Guida di amministrazione

Amazon WorkSpaces Web

Amazon WorkSpaces Web: Guida di amministrazione

Table of Contents

Cos'è Amazon WorkSpaces Web?

Amazon WorkSpaces Web è un servizio on-demand, completamente gestito, basato su Linux progettato per facilitare l'accesso sicuro tramite browser a siti Web interni e applicazioni Software-as-a-Service (SaaS). Accedi al servizio dai browser Web esistenti, senza l'onere amministrativo della gestione dell'infrastruttura, di software client specializzati o di soluzioni di rete privata virtuale (VPN).

Argomenti

Termini da conoscere per l'utilizzo di WorkSpaces Web

Prima di iniziare a usare WorkSpaces Web, è bene acquisire familiarità con i concetti seguenti:

Identity provider (IdP) (Provider di identità)

> Un provider di identità verifica le credenziali degli utenti. Rilascia quindi le asserzioni di autenticazione per fornire l'accesso a un provider di servizi. È possibile configurare un gestore dell'identità digitale esistente per il funzionamento con WorkSpaces Web.
>
> Il processo per configurare il gestore dell'identità digitale (IdP) varia in base all'IdP.
>
> Devi caricare il file di metadati del fornitore di servizi sul tuo IdP. In caso contrario, i tuoi utenti non saranno in grado di accedere. Concedi l'accesso agli utenti del tuo IdP per utilizzare WorkSpaces Web.

Documento di metadati del gestore dell'identità digitale (IdP)

> WorkSpaces Web richiede metadati specifici dal gestore dell'identità digitale (IdP) per stabilire un rapporto di attendibilità. Puoi aggiungere questi metadati a WorkSpaces Web caricando un file di scambio di metadati scaricato dal tuo IdP.

Provider di servizi (SP)

> Un fornitore di servizi accetta asserzioni di autenticazione e fornisce un servizio all'utente. WorkSpaces Web funge da fornitore di servizi per gli utenti che sono stati autenticati dal loro IdP.

Documento di metadati del provider di servizi

Dovrai aggiungere i dettagli dei metadati del fornitore di servizi all'interfaccia di configurazione del tuo gestore dell'identità digitale (IdP). I dettagli di questo processo di configurazione variano tra i provider.

SAML 2.0

Uno standard per lo scambio di dati di autenticazione e autorizzazione tra un provider di identità e un provider di servizi.

Virtual Private Cloud (VPC)

È possibile utilizzare un VPC nuovo o esistente, le sottoreti corrispondenti e i gruppi di sicurezza per collegare il contenuto a WorkSpaces Web.

Le sottoreti devono disporre di una connessione stabile a Internet e il VPC e le sottoreti devono inoltre disporre di una connessione stabile a qualsiasi sito Web interno e Software as a Service (SaaS) per consentire agli utenti di accedere a queste risorse.

I VPC, le sottoreti e i gruppi di sicurezza elencati provengono dalla stessa area della Console WorkSpaces Web.

Trust store (Archivio trust)

Se un utente che accede a un sito Web tramite WorkSpaces Web riceve un errore di privacy, ad esempio NET::ERR_CERT_INVALID, quel sito potrebbe utilizzare un certificato firmato da un'autorità di certificazione privata (PCA). Potrebbe essere necessario aggiungere o modificare i PCA nel tuo trust store. Inoltre, se il dispositivo di un utente richiede l'installazione di un certificato specifico per caricare un sito Web, sarà necessario aggiungere tale certificato al trust store per consentire all'utente di accedere a quel sito in WorkSpaces Web.

I siti Web accessibili al pubblico di solito non richiedono alcuna modifica a un trust store.

Portali Web

Un portale Web fornisce agli utenti l'accesso ai siti Web interni e SaaS dai loro browser. Puoi creare un portale web in qualsiasi area supportata per account. Per richiedere un aumento del limite per più di un portale, contatta il supporto.

Endpoint del portale Web

L'endpoint del portale Web è il punto di accesso da cui gli utenti avvieranno il portale Web dopo aver effettuato l'accesso con il gestore dell'identità digitale configurato per il portale.

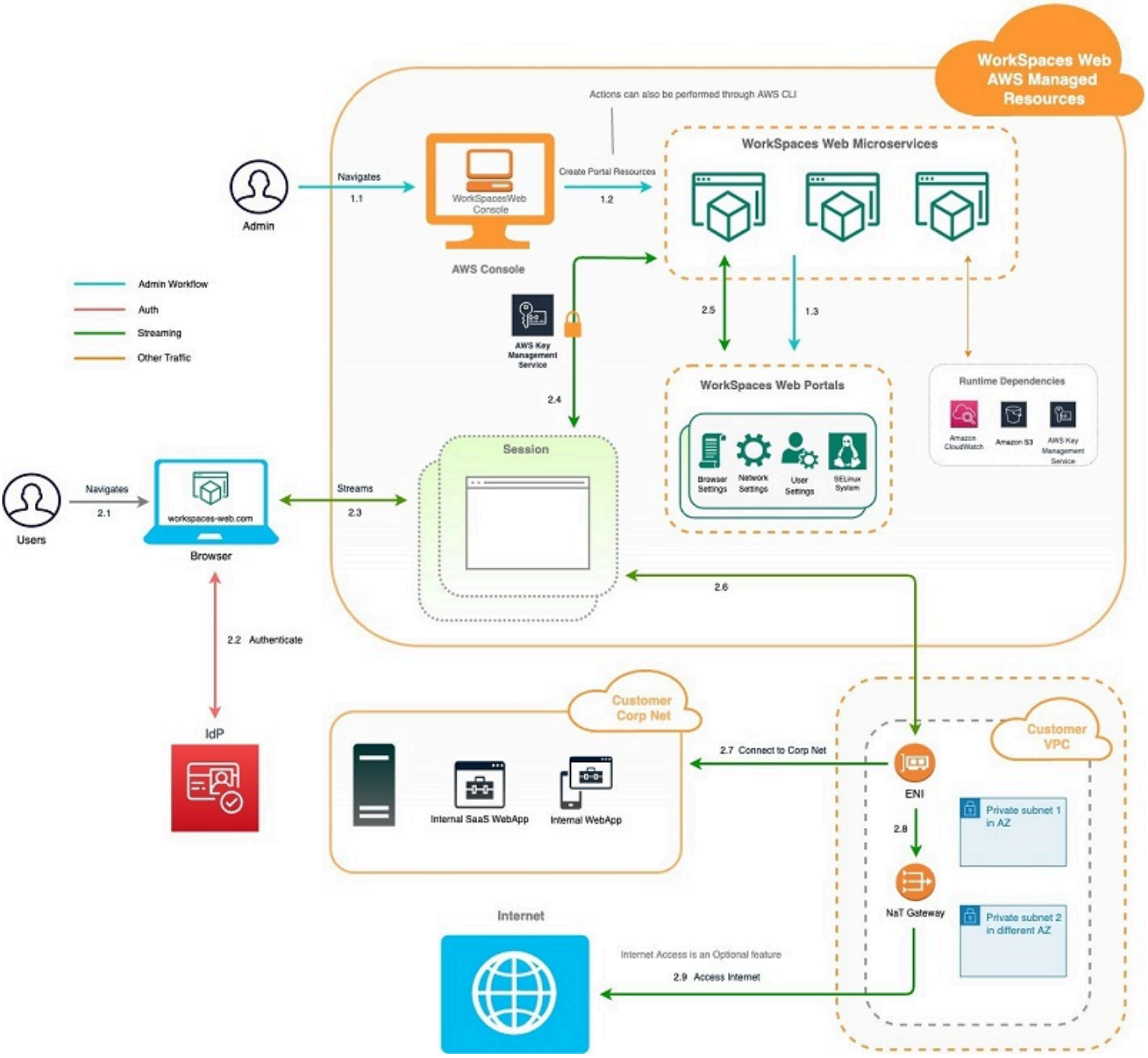
L’endpoint è disponibile pubblicamente su Internet e può essere integrato nella rete.

Servizi correlati

WorkSpaces Web è una funzionalità di Amazon WorkSpaces nel portafoglio AWS End User Computing. Rispetto a WorkSpaces e AppStream 2.0, WorkSpaces Web è progettato specificamente per facilitare carichi di lavoro sicuri e basati sul Web. WorkSpaces Web viene gestito automaticamente, con capacità, scalabilità e immagini fornite e aggiornate su richiesta da AWS. Ad esempio, puoi scegliere di offrire un Workspace Desktop persistente agli sviluppatori di software che devono accedere alle risorse desktop e Amazon WorkSpaces Web agli utenti dei contact center che devono accedere solo ad alcuni siti Web interni e SaaS (compresi quelli ospitati all'esterno della tua rete) su computer desktop.

Architettura

Il diagramma seguente illustra l'architettura di base di WorkSpaces Web.



Accesso ad Amazon WorkSpaces Web

Gli amministratori accedono ad Amazon WorkSpaces Web tramite la console AWS WorkSpaces Web, l'SDK, la CLI o l'API. I tuoi utenti vi accedono tramite l'endpoint Amazon WorkSpaces Web.

Configurazione di Amazon WorkSpaces Web

Prima di poter configurare Amazon WorkSpaces Web per raggiungere i siti Web interni e le applicazioni SaaS, è necessario completare i seguenti prerequisiti.

Argomenti

Registrazione e creazione di un utente

Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo aver effettuato la registrazione di un Account AWS, proteggi Utente root dell'account AWS, abilita AWS IAM Identity Center e crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root della Guida per l'utente di Accedi ad AWS.
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per ricevere istruzioni, consulta Abilitazione di un dispositivo MFA virtuale per l'utente root dell'Account AWS (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita IAM Identity Center

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center.
2. In Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come origine di identità, consulta Configure user access with the default IAM Identity Center directory nella Guida per l'utente di AWS IAM Identity Center.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta Accedere al portale di accesso AWS nella Guida per l'utente Accedi ad AWS.

