namen für das Subnetz ein. z. B. **`WorkSpaces Secure Browser Public Subnet`**.
- Konfigurieren Sie das erste private Subnetz wie folgt:
  - Geben Sie unter Private subnet's IPv4 CIDR (IPv4-CIDR des privaten Subnetzes) den CIDR-Block für das Subnetz an. Notieren Sie sich den von Ihnen angegebenen Wert.
  - Wählen Sie unter Availability Zone eine bestimmte Zone aus und notieren Sie sich die ausgewählte Zone.
  - Geben Sie unter Name für privates Subnetz einen Namen für das Subnetz ein. z. B. **`WorkSpaces Secure Browser Private Subnet1`**.
- Behalten Sie bei den übrigen Feldern die Standardwerte bei, sofern sie zutreffen.
- Geben Sie bei Elastic-IP-Zuordnungs-ID den Wert ein, der der Elastic-IP-Adresse entspricht, die Sie erstellt haben. Diese Adresse wird dann dem NAT-Gateway zugewiesen. Wenn Sie keine Elastic IP-Adresse haben, erstellen Sie mithilfe der Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
- Geben Sie für Service-Endpunkte einen Amazon-S3-Endpunkt an, wenn für Ihre Umgebung ein solcher erforderlich ist.

  Gehen Sie folgendermaßen vor, um einen Amazon–S3Endpunkt anzugeben:

  1. Wählen Sie Add endpoint (Endpunkt hinzufügen) aus.
  2. Wählen Sie für Service die Datei com.amazonaws aus. ***`Region-.s3-Eintrag`***, wobei *`Region`* die ist, in der AWS-Region Sie Ihre VPC erstellen.
  3. Wählen Sie für Subnet (Subnetz) die Option Private subnet (Privates Subnetz) aus.
  4. Behalten Sie unter Policy (Richtlinie) den Standardwert Full Access (Voller Zugriff) bei.
- Behalten Sie unter Enable DNS hostnames (DNS-Hostnamen aktivieren) den Standardwert Yes (Ja) bei.
- Behalten Sie bei Hardware tenancy (Hardware-Tenancy) den Standardwert Default (Standard) bei.
- Wählen Sie VPC erstellen aus.
- Es dauert mehrere Minuten, die VPC einzurichten. Wählen Sie nach dem Erstellen der VPC OK aus.

Schritt 3: Ein zweites privates Subnetz hinzufügen

Im vorherigen Schritt haben Sie eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz erstellt. Schließen Sie die folgenden Schritte ab, um Ihrer VPC ein zweites privates Subnetz hinzuzufügen. Es wird empfohlen, ein zweites privates Subnetz in einer anderen Availability Zone als dem ersten privaten Subnetz hinzuzufügen.

So fügen Sie ein zweites privates Subnetz hinzu

1. Wählen Sie im Navigationsbereich Subnetze aus.
2. Wählen Sie das erste private Subnetz aus, das Sie im vorherigen Schritt erstellt haben. Notieren Sie sich auf der Registerkarte Description (Beschreibung) unterhalb der Liste der Subnetze die Availability Zone für dieses Subnetz.
3. Wählen Sie oben links im Subnetzbereich die Option Create Subnet (Subnetz erstellen) aus.
4. Geben Sie unter Name-Tag einen Namen für das private Subnetz ein. z. B. **`WorkSpaces Secure Browser Private Subnet2`**.
5. Wählen Sie für VPC die VPC aus, die Sie im vorherigen Schritt erstellt haben.
6. Wählen Sie unter Availability Zone eine andere Availability Zone als die aus, die Sie für Ihr erstes privates Subnetz verwenden. Die Auswahl einer anderen Availability Zone erhöht die Fehlertoleranz und verhindert Fehler aufgrund unzureichender Kapazität.
7. Geben Sie für IPv4 CIDR block (IPv4-CIDR-Block) einen eindeutigen CIDR-Blockbereich für das neue Subnetz an. Wenn das erste private Subnetz beispielsweise einen IPv4-CIDR-Blockbereich von **`10.0.1.0/24`** hat, können Sie den CIDR-Blockbereich **`10.0.2.0/24`** für das zweite private Subnetz angeben.
8. Wählen Sie Erstellen.
9. Nachdem Ihr Subnetz erstellt wurde, wählen Sie Close (Schließen) aus.

Schritt 4: Die Subnetz-Routing-Tabellen überprüfen und benennen

Nachdem Sie Ihre VPC erstellt und konfiguriert haben, führen Sie die folgenden Schritte aus, um einen Namen für Ihre Routing-Tabellen anzugeben. Sie müssen überprüfen, ob die folgenden Angaben 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 die Option Subnetze und dann das öffentliche Subnetz aus, das Sie erstellt haben. Zum Beispiel WorkSpaces Secure Browser 2.0 Public Subnet.
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	Ziel	Beschreibung
IPv4-CIDR-Block für öffentlic hes Subnetz (z. B. 10.0.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, die für IPv4-Adressen im IPv4-CIDR-Block des öffentlic hen Subnetzes bestimmt sind. Dieser Datenverkehr wird lokal innerhalb der VPC weitergeleitet.
Datenverkehr, der für alle anderen IPv4-Adressen bestimmt 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 (identifi ziert durch igw-ID) weitergel

Bestimmungsort	Ziel	Beschreibung
		eitet, das vom VPC-Assis tenten erstellt wurde.

5. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie dann das erste private Subnetz aus, das Sie erstellt haben (zum Beispiel **`WorkSpaces Secure Browser Private Subnet1`**).
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 **`workspacesweb-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	Ziel	Beschreibung
IPv4-CIDR-Block für öffentlic hes Subnetz (z. B. 10.0.0/20)	Local	Der gesamte Datenverkehr von den Ressourcen, die für IPv4-Adressen im IPv4-CIDR-Block des öffentlichen Subnetzes bestimmt sind, wird lokal innerhalb der VPC weitergeleitet.
Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, (z. B. 0.0.0.0/0)	Ausgehend (nat-ID)	Datenverkehr, der für alle anderen IPv4-Adressen bestimmt ist, wird an das NAT-Gateway weitergeleitet (identifiziert durch nat-ID).
Für S3-Buckets bestimmter Datenverkehr (anwendbar, wenn Sie einen S3-Endpun kt angegeben haben) [pl-ID (com.amazonaws.region.s3)]	Speicher (vpce-ID)	Datenverkehr, der für S3-Buckets bestimmt ist, wird an den S3-Endpunkt weitergel eitet (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 Sie uneingeschränktes Surfen im Internet (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 erstellen und konfigurieren.