Concessione dell'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se desiderano interagire con AWS esternamente a AWS Management Console. La modalità con cui concedere l'accesso programmatico dipende dal tipo di utente che accede ad AWS.

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Configurazione della AWS CLI per l'uso di AWS IAM Identity Center nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK AWS, gli strumenti e le API AWS, consulta la pagina Autentica zione Centro identità IAM nella Guida di riferimento per SDK e strumenti AWS.
IAM	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni in Utilizzo di credenziali temporanee con le risorse AWS nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche alla AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Autenticazione

Quale utente necessita dell'accesso programmatico?	Per	Come
	CLI, agli SDK AWS o alle API AWS.	tramite credenziali utente IAM nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK e gli strumenti AWS, consulta la pagina Autenticazione con credenziali a lungo termine nella Guida di riferimento per SDK e strumenti AWS. • Per le API AWS, consulta la pagina Gestione delle chiavi di accesso per utenti IAM nella Guida per l'utente IAM.

Reti e accesso

I seguenti argomenti spiegano come configurare le istanze di streaming WorkSpaces Web in modo che gli utenti possano connettersi ad esse. Spiega inoltre come consentire alle istanze di streaming WorkSpaces Web di accedere alle risorse VPC e a Internet.

Argomenti

- Requisiti VPC
- Consigli per l'installazione di VPC
- Zone di disponibilità supportate
- Connessione VPC
- Connessione client/utente

Requisiti VPC

Durante la creazione del portale WorkSpaces Web, selezionerai un VPC nel tuo account. Scegli anche almeno due sottoreti in due diverse zone di disponibilità. Il VPC e le sottoreti devono soddisfare i seguenti requisiti:

- Il VPC deve disporre di una tenancy predefinita. I VPC con tenancy dedicata non sono supportati.
- Per valutare la disponibilità, sono necessarie almeno due sottoreti create in due diverse zone di disponibilità. Le sottoreti devono avere indirizzi IP sufficienti per supportare il traffico Web previsto WorkSpaces . Configura ciascuna delle sottoreti con una subnet mask che consente un numero sufficiente di indirizzi IP client per tenere conto del numero massimo di utenti simultanei previsti. Per ulteriori informazioni, consulta Creazione e configurazione di un nuovo VPC.
- Tutte le sottoreti devono disporre di una connessione stabile a qualsiasi contenuto interno, situato all'interno Cloud AWS o in locale, a cui gli utenti accederanno tramite Web. WorkSpaces

Ti consigliamo di scegliere tre sottoreti in diverse zone di disponibilità per valutare la disponibilità e la scalabilità. Per ulteriori informazioni, consulta Creazione e configurazione di un nuovo VPC.

WorkSpaces Web non assegna alcun indirizzo IP pubblico alle istanze di streaming per consentire l'accesso a Internet. Ciò renderebbe le istanze di streaming accessibili da Internet. Pertanto, qualsiasi istanza di streaming connessa alla sottorete pubblica non avrà accesso a Internet. Se desideri che il tuo portale WorkSpaces Web abbia accesso sia ai contenuti Internet pubblici che ai contenuti VPC privati, completa i passaggi seguenti. Abilita la navigazione Internet senza restrizioni (scelta consigliata)

Creazione e configurazione di un nuovo VPC

In questo argomento viene descritto come utilizzare la procedura guidata del VPC per creare un VPC con una sottorete pubblica e una sottorete privata. Come parte di questo processo, la procedura guidata crea un gateway Internet e un gateway NAT. Viene creata anche una tabella di routing personalizzata associata alla sottorete pubblica. Quindi, viene aggiornata la tabella di routing principale associata alla sottorete privata. Il gateway NAT viene automaticamente creato nella sottorete pubblica del VPC.

Dopo aver utilizzato la procedura guidata per creare la configurazione VPC iniziale, verrà aggiunta una seconda sottorete privata. Per ulteriori informazioni su questa configurazione, consulta VPC con sottoreti pubbliche e private (NAT).

Fase 1: allocazione di un indirizzo IP elastico

Prima di creare il tuo VPC, devi allocare un indirizzo IP elastico nella tua WorkSpaces area Web. Una volta allocato, è possibile associare l'indirizzo IP elastico al gateway NAT. Con un indirizzo IP elastico puoi mascherare l'errore di un'istanza di streaming rimappando rapidamente l'indirizzo a un'altra istanza di streaming nel VPC. Per ulteriori informazioni, consulta Indirizzi IP elastici.

> **Note**
>
> Potrebbero essere applicati dei costi per gli indirizzi IP elastici utilizzati. Per ulteriori informazioni, consulta Indirizzi IP elastici nella pagina dei prezzi.

Se non disponi già di un indirizzo IP elastico, completa la procedura seguente. Se desideri utilizzare un indirizzo IP elastico esistente, assicurati che non sia attualmente associato a un'altra istanza o interfaccia di rete.

Per allocare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Network & Security (Rete e sicurezza), scegliere Elastic IPs (IP elastici).
3. Selezionare Allocate new address (Alloca un nuovo indirizzo), quindi scegliere Allocate (Alloca).
4. Nota l'indirizzo IP elastico mostrato sulla console.
5. Nell'angolo in alto a destra del riquadro IP elastici, fare clic sull'icona × per chiudere il riquadro.

Fase 2: creazione di un nuovo VPC

Completa la procedura seguente per creare un nuovo VPC con una sottorete pubblica e una sottorete privata.

Per creare un nuovo VPC

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare VPC Dashboard (Pannello di controllo VPC).
3. Scegli Launch VPC Wizard (Avvia procedura guidata VPC).

4. In Step 1: Select a VPC Configuration (Fase 1: selezione di una configurazione VPC), scegliere VPC with Public and Private Subnets (VPC con sottoreti pubbliche e private), quindi selezionare Select (Seleziona).
5. In Step 2: VPC with Public and Private Subnets (Fase 2: VPC con sottoreti pubbliche e private), configurare il VPC come segue:

   - In IPv4 CIDR block (Blocco CIDR IPv4), specificare un blocco CIDR IPv4 per il VPC.
   - In IPv6 CIDR block (Blocco CIDR IPv6), mantenere il valore predefinito, No IPv6 CIDR Block (Nessun blocco CIDR IPv6).
   - In Nome VPC, digita un nome univoco per il VPC.
   - Configurare la sottorete pubblica come segue:
     - In Public subnet's IPv4 CIDR (CIDR IPv4 della sottorete pubblica), specificare il blocco CIDR per la sottorete.
     - In Availability Zone (Zona di disponibilità), mantenere il valore predefinito, No Preference (Nessuna preferenza).
     - In Nome sottorete pubblica immetti un nome per la sottorete. Ad esempio, **`WorkSpaces Web Public Subnet`**.
   - Configurare la prima sottorete privata come segue:
     - In Private subnet's IPv4 CIDR (CIDR IPv4 della sottorete privata), specificare il blocco CIDR per la sottorete. Prendere nota del valore specificato.
     - In Availability Zone (Zona di disponibilità), selezionare una zona specifica e prendere nota della zona selezionata.
     - In Nome sottorete privata immetti un nome per la sottorete. Ad esempio, **`WorkSpaces Web Private Subnet1`**.
   - Ove applicabile, mantenere i valori predefiniti per i campi rimanenti.
   - In ID allocazione IP elastico, inserire il valore corrispondente all'indirizzo IP elastico creato. Questo indirizzo viene quindi assegnato al gateway NAT. Se non disponi di un indirizzo IP elastico, creane uno utilizzando la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
   - In Endpoint del servizio, se è richiesto un endpoint Amazon S3 per l'ambiente, specificane uno.

     Per specificare un endpoint Amazon S3, effettua le operazioni seguenti:

     1. Scegli Aggiungi endpoint.

2. Per Assistenza, seleziona la voce com.amazonaws.***Region***.s3, dove *Regione* è l'area Regione AWS in cui stai creando il tuo VPC.
3. In Subnet (Sottorete), scegliere Private subnet (Sottorete privata).
4. In Policy, mantenere il valore predefinito, Full Access (Accesso completo).

- In Enable DNS hostnames (Abilita nomi host DNS), mantenere il valore predefinito, Yes (Sì).
- In Hardware tenancy (Tenancy hardware), mantenere il valore predefinito, Default (Predefinito).
- Seleziona Crea VPC.
- Da notare che occorrono diversi minuti per configurare il VPC. Dopo aver creato il VPC, scegliere OK.

Fase 3: aggiunta di una seconda sottorete privata

Nella fase precedente, è stato creato un VPC con una sottorete pubblica e una sottorete privata. Esegui la procedura seguente per aggiungere una seconda sottorete privata al tuo VPC. Ti consigliamo di aggiungere una seconda sottorete privata in una zona di disponibilità diversa rispetto alla prima sottorete privata.

Aggiunta di una seconda sottorete privata

1. Nel pannello di navigazione, scegli Subnets (Sottoreti).
2. Selezionare la prima sottorete privata creata nella fase precedente. Nella scheda Description (Descrizione), sotto l'elenco di sottoreti, prendere nota della zona di disponibilità per questa sottorete.
3. Nell'angolo in alto a sinistra del riquadro delle sottoreti, scegliere Create Subnet (Crea sottorete).
4. Per Tag nome immettere un nome per la sottorete privata. Ad esempio, **`WorkSpaces Web Private Subnet2`**.
5. In VPC, selezionare il VPC creato nella fase precedente.
6. In Zona di disponibilità, selezionare una zona di disponibilità diversa da quella utilizzata per la prima sottorete privata. La selezione di una zona di disponibilità diversa incrementa la tolleranza ai guasti e consente di prevenire errori dovuti a capacità insufficiente.
7. In IPv4 CIDR block (Blocco CIDR IPv4), specificare un intervallo di blocchi CIDR univoco per la nuova sottorete. Ad esempio, se la prima sottorete privata dispone di un intervallo di blocchi CIDR IPv4 di **`10.0.1.0/24`**, è possibile specificare un intervallo di blocchi CIDR **`10.0.2.0/24`** per la seconda sottorete privata.