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 eines zweiten privaten Subnetzes finden Sie unter the section called “Schritt 3: Ein zweites privates Subnetz hinzufügen”.

> **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.

Aktivieren Sie eingeschränktes Surfen im Internet (mithilfe eines ausgehenden HTTP-Proxys)

Die empfohlene Netzwerkeinrichtung eines WorkSpaces Secure Browser-Portals besteht darin, private Subnetze mit NAT-Gateway zu verwenden, sodass das Portal sowohl öffentliches Internet als auch private Inhalte durchsuchen kann. Weitere Informationen finden Sie unter the section called “Aktivieren Sie uneingeschränktes Surfen im Internet (empfohlen)”. 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-Outbound-Proxy 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

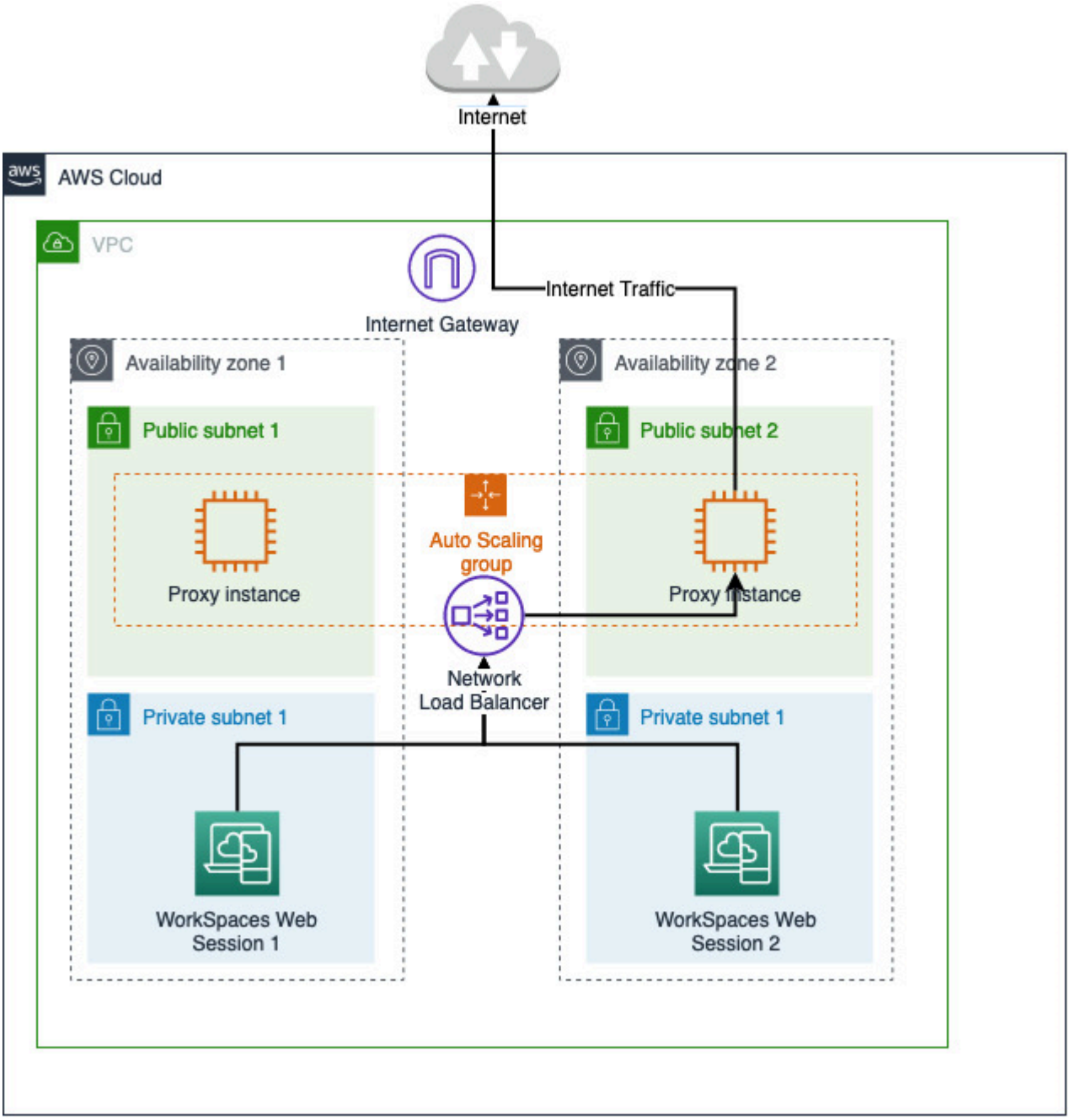
die Verbindung mit dem Proxyendpunkt. Weitere Informationen finden Sie unter So richten Sie einen ausgehenden VPC-Proxy mit Domain-Whitelisting und Inhaltsfilterung ein.

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 abgewickelt wird. Wenn Sie Ihren eigenen Proxy verwenden möchten, ist die Einrichtung des WorkSpaces Secure Browser-Portals ähnlich.

Architektur

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

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.

Richten Sie einen ausgehenden HTTP-Proxy für WorkSpaces Secure Browser ein

Gehen Sie folgendermaßen vor, um einen HTTP-Outbound-Proxy 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 nach den CloudFormation Ausgabeparametern OutboundProxyDomain und OutboundProxy Port. 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

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.

Empfehlungen zur VPC-Einrichtung

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) ausreichen, um Ihren voraussichtlichen Bedarf zu decken. Um eine Kontingenterhöhung zu beantragen, können Sie die Konsole für Service Quotas unter https://console.aws.amazon.com/servicequotas/ verwenden. Informationen zu den Standardkontingenten für WorkSpaces Secure Browser finden Sie unterthe section called “Verwalten Sie Servicekontingenten für Ihr Portal”.
- 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 Elastic Network Interfaces (ENIs) wie die maximal gewünschte Kapazität Ihrer Flotte. Standardmäßig liegt das Limit für ENIs pro Region bei 5 000. Weitere Informationen finden Sie unter Netzwerkschnittstellen.

  Bei der Kapazitätsplanung für sehr große Bereitstellungen, z. B. Tausende gleichzeitiger Streaming-Sitzungen, sollten Sie die Anzahl der ENIs berücksichtigen, die für Ihre Spitzennutzung erforderlich sein könnten. 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 Dimensionierung der VPC und der Subnetze 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 und konfigurieren”.
- 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

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

Mit der Anzeige von AZ-IDs können Sie den Standort von 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 alle AZ-IDs aufgeführt, die Sie für jede Region verwenden können. Informationen über die Zuordnung von AZ-IDs zu Availability Zones in Ihrem Konto finden Sie unter AZ-IDs für Ihre Ressourcen im AWS RAM -Benutzerhandbuch.

Name der Region	Regionscode	Unterstützte AZ-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`
Asia Pacific (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az3`
Asia Pacific (Seoul)	`ap-northeast-2`	`apne2-az1` , `apne2-az2` , `apne2-az3`
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`

Name der Region	Regionscode	Unterstützte AZ-IDs
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`
Europe (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.

VPC-Verbindung

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

Client/Benutzer-Verbindung

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 Domänen aufgelisteten Domains zulassen, um diesen Datenverkehr zuzulassen.

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

Themen

IP-Adresse und Port-Anforderungen

Für den Zugriff auf WorkSpaces Secure Browser-Instanzen 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 Domänen 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 Domänen

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 Dienst zuzugreifen.

Ersetzen Sie in der folgenden Tabelle *{region}* durch den Code der Region des Betriebs-Webportals. 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 appstream2.*{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 cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com

Kategorie	Domain oder IP-Adresse
	*.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 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 WorkSpaces Secure Browser einrichten.

Themen

Schritt 1: Ein Webportal erstellen

Führen Sie zur Erstellung eines Webportals diese Schritte aus.

Themen

Konfigurieren von Netzwerkeinstellungen

1. Öffnen Sie die WorkSpaces Secure Browser-Konsole unter https://console.aws.amazon.com/workspaces-web/home.
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 Netzwerk und Zugriff.
        - 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.

Portaleinstellungen konfigurieren

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 “Verwalten Sie Servicekontingenten für Ihr Portal”.

   > **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. Wählen Sie unter Benutzerzugriffsprotokollierung bei Kinesis-Stream-ID den Amazon-Kinesis-Datenstrom aus, an den Sie Ihre Daten senden möchten. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.
4. Füllen Sie unter Richtlinieneinstellungen folgendes aus:

   - Wählen Sie bei Richtlinienoptionen die Option Visueller Editor oder JSON-Datei-Upload aus. Sie können die Richtlinienkonfigurationsdetails für Ihr Webportal mit beiden Methoden bereitstellen. Weitere Informationen finden Sie unter the section called “Ihre Browser-Richtlinie festlegen oder bearbeiten”.
     - WorkSpaces Secure Browser bietet Unterstützung für Chrome-Unternehmensrichtlinien. Sie können Richtlinien entweder mit einem visuellen Editor oder mit einem manuellen Upload für Richtliniendateien hinzufügen und verwalten. Sie können jederzeit zwischen beiden Optionen wechseln.
     - 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.
   - (Optional) Geben Sie unter Startup-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, die im privaten Modus besucht werden oder bevor ein Benutzer seinen Browserverlauf löscht, können nicht in der Benutzerzugriffsprotokollierung aufgezeichnet werden. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

- Unter URL-Filterung können Sie konfigurieren, welche URLs Benutzer während einer Sitzung aufrufen können. Weitere Informationen finden Sie unter the section called “Richten Sie die URL-Filterung ein”.
- (Optional) Geben Sie bei Browserlesezeichen – 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.

- (Optional) 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.

5. Wählen Sie unter IP-Zugriffskontrolle (optional) aus, ob der Zugriff auf vertrauenswürdige Netzwerke beschränkt werden soll. Weitere Informationen finden Sie unter the section called “IP-Zugriffskontrollen einrichten (optional)”.
6. Wählen Sie Next (Weiter), um fortzufahren.

Benutzereinstellungen 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. Wählen Sie bei Benutzerberechtigungen aus, ob die Erweiterung für Single Sign-On aktiviert werden soll. Weitere Informationen finden Sie unter the section called “Erweiterung für Single-Sign-On aktivieren (optional)”.
2. Wählen Sie bei Zwischenablageberechtigungen die Option Deaktiviert oder Aktiviert aus.
3. Wählen Sie unter Dateiübertragung die Option Deaktiviert oder Aktiviert aus.
4. Wählen Sie unter Benutzern erlauben, von ihrem Webportal aus auf einem lokalen Gerät zu drucken, die Option Erlaubt oder Nicht erlaubt aus.
5. Wählen Sie für Benutzern erlauben, Deeplink 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 zulassen (optional)”
6. Geben Sie bei Benutzersitzungsdetails 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 Mauseingabe mehr machen. 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.

Identitätsanbieter konfigurieren

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

Themen

Wählen Sie den Identitätsanbietertyp

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 “Konfigurieren Sie den 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 “Konfigurieren Sie den IAM Identity Center-Authentifizierungstyp”.

Konfigurieren Sie den Standardauthentifizierungstyp

Für Standard (Standard) verbinden Sie Ihren SAML 2.0-Identitätsanbieter eines Drittanbieters (wie Okta oder Ping) direkt mit Ihrem Portal.

Der Identitätstyp Standard unterstützt service-provider-initiated (SP-initiierte) und identity-provider-initiated (IdP-initiierte) Anmeldeabläufe mit Ihrem SAML 2.0-kompatiblen IdP.

Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters im Secure Browser WorkSpaces

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=Ex Identity-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.

Schritt 2: Konfigurieren Sie Ihren Identitätsanbieter auf Ihrem eigenen IdP

Öffnen Sie eine neue Registerkarte in Ihrem Browser. Schließen Sie dann die folgenden Schritte mit Ihrem Identitätsanbieter ab:

1. 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. Bei einigen Anbietern ist das Hochladen von Dateien nicht zulässig.

   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.
2. 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.

3. 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 “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters im Secure Browser WorkSpaces ” um den Standard-Relay-Status für Ihre IdP-Anwendung festzulegen.

4. 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 “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters im Secure Browser WorkSpaces ” 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.

5. 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.