8. Scegli Crea.
9. Dopo aver creato la sottorete, scegliere Close (Chiudi).

Fase 4: verifica e denominazione delle tabelle di routing della sottorete

Dopo aver creato e configurato il VPC, completa la procedura seguente per specificare un nome per le tabelle di routing. Dovrai verificare che i seguenti dettagli siano corretti per la tua tabella di routing:

- La tabella di routing associata alla sottorete in cui risiede il gateway NAT deve includere un routing che indirizza il traffico Internet a un gateway Internet. Ciò garantisce che il gateway NAT possa accedere a Internet.
- Le tabelle di routing associate alle sottoreti private devono essere configurate per indirizzare il traffico Internet al gateway NAT. Ciò consente alle istanze di streaming nelle sottoreti private di comunicare con Internet.

Verifica e denominazione delle tabelle di routing della sottorete

1. Nel riquadro di navigazione, scegliere Sottoreti e selezionare la sottorete pubblica creata. Ad esempio, WorkSpaces Web 2.0 Public Subnet.
2. Nella scheda Route Table (Tabella di routing), scegliere l'ID della tabella di routing. Ad esempio, rtb-12345678.
3. Seleziona la tabella di instradamento del . In Nome, scegli l'icona Modifica (matita) e immetti un nome per la tabella. Ad esempio, è possibile inserire il nome **`workspacesweb-public-routetable`**. Quindi selezionare il segno di spunta per salvare il nome.
4. Con la tabella di routing pubblica ancora selezionata, nella scheda Routing verificare che esistano due routing: uno per il traffico locale e uno che invia tutto il traffico rimanente al gateway Internet del VPC. La tabella seguente descrive queste due route:

Destinazione	Target	Descrizione
Blocco CIDR IPv4 della sottorete pubblica (ad esempio, 10.0.0/20)	Locale	Tutto il traffico delle risorse destinato agli indirizzi IPv4 all'interno del blocco CIDR IPv4 della sottorete pubblica. Questo traffico

Destinazione	Target	Descrizione
		viene instradato localmente all'interno del VPC.
Traffico destinato a tutti gli altri indirizzi IPv4 (ad esempio, 0.0.0.0/0)	In uscita (igw-ID)	Il traffico destinato a tutti gli altri indirizzi IPv4 viene instradato al gateway Internet (identificato da igw-ID) che è stato creato dalla procedura guidata VPC.

5. Nel pannello di navigazione, scegli Subnets (Sottoreti). Quindi seleziona la prima sottorete privata che hai creato (ad esempio, **`WorkSpaces Web Private Subnet1`**).
6. Nella scheda Tabella di routing, scegliere l'ID della tabella di routing.
7. Seleziona la tabella di instradamento del . In Nome, scegli l'icona Modifica (matita) e immetti un nome per la tabella. Ad esempio, è possibile inserire il nome **`workspacesweb-private-routetable`**. Per salvare il nome, scegli il segno d spunta.
8. Nella scheda Routes (Route), verificare che la tabella di routing includa le seguenti route:

Destinazione	Target	Descrizione
Blocco CIDR IPv4 della sottorete pubblica (ad esempio, 10.0.0/20)	Locale	Tutto il traffico delle risorse destinato agli indirizzi IPv4 all'interno del blocco CIDR IPv4 della sottorete pubblica viene instradato localmente all'interno del VPC.
Traffico destinato a tutti gli altri indirizzi IPv4 (ad esempio, 0.0.0.0/0)	In uscita (nat-ID)	Il traffico destinato a tutti gli altri indirizzi IPv4 viene instradato al gateway NAT (identificato da nat-ID).
Il traffico destinato ai bucket S3 (applicabile se è stato specificato un endpoint S3)	Archiviazione (vpce-ID)	Il traffico destinato ai bucket S3 viene instradato all'endpo

Destinazione	Target	Descrizione
[pl-ID (com.amazonaws.region.s3)]		int S3 (identificato da vpce-ID).

9. Nel pannello di navigazione, scegli Subnets (Sottoreti). Quindi seleziona la seconda sottorete privata che hai creato (ad esempio, **`WorkSpaces Web Private Subnet2`**).
10. Nella scheda Tabella di routing, verificare che la tabella di routing sia la tabella di routing privata (ad esempio **`workspacesweb-private-routetable`**). Se la tabella di routing è diversa, scegliere Modifica e selezionare questa tabella di routing.

Abilita la navigazione Internet senza restrizioni (scelta consigliata)

Per configurare un VPC con un gateway NAT per una navigazione Internet senza restrizioni, segui la procedura illustrata qui. Ciò garantisce l'accesso WorkSpaces Web ai siti sulla rete Internet pubblica e ai siti privati ospitati o con una connessione al tuo VPC.

Configurare un VPC con un gateway NAT per una navigazione Internet senza restrizioni

Se desideri che il tuo portale WorkSpaces Web abbia accesso sia ai contenuti Internet pubblici che ai contenuti VPC privati, procedi nel seguente modo:

> **Note**
>
> Se hai già configurato un VPC, completa la procedura seguente per aggiungere un gateway NAT al VPC. Se occorre creare un nuovo VPC, consulta Creazione e configurazione di un nuovo VPC.

1. Per creare il gateway NAT, completare le fasi in Crea un gateway NAT. Assicurati che questo gateway NAT abbia una connettività pubblica e si trovi in una sottorete pubblica del tuo VPC.
2. È necessario specificare almeno due sottoreti private in diverse zone di disponibilità. L'assegnazione delle sottoreti a diverse zone di disponibilità aiuta a garantire una maggiore disponibilità e una migliore tolleranza agli errori. Per informazioni su come creare una seconda sottorete privata, consulta the section called “Fase 3: aggiunta di una seconda sottorete privata”.

> **Note**
>
> Per assicurarvi che ogni istanza di streaming abbia accesso a Internet, non collegate una sottorete pubblica al WorkSpaces portale Web.

3. Aggiornare la tabella di routing associata a una o più sottoreti private per indirizzare il traffico vincolato a Internet al gateway NAT. Ciò consente alle istanze di streaming nelle sottoreti private di comunicare con Internet. Per informazioni su come associare una tabella di routing a una sottorete privata, completa i passaggi in Configurazione delle tabelle di routing.

Abilita la navigazione Internet con restrizioni (utilizzando il proxy HTTP in uscita)

La configurazione di rete consigliata di un portale WorkSpaces Web consiste nell'utilizzare sottoreti private con gateway NAT, in modo che il portale possa navigare sia su Internet pubblico che su contenuti privati. Per ulteriori informazioni, consulta the section called “Abilita la navigazione Internet senza restrizioni (scelta consigliata)”. Tuttavia, potrebbe essere necessario controllare le comunicazioni in uscita da un portale WorkSpaces Web a Internet utilizzando un proxy Web. Ad esempio, se si utilizza un proxy Web come gateway per Internet, è possibile implementare controlli di sicurezza preventivi, come l'elenco dei domini consentiti e il filtraggio dei contenuti. Ciò può anche ridurre l'utilizzo della larghezza di banda e migliorare le prestazioni della rete memorizzando nella cache le risorse a cui si accede di frequente, come pagine Web o aggiornamenti software a livello locale. In alcuni casi d'uso, potresti avere contenuti privati accessibili solo tramite un proxy web.

Potresti già avere familiarità con la configurazione delle impostazioni del proxy sui dispositivi gestiti o sull'immagine dei tuoi ambienti virtuali. Tuttavia, ciò rappresenta una sfida se non si ha il controllo del dispositivo (ad esempio, quando gli utenti utilizzano dispositivi non di proprietà o gestiti dall'azienda) o se è necessario gestire l'immagine per l'ambiente virtuale. Con WorkSpaces Web, puoi configurare le impostazioni del proxy utilizzando i criteri di Chrome integrati nel browser web. Puoi farlo configurando un proxy HTTP in uscita per il WorkSpaces Web.

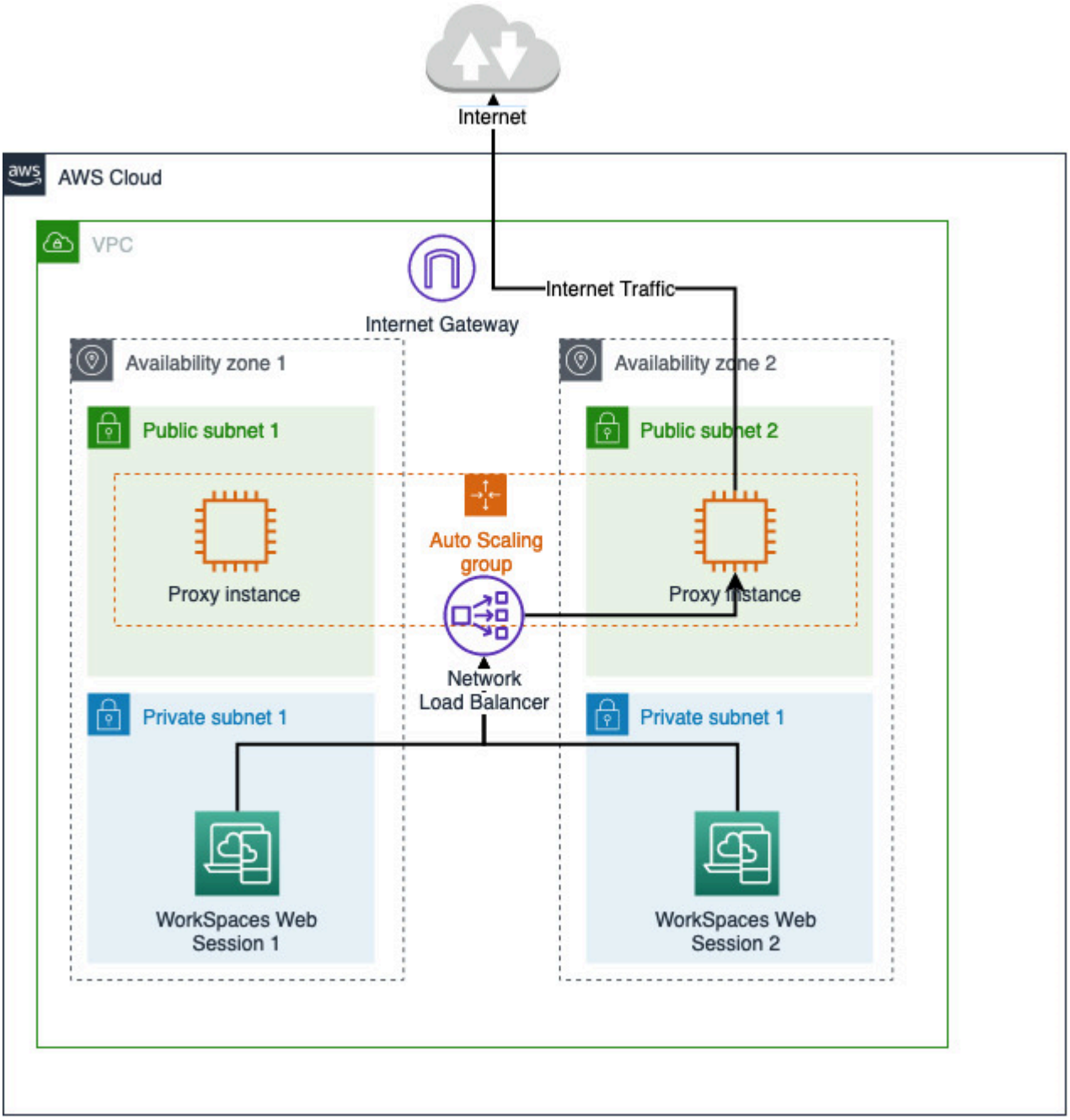
Questa soluzione si basa su una configurazione proxy VPC in uscita consigliata. La soluzione proxy si basa sul proxy HTTP open source Squid. Quindi, utilizza le impostazioni del browser WorkSpaces Web per configurare il portale WorkSpaces Web per la connessione all'endpoint proxy. Per ulteriori informazioni, consulta Come configurare un proxy VPC in uscita con whitelisting del dominio e filtraggio dei contenuti.

Questa soluzione offre i seguenti vantaggi:

- Un proxy in uscita che include un gruppo di istanze Amazon EC2 con scalabilità automatica, ospitate da un sistema di bilanciamento del carico di rete. Le istanze proxy risiedono in una sottorete pubblica e ognuna di esse è collegata a un IP elastico, in modo che possano avere accesso a Internet.
- Un portale WorkSpaces Web distribuito su sottoreti private. Non è necessario configurare il gateway NAT per abilitare l'accesso a Internet. È invece necessario configurare la politica del browser, in modo che tutto il traffico Internet passi attraverso il proxy in uscita. Se si desidera utilizzare il proprio proxy, la configurazione del portale WorkSpaces Web sarà simile.

Architettura

Di seguito è riportato un esempio di configurazione proxy tipica nel tuo VPC. L'istanza proxy Amazon EC2 si trova in sottoreti pubbliche ed è associata a Elastic IP, quindi ha accesso a Internet. Un sistema di bilanciamento del carico di rete ospita un gruppo di istanze proxy con scalabilità automatica. Ciò garantisce la scalabilità automatica delle istanze proxy e il sistema di bilanciamento del carico di rete è l'unico endpoint proxy, che può essere utilizzato dalle sessioni Web. WorkSpaces



Prerequisiti

Prima di iniziare, assicurati di soddisfare i seguenti prerequisiti:

- È necessario un VPC già distribuito, con sottoreti pubbliche e private distribuite su diverse zone di disponibilità (AZ). Per ulteriori informazioni su come configurare l'ambiente VPC, consulta VPC predefiniti.

- È necessario un unico endpoint proxy accessibile da sottoreti private, in cui risiedono le sessioni WorkSpaces Web (ad esempio, il nome DNS del network load balancer). Se desideri utilizzare il proxy esistente, assicurati che disponga anche di un unico endpoint accessibile dalle sottoreti private.

Configura un proxy HTTP in uscita per il Web WorkSpaces

Per configurare un proxy HTTP in uscita per il WorkSpaces Web, segui questi passaggi.

1. Per distribuire un esempio di proxy in uscita sul tuo VPC, segui i passaggi in Come configurare un proxy VPC in uscita con whitelist del dominio e filtraggio dei contenuti.
   a. Segui la procedura descritta in «Installazione (configurazione unica)» per distribuire il modello al tuo account. CloudFormation Assicurati di scegliere il VPC e le sottoreti corretti come parametri del modello. CloudFormation
   b. Dopo la distribuzione, trova il parametro di CloudFormation output e. OutboundProxyDomainOutboundProxyPort Si tratta del nome e della porta DNS del proxy.
   c. Se disponi già di un proxy personale, salta questo passaggio e utilizza il nome DNS e la porta del proxy.
2. Nella console WorkSpaces Web, seleziona il tuo portale, quindi scegli Modifica.
   a. Nei dettagli della connessione di rete, scegli il VPC e le sottoreti private che hanno accesso al proxy.
   b. Nelle impostazioni della politica, aggiungi la seguente ProxySettings politica utilizzando un editor JSON. Il `ProxyServer` campo deve contenere il nome DNS e la porta del proxy. Per ulteriori dettagli sulla ProxySettings politica, consulta 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. Nella sessione WorkSpaces Web, vedrai che il proxy viene applicato all'impostazione di Chrome. Chrome utilizza le impostazioni proxy dell'amministratore.
4. Vai a chrome: //policy e alla scheda Chrome policy per confermare che il criterio sia applicato.
5. Verifica che la tua sessione WorkSpaces Web sia in grado di navigare correttamente nei contenuti Internet senza il gateway NAT. Nei CloudWatch registri, verifica che i registri di accesso al proxy Squid siano registrati.

Risoluzione dei problemi

Dopo aver applicato i criteri di Chrome, se la tua sessione WorkSpaces Web non riesce ancora ad accedere a Internet, segui questi passaggi per cercare di risolvere il problema:

- Verifica che l'endpoint proxy sia accessibile dalle sottoreti private in cui risiede il tuo WorkSpaces portale Web. A tale scopo, crea un'istanza EC2 nella sottorete privata e verifica la connessione dall'istanza EC2 privata all'endpoint proxy.
- Verifica che il proxy abbia accesso a Internet.
- Verifica che la politica di Chrome sia corretta.
  - Conferma la seguente formattazione per il `ProxyServer` campo della politica:`<Proxy DNS name>:<Proxy port>`. Non dovrebbe esserci nessun `http://` or `https://` nel prefisso.
  - Nella sessione WorkSpaces Web, usa Chrome per accedere a chrome: //policy e assicurati che il ProxySettings criterio sia applicato correttamente.

Consigli per l'installazione di VPC

I seguenti consigli consentono di configurare il VPC in modo più efficiente e sicuro.

Configurazione VPC complessiva

- Assicurati che la configurazione VPC possa supportare le esigenze di dimensionamento.
- Assicurati che le quote del servizio WorkSpaces Web (dette anche limiti) siano sufficienti a soddisfare la domanda prevista. Per richiedere un aumento delle quote, puoi usare la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/. Per informazioni sulle quote WorkSpaces Web predefinite, vedere. the section called “Richiedi un aumento della quota di servizio.”

- Se prevedi di fornire alle tue sessioni di streaming l'accesso a Internet, ti consigliamo di configurare un VPC con un gateway NAT in una sottorete pubblica.

Interfacce di rete elastiche

- Ogni sessione WorkSpaces Web richiede la propria interfaccia di rete elastica per tutta la durata dello streaming. WorkSpaces Web crea tante interfacce di rete elastiche (ENI) quante sono le capacità massime desiderate del parco macchine. Per impostazione predefinita, il limite di ENI per regione è 5000. Per ulteriori informazioni, consulta Interfacce di rete.

  Quando pianifichi la capacità per implementazioni molto grandi, ad esempio migliaia di sessioni di streaming simultanee, considera il numero di ENI che potrebbero essere necessari per il picco di utilizzo. Ti consigliamo di mantenere il limite ENI pari o superiore al limite massimo di utilizzo simultaneo configurato per il tuo portale web.

Sottoreti

- Durante lo sviluppo del piano di ampliamento degli utenti, tenete presente che ogni sessione WorkSpaces Web richiede un indirizzo IP client univoco proveniente dalle sottoreti configurate. Pertanto, la dimensione dello spazio degli indirizzi IP del client configurato nelle sottoreti determina il numero di utenti che possono eseguire lo streaming contemporaneamente.
- Configura ciascuna delle sottoreti con una subnet mask che consente un numero sufficiente di indirizzi IP client per tenere conto del numero massimo di utenti simultanei previsti. Inoltre, consenti ulteriori indirizzi IP per tenere conto della crescita prevista. Per ulteriori informazioni, consulta VPC e dimensionamento delle sottoreti in IPv4.
- Si consiglia di configurare una sottorete in ogni zona di disponibilità univoca supportata da WorkSpaces Web nella regione desiderata per tenere conto della disponibilità e della scalabilità. Per ulteriori informazioni, consulta the section called “Creazione e configurazione di un nuovo VPC”.
- Assicurati che le risorse di rete richieste per le applicazioni Web siano accessibili tramite entrambe le sottoreti private.

Gruppi di sicurezza

- Utilizza i gruppi di sicurezza per fornire un controllo degli accessi aggiuntivo al VPC.

I gruppi di sicurezza che appartengono al tuo VPC ti consentono di controllare il traffico di rete tra le istanze di streaming WorkSpaces Web e le risorse di rete richieste dalle applicazioni Web. Assicurati che i gruppi di sicurezza forniscano l'accesso alle risorse di rete richieste dalle applicazioni Web.