6. Optional: Konfigurieren Sie Single Logout. Wenn Sie Single Logout ausgewählt haben, folgen Sie den Schritten in Schritt 5 von, the section called “Schritt 1: Beginnen Sie mit der Konfiguration Ihres Identitätsanbieters im Secure Browser WorkSpaces ” um das Signaturzertifikat auf Ihren IdP hochzuladen, geben Sie Single Logout URL ein und aktivieren Sie Single Logout.

7. Gewähren Sie Ihren Benutzern in Ihrem IdP Zugriff auf die Verwendung von WorkSpaces Secure Browser.

8. Laden Sie eine Metadaten-Austauschdatei von Ihrem Identitätsanbieter herunter. Im nächsten Schritt laden Sie diese Metadaten in den WorkSpaces Secure Browser hoch.

Schritt 3: Schließen Sie die Konfiguration Ihres Identitätsanbieters im WorkSpaces Secure Browser ab

Kehren Sie zur WorkSpaces Secure Browserconsole 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.

1. 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.
2. 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.
3. Klicken Sie anschließend auf Next.
4. 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 können die **<**Your SP Entity ID**><**Your SP ACS URL**>**Service Provider-Details oder das Metadaten-Dokument Ihres Portals entweder über die Konsole oder die CLI aufrufen.
>
> - 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 für bestimmte IdPs

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 Enterprise PingOne	Unterstützt PingOne for Enterprise Verschlüsselung?	SAML 2.0-Einzelabmeldung
Ein Login	Benutzerdefinierte	OneLogin Benutzer	Benutzerdefinierte	Benutzerdefinierte	Benutzerdefinierte	Benutzerdefinierte

IdP	Einrichtung der SAML-Anwendung	Benutzerverwaltung	IDP-initiierte Authentifizierung	Signierung anfordern	Assertion-Verschlüsselung	Einmaliges Abmelden
	r SAML-Konnektor (erweitert) (4266907)	manuell hinzufügen	r SAML-Konnektor (erweitert) (4266907)	r SAML-Konnektor (erweitert) (4266907)	r SAML-Konnektor (erweitert) (4266907)	r 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	N/A	–	N/A

Konfigurieren Sie den IAM Identity Center-Authentifizierungstyp

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 “Konfigurieren Sie den 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.

So erstellen Sie ein Webportal mit IAM Identity Center

1. Wählen Sie bei der Portalerstellung unter Schritt 4: Identitätsanbieter 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 „Benutzer und/oder Gruppen“.
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.

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.

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 Sicherer 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.

Um Benutzer und Gruppen für Ihr Webportal anzuzeigen oder zu entfernen

- Sie können den Benutzerzugriff auf diese Anwendung anzeigen oder entfernen, indem Sie die Aktionen verwenden, die in der Tabelle Zugewiesene Benutzer verfügbar sind. 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 Sie den Identitätsanbietertyp

Gehen Sie wie folgt vor, um den Authentifizierungstyp Ihres Portals jederzeit zu ändern:

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

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.

Überprüfen und 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.

Schritt 2: Ihr Webportal testen

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 “Identitätsanbieter konfigurieren” abgeschlossen haben, können Sie diesen Abschnitt überspringen und bei Schritt 3: Ihr Webportal verteilen fortfahren.

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, Webportale, wählen Sie Ihr Webportal und wählen Sie 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 URLs in die Adressleiste eingeben.

Schritt 3: Ihr Webportal verteilen

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 “Konfigurieren Sie den 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.

Nächste Schritte

Nachdem Sie Ihr erstes Webportal erstellt haben, können Sie jederzeit Details anzeigen, Details bearbeiten oder das Webportal löschen. Weitere Informationen finden Sie unter Verwalten Ihres Webportals.

Sie AWS-Konto können in jedem Bereich, in AWS-Region dem WorkSpaces Secure Browser verfügbar ist, ein Webportal erstellen. Jedes Webportal kann bis zu 25 Benutzerverbindungen gleichzeitig unterstützen. Informationen zur Erhöhung der Anzahl der Portale, die Sie in einer Region erstellen können, oder zur Unterstützung mehrerer gleichzeitiger Sitzungen für ein Portal finden Sie unter the section called “Verwalten Sie Servicekontingenten für Ihr Portal”.

Verwalten Ihres Webportals

Nachdem Sie Ihr Webportal eingerichtet haben, können Sie dessen Details anzeigen oder bearbeiten sowie das Portal löschen, falls es nicht mehr benötigt wird.

Themen

Webportal-Details anzeigen

So zeigen Sie Webportal-Details an

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.

Ein Webportal bearbeiten

So bearbeiten Sie ein Webportal

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

Ein Webportal löschen

So löschen Sie ein Webportal

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.

Verwalten Sie Servicekontingenten für Ihr Portal

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

> **Important**
>
> Dienstkontingente gelten jeweils AWS-Region 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.

So fordern Sie eine Erhöhung Ihrer Service Quota an

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

   > **Important**
   >
   > WorkSpaces Die Kontingente für den Secure Browser Service 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.

Beantragen Sie eine Erhöhung des Portals

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.

Fordern Sie eine Erhöhung der maximalen Anzahl gleichzeitiger Sitzungen an

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 und/oder der Dringlichkeit hinzu. Diese Informationen helfen dem Serviceteam, Anfragen zu priorisieren und sicherzustellen, dass Ihrem Konto ausreichend Kapazität zugewiesen wird.

Beispiel einschränken

Nehmen wir beispielsweise 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).

Servicekontingenten verwalten

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

Andere Servicekontingente

Sie können Erhöhungen für andere Kontingente, die auf der Seite Service Quotas aufgeführt sind, einsehen und beantragen. In der Praxis werden die meisten Kunden es 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.

Das Intervall für die erneute Authentifizierung eines SAML-IdP-Tokens steuern

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 “Schritt 1: Ein Webportal erstellen”.

   > **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.

Benutzerzugriffsprotokollierung einrichten

Sie können die Benutzerzugriffsprotokollierung einrichten, um folgende Benutzerereignisse aufzuzeichnen:

- Sitzungsstart — Markiert den Beginn einer WorkSpaces Secure Browser-Sitzung.
- Sitzungsende — Kennzeichnet das Ende einer WorkSpaces Secure Browser-Sitzung.
- URL-Navigation: Protokolliert die URL, die ein Benutzer lädt.