Zone di disponibilità supportate

Quando si crea un cloud privato virtuale (VPC) da utilizzare con il WorkSpaces Web, le sottoreti del VPC devono risiedere in diverse zone di disponibilità nella regione in cui si avvia Web. WorkSpaces Le zone di disponibilità sono sedi separate progettate per rimanere isolate dai guasti che si verificano in altre zone di disponibilità. Avviando istanze in zone di disponibilità separate, potrai proteggere le tue applicazioni dai guasti di una singola posizione. Ogni sottorete deve risiedere totalmente all'interno di una zona di disponibilità e non può estendersi in altre zone. Ti consigliamo di configurare una sottorete per ogni AZ supportata nella regione desiderata per la massima resilienza

Una zona di disponibilità è rappresentata da un codice Regione seguito da un identificatore di lettera, ad esempio `us-east-1a`. Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account AWS. Ad esempio, la zona di disponibilità `us-east-1a` per l'account AWS potrebbe avere un'ubicazione diversa rispetto a `us-east-1a` per un altro account AWS.

Per coordinare le zone di disponibilità tra account, devi utilizzare l'ID AZ, identificatore unico e coerente per una zona di disponibilità. Ad esempio, `use1-az2` è un ID AZ per la regione `us-east-1` e ha la stessa posizione in ogni account AWS.

La visualizzazione degli ID AZ consente di stabilire la posizione delle risorse in un account rispetto alle risorse in un altro account. Ad esempio, se condividi una sottorete nella zona di disponibilità con l'ID AZ `use1-az2` con un altro account, questa sottorete è disponibile per tale account nella zona di disponibilità il cui ID AZ è anche `use1-az2`. L'ID AZ per ogni VPC e sottorete viene visualizzato nella console Amazon VPC.

WorkSpaces Il Web è disponibile in un sottoinsieme delle zone di disponibilità per ogni regione supportata. Nella tabella seguente sono elencati gli ID AZ che puoi utilizzare per ciascuna regione. Per vedere la mappatura degli ID AZ rispetto alle zone di disponibilità nel tuo account, consulta la sezione ID AZ per le tue risorse nella Guida per l'utente di AWS RAM.

Nome Regione	Codice regione	ID AZ supportati
Stati Uniti orientali (Virginia settentrionale)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
US West (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia Pacifico (Mumbai)	ap-south-1	aps1-az1, aps1-az3
Asia Pacifico (Seoul)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
Asia Pacifico (Singapore)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Asia Pacifico (Sydney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Asia Pacifico (Tokyo)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Canada (Centrale)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
Europa (Francoforte)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londra)	eu-west-2	euw2-az1, euw2-az2

Per ulteriori informazioni sulle zone di disponibilità e gli ID AZ, consulta Regioni, zone di disponibilità e zone locali nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Connessione VPC

Ogni istanza di streaming WorkSpaces Web dispone di un'interfaccia di rete del cliente che fornisce connettività alle risorse all'interno del VPC, nonché a Internet se sono configurate sottoreti private con gateway NAT.

Per la connettività Internet, le porte seguenti devono essere aperte per tutte le destinazioni. Se utilizzi un gruppo di sicurezza modificato o personalizzato, devi aggiungere le regole necessarie manualmente. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.

> **Note**
>
> Questo vale per il traffico in uscita.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

Connessione client/utente

WorkSpaces Il Web è configurato per instradare le connessioni di streaming sulla rete Internet pubblica. La connettività Internet è necessaria per autenticare gli utenti e fornire le risorse Web di cui il WorkSpaces Web ha bisogno per funzionare. Per consentire questo traffico, è necessario autorizzare i domini elencati in Domini consentiti.

I seguenti argomenti forniscono informazioni su come abilitare le connessioni degli utenti al WorkSpaces Web.

Argomenti

- Requisiti relativi a indirizzo IP e porta
- Domini consentiti

Requisiti relativi a indirizzo IP e porta

Per accedere alle istanze WorkSpaces Web, i dispositivi utente richiedono l'accesso in uscita sulle seguenti porte:

- Porta 443 (TCP)
  - La porta 443 viene utilizzata per la comunicazione HTTPS tra i dispositivi degli utenti e le istanze di streaming quando si utilizzano gli endpoint Internet. Di solito, quando gli utenti finali esplorano il Web durante le sessioni di streaming, il browser Web seleziona a caso una porta di origine nell'intervallo superiore per il traffico di streaming. Devi accertarti che il traffico di ritorno a questa porta è consentito.
  - Questa porta deve essere aperta ai domini richiesti elencati in Domini consentiti.
  - AWSpubblica gli intervalli di indirizzi IP correnti, inclusi gli intervalli in cui il Session Gateway e i CloudFront domini possono risolvere, in formato JSON. Per informazioni su come scaricare il file .json e visualizzare gli intervalli correnti, consulta Intervalli di indirizzi IP AWS. Oppure, se si utilizzaAWS Tools for Windows PowerShell, è possibile accedere alle stesse informazioni utilizzando il comando. Get-AWSPublicIpAddressRange PowerShell Per ulteriori informazioni, vedi l'argomento relativo al recupero di intervalli di indirizzi IP pubblici per AWS.
- (Opzionale) Porta 53 (UDP)
  - La porta 53 viene utilizzata per le comunicazioni tra i dispositivi degli utenti e i server DNS.
  - Questa porta è facoltativa se non utilizzi il server DNS per la risoluzione dei nomi di dominio.
  - La porta deve essere aperta per gli indirizzi IP per i server DNS di modo che i nomi di dominio pubblici possano essere risolti.

Domini consentiti

Per consentire all'utente di accedere al servizio WorkSpaces Web dal browser locale, è necessario aggiungere i seguenti domini e indirizzi IP all'elenco degli indirizzi consentiti sulla rete da cui l'utente sta tentando di accedere al servizio.

Il nome del sistema operativo Regione AWS deve essere sostituito dalla *{Region}* riportata di seguito. Ad esempio, s3.*{region}*.amazonaws.com dovrebbe essere s3.eu-west-1.amazonaws.com se è per l'Europa (Irlanda) (eu-west-1).

Categoria	Dominio o indirizzo IP
WorkSpaces Risorsa per lo streaming Web	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com

Categoria	Dominio o indirizzo IP
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces WebApp Risorsa Web	*.workspaces-web.com
WorkSpaces Autenticazione Web	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Metriche e report Web	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

A seconda del gestore dell'identità digitale configurato, potrebbe anche essere necessario aggiungere altri domini all'elenco consentiti. Consulta la documentazione del tuo IdP per identificare quali domini devi inserire nell'elenco per consentire a WorkSpaces Web di utilizzare quel provider. Se utilizzi IAM Identity Center, consulta i prerequisiti di IAM Identity Center per ulteriori informazioni.

Guida introduttiva ad Amazon WorkSpaces Web

Segui questi passaggi per creare un portale WorkSpaces Web Web e fornire agli utenti l'accesso ai siti Web interni e SaaS dai browser esistenti. Puoi creare un portale web in qualsiasi area supportata per account.

> **Note**
>
> Per richiedere un aumento del limite per più di un portale, contatta l'assistenza indicando il tuo Account AWS ID, il numero di portali da richiedere e. Regione AWS

Questo processo richiede in genere cinque minuti con la procedura guidata di creazione del portale Web e fino a altri 15 minuti affinché il portale diventi attivo.

Non ci sono costi associati alla configurazione di un portale web. WorkSpaces Web offre pay-as-you-go prezzi, incluso un prezzo mensile basso per gli utenti che utilizzano attivamente il servizio. Non ci sono costi iniziali, licenze o impegni a lungo termine.

> **Important**
>
> Prima di iniziare devi completare i prerequisiti necessari per un portale web. Per ulteriori informazioni sui prerequisiti, consulta Configurazione di Amazon WorkSpaces Web.

Argomenti

Fase 1: creazione di un portale Web

Per creare un portale web, segui queste fasi:

Argomenti

Configurazione delle impostazioni di rete

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Web, quindi Portali Web, quindi scegli Crea portale web.
3. Nella pagina Passaggio 1: specificare la connessione di rete, completa i seguenti passaggi per connettere il VPC al portale Web e configurare il VPC e le sottoreti.

    1. Per i dettagli sulla rete, scegli un VPC con una connessione ai contenuti a cui desideri che i tuoi utenti accedano tramite WorkSpaces Web.
    2. Scegli fino a tre sottoreti private che soddisfino i seguenti requisiti. Per ulteriori informazioni, consulta Reti e accesso.
        - È necessario scegliere un minimo di due sottoreti private per creare un portale.
        - Per garantire un'elevata disponibilità del tuo portale web, ti consigliamo di fornire il numero massimo di sottoreti private in zone di disponibilità uniche per il tuo VPC.
    3. Scelta del gruppo di sicurezza.

Per configurare le impostazioni del portale

Nella pagina Passaggio 2: Configurazione delle impostazioni del portale web, completa i seguenti passaggi per personalizzare l'esperienza di navigazione degli utenti all'inizio di una sessione.

1. In Dettagli del portale Web, in Nome visualizzato, inserisci un nome identificabile per il tuo portale web.
2. In Registrazione degli accessi utente, per ID flusso Kinesis, seleziona il flusso di dati Amazon Kinesis a cui desideri inviare i dati. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.
3. In Impostazioni delle policy, completa quanto segue:

- Per le Opzioni relative alle policy, seleziona Visual Editor o Caricamento di file JSON. È possibile utilizzare entrambi i metodi per fornire i dettagli di configurazione delle policy per il portale Web. Per ulteriori informazioni, consulta the section called “Imposta o modifica la policy del browser”.
  - WorkSpaces Il Web include il supporto per le politiche aziendali di Chrome. Puoi aggiungere e gestire le policy con un editor visivo o un caricamento manuale dei file delle policy. Puoi passare da un'opzione all'altra in qualsiasi momento.
  - Quando carichi un file di policy, puoi vedere le policy disponibili nel file nella console. Tuttavia, non è possibile modificare tutte le policy nell'editor visivo. La console elenca le policy nel file JSON che non è possibile modificare con l'editor visivo in Policy JSON aggiuntive. Per apportare modifiche a queste policy, devi modificarle manualmente.
- (Facoltativo) Per URL di avvio: facoltativo, inserisci un dominio da utilizzare come home page quando gli utenti avviano il browser. Il VPC deve includere una connessione stabile a questo URL.
- Seleziona o deseleziona Navigazione privata ed Eliminazione della cronologia per attivare o disattivare queste funzionalità durante la sessione di un utente

> **Note**
>
> Gli URL visitati durante la navigazione privata o prima che un utente elimini la cronologia del browser non possono essere registrati nella registrazione degli accessi degli utenti. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.