> **Note**
>
> URL-Navigationsprotokolle werden aus dem Browserverlauf aufgezeichnet. URLs, die nicht im Browserverlauf aufgezeichnet wurden (entweder im Inkognitomodus besucht oder aus dem Browserverlauf gelöscht), werden nicht in Protokollen aufgezeichnet. Es liegt an den Kunden, anhand ihrer Browser-Richtlinie zu entscheiden, ob sie den Inkognitomodus oder das Löschen des Verlaufs deaktivieren möchten.

Darüber hinaus sind für jedes Ereignis die folgenden Informationen enthalten:

- Ereigniszeit
- Username
- Webportal-ARN

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

Die Aktivierung von Benutzerzugriffsprotokollen in Ihrem WorkSpaces Secure Browser-Portal kann zu Gebühren von Amazon Kinesis Data Streams führen. Weitere Details zu den Preisen finden Sie unter Amazon Kinesis Data Streams – Preise.

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?

> **Note**
>
> 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?.

Beispielprotokolle

Im Folgenden finden Sie ein Beispiel für jedes verfügbare Ereignis, einschließlich Validierung, StartSession, VisitPageund. EndSession

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"
}
```

Ihre Browser-Richtlinie festlegen oder bearbeiten

Mit WorkSpaces Secure Browser können Sie mithilfe der Chrome-Richtlinien, die für die neueste stabile Version verfügbar sind, eine benutzerdefinierte Browserrichtlinie festlegen. Es gibt mehr als 300 Richtlinien, die Sie auf ein Webportal anwenden können. Weitere Informationen finden Sie unter the section called “Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel)” und in der Liste der Chrome Unternehmensrichtlinien.

Wenn Sie die Konsolenansicht verwenden, um ein Webportal zu erstellen, können Sie die folgenden Richtlinien anwenden:

- `StartURL`
- Lesezeichen und Lesezeichenordner
- Aktivieren und Deaktivieren von privatem Browsing
- Löschung des Verlaufs
- URL-Filterung mit `AllowURL` und `BlockURL`

Weitere Informationen über die Verwendung von Richtlinien für die Konsolenansicht finden Sie unter Erste Schritte mit WorkSpaces Secure Browser.

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 “Bearbeiten Sie die grundlegende Browser-Richtlinie”.

Themen

Eine benutzerdefinierte Browser-Richtlinie festlegen (Beispiel)

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 Beispiel 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.

Themen

Schritt 1: Ein Webportal erstellen

Um Ihre JSON-Datei für die Chrome-Richtlinie hochzuladen, müssen Sie ein WorkSpaces Secure Browser-Portal erstellen. Weitere Informationen finden Sie unter the section called “Schritt 1: Ein Webportal erstellen”.

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 Lesezeichen-URLs ein.

   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 die Startup-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. Dadurch wird die `RestoreOnStartup`-Aktion zum Öffnen einer URL-Liste festgelegt. Sie können auch andere Aktionen für Ihre Startup-URLs verwenden. Weitere Informationen finden Sie in der Liste der Chrome-Unternehmensrichtlinien.

   b. Legen Sie `RestoreOnStartupURLs` auf https://www.aboutamazon.com/news fest.

```
     "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 Sie die grundlegende Browser-Richtlinie

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.

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.
- Die Richtlinien `URLAllowlist` und `URLBlocklist` können mithilfe des URL-Filter-Features der Konsolenansicht oder mithilfe des JSON-Uploads erweitert werden. Die Baseline-URLs

können jedoch nicht überschrieben werden. Diese Richtlinien sind in einer JSON-Datei, die von Ihrem Webportal heruntergeladen wurde, nicht sichtbar. Wenn Sie jedoch während einer Sitzung „chrome://policy“ aufrufen, zeigt der Remote-Browser die angewendeten Richtlinien an.

Den Eingabemethoden-Editor (IME) konfigurieren

Ein Eingabemethoden-Editor (IME) ist ein Hilfsprogramm, das Endbenutzern Optionen zur Texteingabe in Sprachen bietet, bei denen ein anderes Tastaturlayout als eine QWERTY-Tastatur verwendet wird. IMEs helfen Benutzern bei der Eingabe von Text in Sprachen mit größeren und 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 IMEs

  - Wenn Sie Shift+Control+Left Alt drücken, können Sie den IME vorwärts durchgehen (bzw. zum richtigen Tastaturlayout wechseln).
- Japanisch
  - Zur Auswahl von Hiragana drücken Sie F6.
  - Zur Auswahl von Katakana drücken Sie F7.
  - Zur Auswahl von Latin drücken Sie F10.
  - Zur Auswahl von Wide Latin drücken Sie F9.
  - Zur Auswahl von Direct Input drücken Sie ALT +, ALT+@, Zenkaku Hankaku.
- Koreanisch
  - Zur Auswahl von Hangul drücken Sie Shift+Space.
  - Zur Auswahl von Hanja drücken Sie F9.

Wenn Sie die IME-Symbolleiste und das IME-Menü entfernen oder die Bildschirmtastatur aus Ihren WorkSpaces Secure Browser-Sitzungen ausschalten möchten, wenden Sie sich an AWS Support.

Die sitzungsinterne Lokalisierung konfigurieren

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 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)

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

Führen Sie einen der folgenden Schritte aus, 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.

IP-Zugriffskontrollen einrichten (optional)

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.

Eine IP-Zugriffskontrollgruppe erstellen

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.

Eine IP-Zugriffseinstellung einem Webportal zuordnen

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 konfigurieren” 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.

Eine IP-Zugriffskontrollgruppe bearbeiten

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.

Einer IP-Zugriffskontrollgruppe löschen

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.

Erweiterung für Single-Sign-On aktivieren (optional)

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.

Benutzer werden aufgefordert, die Erweiterung zu installieren, wenn sie sich bei einem Portal anmelden.

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.

Sie können die vorhandene Benutzereinstellungskonfiguration eines Portals aktualisieren oder dies bei der ersten Erstellung eines Webportals tun. 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

Besuchen Sie als Nächstes Ihr Webportal in der Konsole. Lassen Sie dann die Erweiterung zu und fügen Sie hinzu, welche Domain-Cookies synchronisiert werden sollen. Gehen Sie wie folgt vor, um ein neues Portal mit der zugelassenen Erweiterung zu erstellen oder ein vorhandenes Portal zu aktualisieren.