- In Filtraggio URL, puoi configurare gli URL che gli utenti possono visitare durante una sessione. Per ulteriori informazioni, consulta the section called “Imposta il filtraggio degli URL”.
- (Facoltativo) Per i Segnalibri del browser: facoltativo, inserisci il Nome visualizzato, il dominio e la Cartella per tutti i segnalibri che desideri che gli utenti vedano nel browser. Quindi, scegli Aggiungi segnalibro.

> **Note**
>
> Il dominio è un campo obbligatorio per i segnalibri del browser.
> In Chrome, gli utenti possono trovare i segnalibri gestiti nella cartella Segnalibri gestiti sulla barra degli strumenti dei segnalibri.

- (Facoltativo) Aggiungi tag per il portale. Puoi utilizzare i tag per cercare o filtrare le tue AWS risorse. I tag sono costituiti da un valore chiave e facoltativo e sono associati alla risorsa del portale.

4. In Controllo dell'accesso IP (opzionale), scegli se limitare l'accesso a reti affidabili. Per ulteriori informazioni, consulta the section called “Configura i controlli di accesso IP (opzionale)”.
5. Seleziona Successivo per continuare.

Configurazione delle impostazioni utente

Nel Passaggio 3: Seleziona la pagina delle impostazioni utente, completa i seguenti passaggi per scegliere a quali funzionalità gli utenti possono accedere dalla barra di navigazione in alto durante la sessione, quindi scegli Avanti:

1. Per le Autorizzazioni utente, scegli se abilitare l'estensione per il Single Sign-On. Per ulteriori informazioni, consulta the section called “Abilita l’estensione per Single Sign-On (opzionale)”.
2. Per le autorizzazioni per gli Appunti, scegli Disabilitato o Abilitato.
3. In Trasferimento file, scegli Disabilitato o Abilitato.
4. Per Stampa su dispositivo locale, scegli Consentito o Non consentito.
5. Per i Dettagli della sessione utente specifica quanto segue:

   - Per Disconnect timeout in minutes (Scollega timeout in pochi minuti), scegliere la quantità di tempo in cui una sessione di streaming rimane attiva dopo la disconnessione degli utenti. Se gli utenti provano a riconnettersi alla sessione di streaming dopo una disconnessione o un'interruzione di rete entro questo intervallo di tempo, vengono connessi alla sessione precedente. In caso contrario, vengono connessi a una nuova sessione con una nuova istanza di streaming.

     Se un utente termina la sessione, il timeout di disconnessione non si applica. Al contrario, all'utente viene chiesto di salvare qualsiasi documento aperto e quindi viene immediatamente disconnesso dall'istanza di streaming. L'istanza che l'utente stava utilizzando viene quindi terminata.
   - Per Idle disconnect timeout in minutes (Timeout disconnessione inattività in pochi minuti), scegliere la quantità di tempo in cui gli utenti possono rimanere inattivi prima di essere disconnessi dalla sessione di streaming e l'inizio dell'intervallo di tempo Disconnect timeout in minutes (Timeout disconnessione in minuti). Gli utenti ricevono una notifica prima che siano disconnessi a causa di inattività. Se tentano di riconnettersi alla sessione di streaming prima

che sia trascorso l'intervallo di tempo specificato in Disconnect timeout in minutes (Timeout disconnessione in minuti), vengono collegati alla sessione precedente. In caso contrario, vengono connessi a una nuova sessione con una nuova istanza di streaming. L'impostazione di questo valore su 0 lo disabilita. Quando questo valore viene disabilitato, gli utenti non vengono disconnessi a causa di inattività.

> **Note**
>
> Gli utenti sono considerati inattivi quando smettono di inviare input mediante tastiera o mouse nelle sessioni di streaming. Download e upload dei file, file audio in entrata e in uscita e modifiche dei pixel non vengono considerati attività degli utenti. Se gli utenti continueranno ad essere inattivi una volta trascorso Idle disconnect timeout in minutes (Timeout disconnessione inattività in pochi minuti), vengono disconnessi.

Configurazione dei gestore dell'identità digitale

Utilizza i seguenti passaggi per configurare il tuo provider di identità (IdP).

Argomenti

Scegli il tipo di provider di identità

WorkSpaces Web offre due tipi di autenticazione: Standard e AWS IAM Identity Center. È possibile scegliere il tipo di autenticazione da utilizzare con il portale nella pagina Configura provider di identità.

- Per Standard (opzione predefinita), federate il vostro provider di identità SAML 2.0 di terze parti (come Okta o Ping) direttamente con il portale. Per ulteriori informazioni, consulta the section called “Configura il tipo di autenticazione standard”. Il tipo standard supporta sia i flussi di autenticazione avviati da SP che quelli avviati da IdP.
- Per IAM Identity Center (opzione avanzata), federa IAM Identity Center con il tuo portale. Per utilizzare questo tipo di autenticazione, l'IAM Identity Center e il portale WorkSpaces Web devono

risiedere entrambi nello stesso. Regione AWS Per ulteriori informazioni, consulta the section called “Configura il tipo di autenticazione IAM Identity Center”.

Configura il tipo di autenticazione standard

Per Standard (impostazione predefinita), federa il tuo provider di identità SAML 2.0 di terze parti (come Okta o Ping) direttamente con il tuo portale.

Il tipo di identità Standard può supportare flussi di accesso service-provider-initiated (iniziati da SP) e identity-provider-initiated (avviati da IdP) con il tuo IdP conforme a SAML 2.0.

Passaggio 1: inizia a configurare il tuo provider di identità sul Web WorkSpaces

Completa i seguenti passaggi per configurare il tuo provider di identità:

1. Nella pagina Configura gestore dell'identità digitale della procedura guidata di creazione, scegli Standard.
2. Scegli Continua con IdP standard.
3. Scarica il file di metadati SP e mantieni aperta la scheda per i singoli valori dei metadati.
   - Se il file di metadati SP è disponibile, scegli Scarica file di metadati per scaricare il documento di metadati del fornitore di servizi (SP) e carica il file di metadati del fornitore di servizi sul tuo IdP nel passaggio successivo. Senza questo, gli utenti non saranno in grado di accedere.
   - Se il tuo provider non carica i file di metadati SP, inserisci manualmente i valori dei metadati.
4. In Scegli il tipo di accesso SAML, scegli tra asserzioni SAML avviate da SP e IdP o solo asserzioni SAML avviate da SP.
   - Le asserzioni SAML avviate da SP e IdP consentono al portale di supportare entrambi i tipi di flussi di accesso. I portali che supportano i flussi avviati dall'IdP consentono di presentare asserzioni SAML all'endpoint di federazione delle identità del servizio senza richiedere agli utenti di avviare una sessione visitando l'URL del portale.
     - Seleziona questa opzione per consentire al portale di accettare asserzioni SAML non richieste avviate da IdP.
     - Questa opzione richiede la configurazione di un Relay State predefinito nel tuo provider di identità SAML 2.0. Il parametro Relay state per il tuo portale si trova nella console in Accesso SAML avviato da IdP oppure puoi copiarlo dal file di metadati SP sotto. `<md:IdPInitRelayState>`
     - Nota

- Di seguito è riportato il formato dello stato del relè:. `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`
- Se copi e incolli il valore dal file di metadati SP, assicurati di passare `&` a. & `&`è un carattere di escape XML.

- Scegliete solo asserzioni SAML avviate da SP affinché il portale supporti solo i flussi di accesso avviati da SP. Questa opzione rifiuterà le asserzioni SAML non richieste dai flussi di accesso avviati dall'IdP.

> **Note**
>
> Alcune terze parti IdPs consentono di creare un'applicazione SAML personalizzata in grado di fornire esperienze di autenticazione avviate da IdP sfruttando i flussi avviati da SP. Ad esempio, consulta Aggiungere un'applicazione di segnalibri Okta.

5. Scegli se abilitare le richieste Sign SAML a questo provider. L'autenticazione avviata da SP consente all'IdP di verificare che la richiesta di autenticazione provenga dal portale, il che impedisce l'accettazione di altre richieste di terze parti.
   a. Scarica il certificato di firma e caricalo sul tuo IdP. Lo stesso certificato di firma può essere utilizzato per il singolo logout.
   b. Abilita la richiesta firmata nel tuo IdP. Il nome potrebbe essere diverso, a seconda dell'IdP.

> **Note**
>
> RSA-SHA256 è l'unico algoritmo di richiesta e firma delle richieste predefinito supportato.

6. Scegli se abilitare le asserzioni SAML crittografate Require. Ciò ti consente di crittografare l'asserzione SAML che proviene dal tuo IdP. Può impedire che i dati vengano intercettati nelle asserzioni SAML tra l'IdP e il Web. WorkSpaces

> **Note**
>
> Il certificato di crittografia non è disponibile in questa fase. Verrà creato dopo l'avvio del portale. Dopo aver avviato il portale, scarica il certificato di crittografia e caricalo sul tuo

IdP. Quindi, abilita la crittografia delle asserzioni nel tuo IdP (il nome potrebbe essere diverso a seconda dell'IdP).

7. Scegli se abilitare il Single Logout. Il single logout consente agli utenti finali di disconnettersi sia dall'IdP WorkSpaces che dalla sessione Web con un'unica azione.
   a. Scarica il certificato di firma dal WorkSpaces Web e caricalo sul tuo IdP. Si tratta dello stesso certificato di firma utilizzato per Request Signing nel passaggio precedente.
   b. L'utilizzo di Single Logout richiede la configurazione di un URL Single Logout nel provider di identità SAML 2.0. Puoi trovare l'URL di accesso singolo per il tuo portale nella console in Dettagli del fornitore di servizi (SP) - Mostra valori di metadati individuali o dal file di metadati SP sotto. `<md:SingleLogoutService>`
   c. Abilita Single Logout nel tuo IdP. Il nome potrebbe essere diverso, a seconda dell'IdP.

Passaggio 2: configura il tuo provider di identità sul tuo IdP

Apri una nuova scheda nel browser. Quindi, completa questa procedura con il tuo IdP:

1. Aggiungi i metadati del tuo portale al tuo IdP SAML.

   Carica il documento di metadati SP scaricato nel passaggio precedente sul tuo IdP oppure copia e incolla i valori dei metadati nei campi corretti del tuo IdP. Alcuni provider non consentono il caricamento di file.

   I dettagli di questo processo possono variare tra i provider. the section called “Linee guida per scopi specifici IdPs”Per assistenza su come aggiungere i dettagli del portale alla configurazione del tuo IdP, consulta la documentazione del tuo provider.
2. Conferma il NameID per l'asserzione SAML.

   Assicurati che il tuo IdP SAML inserisca NameID nell'asserzione SAML con il campo email dell'utente. Il NameID e l'e-mail dell'utente vengono utilizzati per identificare in modo univoco l'utente federato SAML con il portale. Utilizza il formato persistente SAML Name ID.
3. Facoltativo: configurare lo stato di inoltro per l'autenticazione avviata dall'IdP.

   Se nel passaggio precedente hai scelto Accetta asserzioni SAML avviate da SP e IdP, segui i passaggi del passaggio 2 di per impostare lo stato di inoltro predefinito the section called “Passaggio 1: inizia a configurare il tuo provider di identità sul Web WorkSpaces ” per la tua applicazione IdP.

4. Facoltativo: configura la firma delle richieste. Se hai scelto Firma richieste SAML a questo provider nel passaggio precedente, segui i passaggi del passaggio 3 the section called “Passaggio 1: inizia a configurare il tuo provider di identità sul Web WorkSpaces ” per caricare il certificato di firma sul tuo IdP e abilitare la firma delle richieste. Alcuni IdPs come Okta potrebbero richiedere che il NameID appartenga al tipo «persistente» per utilizzare la firma delle richieste. Assicurati di confermare il tuo NameID per l'asserzione SAML seguendo i passaggi precedenti.
5. Facoltativo: configura la crittografia delle asserzioni. Se hai scelto Richiedi asserzioni SAML crittografate da questo provider, attendi il completamento della creazione del portale, quindi segui il passaggio 4 in «Carica metadati» di seguito per caricare il certificato di crittografia sul tuo IdP e abilitare la crittografia delle asserzioni.
6. Facoltativo: configura Single Logout. Se hai scelto Single Logout, segui i passaggi indicati nel passaggio 5 the section called “Passaggio 1: inizia a configurare il tuo provider di identità sul Web WorkSpaces ” per caricare il certificato di firma sul tuo IdP, inserire Single Logout URL e abilitare Single Logout.
7. Concedi l'accesso ai tuoi utenti nel tuo IdP per utilizzare WorkSpaces il Web.
8. Scarica un file di scambio di metadati dal tuo gestore dell'identità digitale. Caricherai questi metadati WorkSpaces sul Web nel passaggio successivo.

Passaggio 3: Completare la configurazione del provider di identità sul Web WorkSpaces

Torna alla console WorkSpaces Web. Nella pagina Configura provider di identità della procedura guidata di creazione, in Metadati IdP, carica un file di metadati o inserisci un URL di metadati dal tuo IdP. Il portale utilizza questi metadati del tuo IdP per stabilire la fiducia.

1. Per caricare un file di metadati, in Documento di metadati IdP, scegli Scegli file. Carica il file di metadati in formato XML dal tuo IdP scaricato nel passaggio precedente.
2. Per utilizzare un URL di metadati, vai al tuo IdP che hai configurato nel passaggio precedente e ottieni il relativo URL dei metadati. Torna alla console WorkSpaces Web e, in URL dei metadati IdP, inserisci l'URL dei metadati che hai ottenuto dal tuo IdP.
3. Al termine, seleziona Next (Avanti).
4. Per i portali in cui hai abilitato l'opzione Richiedi asserzioni SAML crittografate da questo provider, devi scaricare il certificato di crittografia dalla sezione dei dettagli dell'IdP del portale e caricarlo sul tuo IdP. Quindi, puoi abilitare l'opzione Iì.

Note

WorkSpaces Il Web richiede che l'oggetto o il NameID siano mappati e impostati nell'asserzione SAML all'interno delle impostazioni del tuo IdP. Il tuo IdP può creare queste mappature automaticamente. Se queste mappature non sono configurate correttamente, gli utenti non possono accedere al portale web e iniziare una sessione.
WorkSpaces Web richiede che le seguenti affermazioni siano presenti nella risposta SAML. Puoi trovare <Your SP Entity ID>e consultare i <Your SP ACS URL>dettagli del fornitore di servizi o il documento di metadati del tuo portale, tramite la console o la CLI.

- Un `AudienceRestriction` claim con un `Audience` valore che imposta il tuo SP Entity ID come obiettivo della risposta. Esempio:

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

- Una richiesta `Response` con il valore `InResponseTo` dell'ID della richiesta SAML originale. Esempio:

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

- Un'`SubjectConfirmationData`attestazione con un `Recipient` valore dell'URL SP ACS e un `InResponseTo` valore che corrisponde all'ID della richiesta SAML originale. Esempio:

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

WorkSpaces Web convalida i parametri della richiesta e le asserzioni SAML. Per le asserzioni SAML avviate da IdP, i dettagli della richiesta devono essere formattati come `RelayState` parametri nel corpo di una richiesta HTTP POST. Il corpo della richiesta deve contenere anche l'asserzione SAML come parametro. `SAMLResponse` Entrambi dovrebbero essere presenti se hai seguito il passaggio precedente.
Di seguito è riportato un `POST` corpo di esempio per un provider SAML avviato da IdP.

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

Linee guida per scopi specifici IdPs

Per assicurarti di configurare correttamente la federazione SAML per il tuo portale, consulta i link seguenti per la documentazione di uso IdPs comune.

IdP	Configurazione dell'applicazione SAML	Gestione degli utenti	Autenticazione avviata da IDP	Richiedi la firma	Crittografia delle asserzioni	Disconnessione singola
Okta	Crea integrazioni di app SAML	Gestione degli utenti	Riferimento al campo SAML di Application Integration Wizard	Riferimento al campo SAML di Application Integration Wizard	Riferimento al campo SAML di Application Integration Wizard	Riferimento al campo SAML di Application Integration Wizard
Entra	Crea la tua applicazione	Quickstart: crea e assegna un account utente	Abilita il Single Sign-On per un'applicazione aziendale	Verifica della firma delle richieste SAML	Configurare la crittografia del token SAML Microsoft Entra	Protocollo SAML Single Sign-Out
Ping	Aggiungi un'applicazione SAML	Utenti	Abilitazione dell'SSO avviato da IdP	Configurazione della richiesta di autenticazione per l'accesso a	PingOne For Enterprise supporta la crittografia?	Disconnessione singola SAML 2.0

IdP	Configurazione dell'applicazione SAML	Gestione degli utenti	Autenticazione avviata da IDP	Richiedi la firma	Crittografia delle asserzioni	Disconnessione singola
				Enterprise PingOne		
Un accesso	Connettore personalizzato SAML (avanzato) (4266907)	Aggiungi utenti a Manualmente OneLogin	Connettore personalizzato SAML (avanzato) (4266907)	Connettore personalizzato SAML (avanzato) (4266907)	Connettore personalizzato SAML (avanzato) (4266907)	Connettore personalizzato SAML (avanzato) (4266907)
IAM Identity Center	Configura la tua applicazione SAML 2.0	Configura la tua applicazione SAML 2.0	Configura la tua applicazione SAML 2.0	N/D	N/D	N/D

Configura il tipo di autenticazione IAM Identity Center

Per il tipo IAM Identity Center (avanzato), federerai IAM Identity Center con il tuo portale. Seleziona questa opzione solo se ti riguarda quanto segue:

- Il tuo IAM Identity Center è configurato nello stesso Account AWS portale web. Regione AWS
- Se utilizzi AWS Organizations, stai utilizzando un account di gestione.

Prima di creare un portale web con il tipo di autenticazione IAM Identity Center, devi configurare IAM Identity Center come provider autonomo. Per ulteriori informazioni, consulta Introduzione alle attività comuni in IAM Identity Center. In alternativa, puoi connettere il tuo IdP SAML 2.0 a IAM Identity Center. Per ulteriori informazioni, consulta Connect to a un provider di identità esterno. Altrimenti, non avrai utenti o gruppi da assegnare al tuo portale web.

Se utilizzi già IAM Identity Center, puoi scegliere IAM Identity Center come tipo di provider e seguire i passaggi seguenti per aggiungere, visualizzare o rimuovere utenti o gruppi dal tuo portale web.

> **Note**
>
> Per utilizzare questo tipo di autenticazione, il tuo IAM Identity Center deve trovarsi nello stesso Account AWS portale WorkSpaces Web. Regione AWS Se il tuo IAM Identity Center si trova in un altro Account AWS o Regione AWS, segui le istruzioni per il tipo di autenticazione Standard. Per ulteriori informazioni, consulta the section called “Configura il tipo di autenticazione standard”.
> Se lo utilizzi AWS Organizations, puoi creare portali WorkSpaces Web integrati con IAM Identity Center solo utilizzando un account di gestione.