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

1. Folgen Sie den Anweisungen unter the section called “Schritt 1: Ein Webportal erstellen”, bis Sie zu the section called “Benutzereinstellungen konfigurieren” gelangen.
2. Wählen Sie für Schritt 1 von the section called “Benutzereinstellungen konfigurieren” 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 konfigurieren” aus und schließen Sie die verbleibenden Abschnitte unter the section called “Schritt 1: Ein Webportal erstellen” ab, um Ihr Webportal zu erstellen.

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

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

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

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

Einzelheiten zum Benutzererlebnis mit der Erweiterung finden Sie unter the section called “Erweiterung für Single Sign-On”.

Richten Sie die URL-Filterung ein

Sie können die Chrome-Richtlinie verwenden, um zu filtern, auf welche URLs Benutzer von ihrem Remote-Browser aus zugreifen können. Die Chrome-Richtlinie bietet zwei Mechanismen zum Filtern von URLs: UrlAllowList und UrlBlockList. Sie können die Schnittstelle der WorkSpaces Secure Browser-Konsole verwenden, um die URL-Filterung als Portaleinstellung zu konfigurieren, oder Sie können sie als Teil Ihrer benutzerdefinierten JSON-Anweisung hinzufügen (entweder im Inline-Editor oder als JSON-Datei-Upload).

So richten Sie die URL-Filterung mithilfe der Konsole ein

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.
3. Wählen Sie für die URL-Filterung aus den folgenden Optionen:

   - Zugriff auf alle URLs zulassen: Standardmäßig ermöglicht ein Webportal den Zugriff auf alle URLs. Sie können der BlockURL-Liste bestimmte Websites hinzufügen, um zu verhindern, dass Benutzer diese Websites während einer Sitzung besuchen. Wenn Sie beispielsweise www.anycorp.com zur BlockURL-Liste hinzufügen, wird verhindert, dass Benutzer während ihrer Sitzung zu www.anycorp.com navigieren.
   - Zugriff auf alle URLs blockieren: Standardmäßig blockiert das Webportal den Zugriff auf alle URLs. Sie können der URL-Zulassungsliste bestimmte Websites hinzufügen, um eine Liste der Websites zu erstellen, die Benutzer besuchen können, und den Traffic zu anderen Websites blockieren. Erwägen Sie, jede URL als Lesezeichen hinzuzufügen, um Benutzern während ihrer Sitzung den Zugriff mit einem Klick zu ermöglichen.
   - Erweiterte Konfiguration: Wählen Sie diese Option, um AllowURL - und BlockURL-Listen parallel zu erstellen. Die URL-Zulassungsliste hat Vorrang vor der URL-Blockliste. Diese Option ermöglicht die URL-Filterung nach Pfad. Sie können beispielsweise www.anycorp.com zur Blockliste hinzufügen und dann www.anycorp.com/hr zur Zulassungsliste hinzufügen. Auf diese Weise können Benutzer www.anycorp.com/hr besuchen, aber sie können nicht auf andere URL-Pfade zugreifen, z. B. www.anycorp.com/finance.

Weitere Hinweise zur Verwendung von URLs zum Sperren und Zulassen finden Sie unter Zulassen oder Blockieren des Zugriffs auf Websites. Fügen Sie diesen Listen URLs gemäß dem Blocklisten-Filterformat von Chrome hinzu, um die besten Ergebnisse zu erzielen. Weitere Informationen finden Sie unter URL-Sperrlisten-Filterformat.

So richten Sie die URL-Filterung mit dem JSON-Editor oder dem Datei-Upload ein

1. Wählen Sie im Modul „Richtlinieneinstellungen“ den JSON-Editor aus und umgehen Sie das Konsolen-Benutzeroberflächenmodul für die Ansicht „Editor“ oder „Datei-Upload“.
   - Der Editor ermöglicht es Kunden, benutzerdefinierte Richtlinienerklärungen direkt in der Konsole zu erstellen. Der Editor hebt Fehler in der JSON-Anweisung während der Richtlinienerstellung hervor.
   - Beim Datei-Upload können Kunden eine JSON-Datei hinzufügen, die außerhalb der Konsole erstellt wurde (z. B. aus einem vorhandenen Chrome-Browser exportiert).
2. Informationen zur korrekten Formatierung einer Allow/DenyURL-Liste für Ihr Webportal finden Sie in den Chrome-Richtliniendetails für UrlAllowList und UrlBlockList. Weitere Informationen finden Sie unter URLAllowList und URLBlockList.

Deep-Links zulassen (optional)

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. Um die Erlaubnis für Deep-Links zu gewähren, wählen Sie bei der Erstellung von Benutzereinstellungen die Option Zulässig aus. Weitere Informationen finden Sie unter the section called “Benutzereinstellungen konfigurieren”.

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.

Deep-Links müssen die folgenden Anforderungen erfüllen:

- Für das Portal müssen die Deep-Link-Berechtigungen auf Zugelassen gesetzt sein. Weitere Informationen finden Sie unter the section called “Benutzereinstellungen konfigurieren”.
- Die Site, zu der Sie einen Deeplink erstellen möchten, muss URL-kodiert sein. Um beispielsweise einen Benutzer mit „https://www.example.com/?query=true“ zu verknüpfen, aktualisieren Sie den Link auf https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue.
- Hängen Sie die URL im folgenden Format an eine Portal-URL auf der Zulassungsliste an, wobei UUID die Portal-ID ist:

  <uuid>https://.workspaces-web.com/? deeplinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue
- Ein Deeplink kann bis zu 10 durch Komma getrennte URLs enthalten. Beispielsweise:

  <uuid>https://.workspaces-web.com/? deeplinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue, https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue2, https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue3, https%3A%2F%2Fwww.example.com .com%2F%3FQuery%3DTrue4

Jeder Benutzer, mit dem Sie diesen Portal-Link teilen, kann den Deep-Link-Wert manipulieren, um eine Website zu besuchen, wenn diese Domain vom Portal aus erreichbar ist und nicht auf der URL-Blocklist 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. Weitere Informationen finden Sie unter the section called “Richten Sie die URL-Filterung ein” Zugriff auf Websites zulassen oder blockieren.

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

- 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 im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- 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 FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

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 AWS-Services über die Konsole arbeiten,API, AWS CLI oder. 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 einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Datenverschlüsselung

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 eine Rolle mit 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 Daten im Ruhezustand 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

Verschlüsselung im Ruhezustand ist standardmäßig konfiguriert. Kundenspezifische Daten, die im WorkSpaces Secure Browser verwendet werden, werden mit AWS KMS verschlüsselt. WorkSpaces Secure Browser bietet Verschlüsselung im Ruhezustand für Ressourcen, die Sie erstellen. Der Dienst akzeptiert bei der Erstellung einer Ressource einen vom AWS KMS Kunden verwalteten Schlüssel. Wenn kein Schlüssel bereitgestellt wird, wird ein AWS eigener Schlüssel verwendet, um die ruhenden Ressourcen zu verschlüsseln. Der Service verschlüsselt das Dokument mit den Browser-Richtlinien, das Sie zur Anpassung Ihrer Browsersitzungen bereitstellen können, sowie die Konfiguration Ihres Identitätsanbieters und die Anzeigenamen für Ihre Portale. Diese Informationen bleiben entweder mit dem vom Kunden verwalteten Schlüssel oder dem AWS eigenen Schlüssel verschlüsselt, solange sie in unserem Backend gespeichert werden.

Sie können entscheiden, welcher Schlüssel verwendet werden soll, wenn Sie eine WorkSpaces Secure Browser-Ressource erstellen. Wenn Daten, die Teil dieser Ressource sind, verschlüsselt sind, akzeptiert WorkSpaces Secure Browser das `customerManagedKeyArn` Feld als Teil der `create`API. Der angegebene Schlüssel muss ein symmetrischer AWS KMS -Schlüssel sein, und der Administrator, der die Ressource mit diesem Schlüssel erstellt, muss über die Berechtigungen `kms:Decrypt`, `kms:GenerateDataKey` und `kms:CreateGrant` verfügen. Nachdem eine Ressource mit dem Schlüssel erstellt wurde, kann der Schlüssel nicht mehr entfernt oder geändert werden. Wenn Sie einen vom Kunden verwalteten Schlüssel verwendet haben, muss der Administrator, der auf die Ressource zugreift, über die erforderlichen `kms:Decrypt`- und `kms:GenerateDataKey`-Berechtigungen verfügen. Wenn Sie bei der Verwendung der Konsole die Fehlermeldung erhalten, dass der Zugriff verweigert wurde, stellen Sie sicher, dass der Benutzer, der die Konsole verwendet, über diese Berechtigungen für den verwendeten Schlüssel verfügt.

Sie können Fehler beheben und die Verwendung von Schlüsseln überprüfen, indem Sie den Status der AWS KMS Zuschüsse überprüfen. Weitere Informationen finden Sie unter Verwalten von Erteilungen. Während der Portalerstellung erstellt WorkSpaces Secure Browser einen Grant, damit der Service asynchron auf den Schlüssel zugreifen kann. Sie können den Status unserer Schlüsselnutzung überprüfen, indem Sie die Gewährung sowie den Verschlüsselungskontext überprüfen, der bei der Verwendung der Gewährung angegeben wurde. Der Verschlüsselungskontext enthält immer einen Eintrag mit dem Schlüssel `aws:workspaces-web:portal:id` und einem Wert, der Ihrer Portal-ID entspricht. Bei anderen Ressourcen enthält der Verschlüsselungskontext immer einen Eintrag im Format `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` und die entsprechende Ressourcen-ID.

Verschlüsselung während der Übertragung

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

Die Verschlüsselung bei der Übertragung ist standardmäßig konfiguriert, und sichere Verbindungen (HTTPS,TLS) sind standardmäßig konfiguriert.

Schlüsselverwaltung

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 mit dem festlegen AWS SDK.

Datenschutz für den Datenverkehr zwischen Netzwerken

Um Verbindungen zwischen WorkSpaces Secure Browser und lokalen Anwendungen zu sichern, verwenden Sie WorkSpaces Secure Browser, um Browsersitzungen in Ihren eigenen VPC zu starten. Die Verbindung zu lokalen Anwendungen wird von Ihnen selbst VPC konfiguriert und 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 dienstverknüpften Rollen für WorkSpaces Secure Browser.

Benutzerzugriffsprotokollierung

Administratoren sind in der Lage, WorkSpaces Secure Browser-Sitzungsereignisse wie Start, Stopp und URL Besuche aufzuzeichnen. 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. URLBesuche im Inkognitomodus oder URLs aus dem Browserverlauf gelöschte Besuche 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 AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um WorkSpaces Secure Browser-Ressourcen zu verwenden. IAMist eine AWS-Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt davon ab, welche Arbeit Sie im WorkSpaces Secure Browser ausführen.

Dienstbenutzer — Wenn Sie den WorkSpaces Secure Browser-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr WorkSpaces Secure Browser-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie im WorkSpaces abgesicherten Browser nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf Amazon WorkSpaces Secure Browser.

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für die WorkSpaces Secure Browser-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf WorkSpaces Secure Browser. Es ist Ihre Aufgabe, zu bestimmen, auf welche WorkSpaces Secure Browser-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen WorkSpaces Secure Browser nutzen IAM kann, finden Sie unterSo funktioniert Amazon WorkSpaces Secure Browser mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf WorkSpaces Secure Browser schreiben können. Beispiele für identitätsbasierte WorkSpaces Secure Browser-Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. 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 (angemeldet bei AWS) oder indem Sie eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden,

konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
  - Dienstbezogene Rolle — 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. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und

gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die

`iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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

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

Zugriffskontrolllisten () ACLs

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

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon WorkSpaces Secure Browser mit IAM

Bevor Sie IAM den Zugriff auf WorkSpaces Secure Browser verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen mit WorkSpaces Secure Browser zur Verfügung stehen.

IAMFunktionen, die Sie mit Amazon WorkSpaces Secure Browser verwenden können

IAMFunktion	WorkSpaces Unterstützung für sicheren Browser
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	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 IAM im IAMBenutzerhandbuch unter AWS Dienste, die mit funktionieren.

Identitätsbasierte Richtlinien für Secure Browser WorkSpaces

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

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 anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff.

Richtlinienaktionen für WorkSpaces Secure Browser

Unterstützt Richtlinienaktionen: Ja

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

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, 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 zu den Aktionen, mit denen Sie die ARN einzelnen Ressourcen 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 Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

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

UnterstütztACLs: Nein

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

Attributbasierte Zugriffskontrolle () mit Secure Browser ABAC WorkSpaces

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

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 finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit Secure Browser verwenden WorkSpaces

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn

Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Serviceübergreifende Prinzipalberechtigungen für WorkSpaces Secure Browser

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für WorkSpaces Secure Browser

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.

> **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 dienstverknüpfte Rollen: Ja

Eine serviceverknüpfte 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 dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, die mit funktionieren. IAM 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. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

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 Richtlinien
- Verwenden der WorkSpaces Secure Browser-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

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. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen 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 AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der 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 Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie 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 im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die internen und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
    "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.

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 serviceverknüpften 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 Availability Zones zu beschreiben, Netzwerkschnittstellen zu erstellen, zu kennzeichnen, zu beschreiben und zu löschen, eine Adresse zuzuordnen oder zu trennen und Routing-Tabellen, 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 “Benutzerzugriffsprotokollierung 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 es Prinzipalen, VPCs, Subnetze und Sicherheitsgruppen zu beschreiben. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet, um Ihnen Ihre VPCs, Subnetze und Sicherheitsgruppen anzuzeigen, die für die Verwendung mit dem Service 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 es Prinzipalen, VPCs, Subnetze und Sicherheitsgruppen zu beschreiben. Dies wird in der AWS Management Console im WorkSpaces Secure Browser verwendet, um Ihnen Ihre VPCs, Subnetze und Sicherheitsgruppen anzuzeigen, die für die Verwendung mit dem Service 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.

Änderung	Beschreibung	Datum
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— Aktualisierte Richtlinie	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, sodass CreateNetworkInterface nur noch Tags mit aws:RequestTag/WorkSpacesWebManaged: true und Aktionen auf Subnetz- und Sicherheitsgruppenressourcen sowie auf ENIs DeleteNetworkInterface beschränkt werden, die mit aws:ResourceTag/WorkSpacesWebManaged: true gekennzeichnet sind.	15. Dezember 2022
AmazonWorkSpacesWebReadOnly— Die Richtlinie wurde aktualisiert	WorkSpaces Secure Browser hat die Richtlinie um Leseberechtigungen	02. November 2022

Änderung	Beschreibung	Datum
	für die Protokollierung von Benutzerzugriffen und die Auflistung von Kinesis-Datenströmen erweitert. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.	
AmazonWorkSpacesWebServiceRolePolicy— Die Richtlinie wurde aktualisiert	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 “Benutzerzugriffsprotokollierung einrichten”.	17. Oktober 2022
AmazonWorkSpacesWebServiceRolePolicy— Die Richtlinie wurde aktualisiert	WorkSpaces Secure Browser hat die Richtlinie zur Erstellung von Tags während der ENI-Erstellung aktualisiert.	6. September 2022
AmazonWorkSpacesWebServiceRolePolicy— Die Richtlinie wurde aktualisiert	WorkSpaces Secure Browser hat die Richtlinie aktualisiert, um den AWS/Usage-Namespace zu den PutMetricData API-Berechtigungen hinzuzufügen.	6. April 2022

Änderung	Beschreibung	Datum
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 auftreten könnenIAM.

Themen

- Ich bin nicht autorisiert, 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 autorisiert, 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 `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `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, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden 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 anderen IAMBenutzer AWS-Konto , der Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Verwenden von dienstverknüpften Rollen für 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.

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 Management Console, 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 AWSServiceRoleForAmazonWorkSpacesWeb

- 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 AWSServiceRoleForAmazonWorkSpacesWeb 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. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

> **Note**
>
> Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

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:

- Sichern von Inhalten zwischen Availability Zones oder Regionen
- Verschlüsselte Sicherungen
- Verschlüsseln von Inhalten, die während der Übertragung zwischen Availability Zones oder Regionen übertragen 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:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

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 dem Subnetz oder der VPC Sicherheitsgruppe gesteuert werden. Multi-Tenancy und VPC Endpoints (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.

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 finden 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 finden 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 “Benutzerzugriffsprotokollierung 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 Amazon EC2 EC2-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 Amazon EC2 EC2-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs können 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
`GlobalCpuPercent`	Die CPU-Auslastung der Amazon WorkSpaces Secure Browser-Sitzungsinstanz.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Prozent
`GlobalMemoryPercent`	Die Speichernutzung (RAM) der Amazon WorkSpaces Secure Browser-Sitzungsinstanz.	`PortalId`	Durchschnitt, Summe, Maximum, Minimum	Prozent

> **Note**
>
> Sie können die Metrikstatistik „SampleCount“ für `GlobalCpuPercent` oder `GlobalMemoryPercent` um die Anzahl der gleichzeitig aktiven Sitzungen auf Ihrem Portal zu ermitteln, einsehen. Die Datenpunkte werden von jeder Sitzung einmal pro Minute ausgegeben.

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.

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 dem CloudTrail UserIdentity-Element.

Grundlegendes zu WorkSpaces Einträgen in 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"
    }]
}
```

Benutzerzugriffsprotokollierung

Mit Amazon WorkSpaces Secure Browser können Kunden Sitzungsereignisse wie Start- und Stopp- und URL-Besuche aufzeichnen. Diese Protokolle werden an einen Amazon-Kinesis-Datenstrom übermittelt, den Sie für Ihr Webportal angeben. Weitere Informationen finden Sie unter the section called “Benutzerzugriffsprotokollierung einrichten”.

Anleitung für WorkSpaces Secure Browser-Benutzer

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.

Themen

Browser- und Gerätekompatibilität

Amazon WorkSpaces Secure Browser wird vom NICE DCV 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

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).

Anleitung zur Sitzung

Nachdem Sie sich beim Webportal angemeldet haben, können Sie eine Sitzung starten und während Ihrer Sitzung verschiedene Aktionen ausführen.

Themen

Starten einer Sitzung

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.

Die Symbolleiste 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 den Aufwärtspfeil 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.
	**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 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.

Beenden einer Sitzung

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.

Fehlerbehebung

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.

Erweiterung für Single Sign-On

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.

Kompatibilität

Die Erweiterung funktioniert bei folgenden Geräten:

- Laptops
- Desktop-Computer

Die Erweiterung funktioniert mit folgenden Browsern:

- Chrome
- Firefox

Installation

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

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
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	Sie können die Chrome-Richtlinie verwenden, um zu filtern, auf welche URLs Benutzer von ihrem Remote-	21. Februar 2024

	Browser aus zugreifen können.	
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 API-Berechtigungen hinzuzufügen PutMetricData	6. April 2022
Serviceverknüpfte Rolle	Neue serviceverknüpfte Rolle AWSServiceRoleForAmazonWorkSpacesWeb	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.