Per creare un portale web con IAM Identity Center

1. Durante la creazione del portale nella Fase 4: Configura il provider di identità, scegli AWS IAM Identity Center.
2. Scegli Continua con IAM Identity Center.
3. Nella pagina Assegna utenti e gruppi, scegli la scheda Utenti e/o gruppi.
4. Seleziona la casella accanto agli utenti o ai gruppi che desideri aggiungere al portale.
5. Dopo aver creato il portale, gli utenti che hai associato possono accedere al WorkSpaces Web con il nome utente e la password di IAM Identity Center.

Per gestire un portale Web con IAM Identity Center

1. Dopo aver creato il portale, questo viene elencato nella console IAM Identity Center come applicazione configurata.
2. Per accedere alla configurazione di questa applicazione, scegli Applicazioni nella barra laterale e cerca un'applicazione configurata con un nome che corrisponda al nome visualizzato del tuo portale web.

   > **Note**
   >
   > Se non hai inserito un nome visualizzato, viene visualizzato il GUID del portale. Il GUID è l'ID con il prefisso dell'URL dell'endpoint del portale web.

Per aggiungere altri utenti e gruppi a un portale web esistente

1. Apri la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegliete WorkSpaces Web, Portali Web, scegliete il vostro portale Web, quindi scegliete Modifica.
3. Scegli le Impostazioni del gestore dell'identità digitale e Assegna utenti e gruppi aggiuntivi. Da qui, puoi aggiungere utenti e gruppi al tuo portale Web.

> **Note**
>
> Non puoi aggiungere utenti o gruppi dalla console IAM Identity Center. È necessario eseguire questa operazione dalla pagina di modifica del portale WorkSpaces Web.

Per visualizzare o rimuovere utenti e gruppi dal portale web

- È possibile visualizzare o rimuovere l'accesso degli utenti a questa applicazione utilizzando le azioni disponibili nella tabella Utenti assegnati. Per ulteriori informazioni, consulta Gestire l'accesso alle applicazioni.

> **Note**
>
> Non è possibile visualizzare o rimuovere utenti e gruppi dalla pagina di modifica del WorkSpaces portale Web. È necessario eseguire questa operazione dalla pagina di modifica della console IAM Identity Center.

Modificare il tipo di provider di identità

Segui questi passaggi per modificare il tipo di autenticazione del portale in qualsiasi momento:

- Per passare da IAM Identity Center a Standard, segui i passaggi riportati inthe section called “Configura il tipo di autenticazione standard”.
- Per passare da Standard a IAM Identity Center, segui i passaggi riportati inthe section called “Configura il tipo di autenticazione IAM Identity Center”.

L'implementazione delle modifiche al tipo di provider di identità può richiedere fino a 15 minuti e non interromperanno automaticamente le sessioni in corso.

È possibile visualizzare le modifiche al tipo di provider di identità apportate al portale AWS CloudTrail controllando gli eventi. `UpdatePortal` Il tipo è visibile nei payload di richiesta e risposta dell'evento.

Revisione e avvio

1. Nella pagina Passo 5: Rivedi e avvia, controlla le impostazioni che hai selezionato per il tuo portale web. Puoi scegliere Modifica per modificare le impostazioni all'interno di una determinata sezione. È inoltre possibile modificare queste impostazioni in un secondo momento dalla scheda Portali Web della console.
2. Al termine, scegli Avvia portale web.
3. Per visualizzare lo stato del tuo portale web, scegli Portali Web, scegli il tuo portale e quindi scegli Visualizza dettagli.

   Un portale Web ha uno dei seguenti stati:

   - Incompleto: nella configurazione del portale web mancano le impostazioni richieste del gestore dell'identità digitale.
   - In sospeso: il portale web sta applicando modifiche alle sue impostazioni.
   - Attivo: il portale web è pronto e disponibile per l'uso.
4. Attendi fino a 15 minuti prima che il portale diventi Attivo.

Fase 2: verificare il portale web

Dopo aver creato un portale Web, è possibile accedere all'endpoint WorkSpaces Web per sfogliare i siti Web collegati come farebbe un utente finale.

Se hai già completato questi passaggi in the section called “Configurazione dei gestore dell'identità digitale”, puoi ignorare questa sezione e andare su Fase 3: Distribuisci il tuo portale web.

1. Aprire la console WorkSpaces Web all'indirizzo https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Web, Portali Web, scegli il tuo portale Web, quindi scegli Visualizza dettagli
3. In Endpoint del portale web, vai all'URL specificato per il tuo portale. L'endpoint del portale Web è il punto di accesso da cui gli utenti avvieranno il portale Web dopo aver effettuato l'accesso con

il gestore dell'identità digitale configurato per il portale. È disponibile pubblicamente su Internet e può essere integrato nella rete.

4. Nella pagina di accesso WorkSpaces Web, scegli Accedi, SAML e inserisci le tue credenziali SAML.
5. Quando viene visualizzata la pagina La sessione è in preparazione, la sessione WorkSpaces Web viene avviata. Non chiudere o uscire da questa pagina.
6. Il browser Web si avvia, visualizzando l'URL di avvio e qualsiasi altro comportamento aggiuntivo configurato tramite le impostazioni della policy del browser.
7. Ora puoi navigare verso i siti Web collegati scegliendo i link o inserendo gli URL nella barra degli indirizzi.

Fase 3: Distribuisci il tuo portale web

Quando si è pronti per consentire agli utenti di iniziare a utilizzare il WorkSpaces Web, è possibile scegliere tra le seguenti opzioni per distribuire il portale:

- Aggiungi il tuo portale al tuo gateway applicativo SAML per consentire agli utenti di avviare una sessione direttamente dal proprio IdP. Ad esempio, consulta Creare un'integrazione con l'app Bookmark.
- Aggiungi l'URL del portale a un sito web di tua proprietà e utilizza un reindirizzamento del browser per indirizzare gli utenti al portale web.
- Invia l'URL del portale via e-mail agli utenti o invialo a un dispositivo che gestisci come home page del browser o come segnalibro.

Passaggi successivi

Dopo aver creato il primo portale web, puoi visualizzare i dettagli, modificare i dettagli o eliminare il portale web in qualsiasi momento. Per ulteriori informazioni, consulta Gestione del portale web.

Account AWS È possibile creare un portale Web in ogni Regione AWS luogo in cui WorkSpaces Web è disponibile. Ogni portale Web può supportare fino a 25 connessioni utente in qualsiasi momento. Per aumentare il numero di portali che è possibile creare in una regione o per supportare più sessioni simultanee per un portale, vedi the section called “Richiedi un aumento della quota di servizio.”.

Gestione del portale web

Dopo aver configurato il portale web, è possibile visualizzarne o modificarne i dettagli, nonché eliminare il portale se non è più necessario.

Argomenti

Visualizzazione dei dettagli del portale web

Visualizzazione dei dettagli del portale web

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Web, Portali Web, scegli il tuo portale Web, quindi scegli Visualizza dettagli.

Modifica di un portale web

Modifica di un portale web

1. Apri la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.

2. Scegliete WorkSpaces Web, Portali Web, scegliete il vostro portale Web, quindi scegliete Modifica.

> **Note**
>
> Le modifiche alle impostazioni di rete o alle impostazioni di timeout interrompono immediatamente tutte le sessioni attive del portale. Gli utenti sono disconnessi e devono riconnettersi per iniziare una nuova sessione. Le modifiche alle Autorizzazioni per gli appunti, alle Autorizzazioni per il trasferimento di file o alla Stampa su dispositivo locale si applicano a partire dalla prima nuova sessione. Le sessioni attualmente attive non sono disconnesse. Gli utenti connessi alle sessioni attive non sono interessati dalle modifiche finché non si disconnettono e si connettono a una nuova sessione.

Eliminazione di un portale web

Eliminazione di un portale web

1. Apri la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegliete WorkSpaces Web, Portali Web, scegliete il vostro portale Web, quindi scegliete Elimina.

Richiedi un aumento della quota di servizio.

Quando crei il tuo AWS account, impostiamo automaticamente le quote di servizio predefinite (note anche come limiti) per l'utilizzo delle risorse con AWS i Servizi. WorkSpaces Web imposta le quote su due tipi di risorse: portali web (per regione) e numero massimo di sessioni simultanee (per portale web). WorkSpaces Web ha attualmente i seguenti limiti di quote di servizio:

Quote predefinite all'interno e per account Regione AWS	Valore
Portali Web	1
Numero massimo di sessioni simultanee	25

Un portale web è la risorsa fondamentale all'interno WorkSpaces del Web. È un'associazione tra il tuo gestore dell'identità digitale SAML 2.0 e la tua connessione di rete a Internet e ai tuoi contenuti. È possibile creare un portale Web Regione AWS ovunque sia disponibile il WorkSpaces Web. Consulta la Tabella delle Regioni per la disponibilità attuale.

Il numero massimo di sessioni simultanee è il numero massimo di utenti che saranno connessi contemporaneamente a un determinato portale web. Se il limite della quota di servizio per il numero massimo di sessioni simultanee non è impostato in modo appropriato, gli utenti potrebbero scoprire che la loro sessione non è disponibile quando WorkSpaces accedono al Web. È inoltre necessario assicurarsi che il VPC e le sottoreti dispongano di spazio IP sufficiente per supportare il numero massimo di sessioni simultanee, altrimenti gli utenti potrebbero non essere in grado di connettersi a una sessione.

Ad esempio, un cliente ha due portali Web negli Stati Uniti orientali (Virginia settentrionale) e 125 utenti. Il primo portale web (portale A) ha 25 utenti e non richiede un aumento della quota di servizio. Il secondo portale web (portale B) deve essere disponibile per un massimo di 100 utenti. Questi utenti sono distribuiti su due turni e i loro orari di lavoro non si sovrappongono. Pertanto, il cliente dovrebbe richiedere un aumento della quota di servizio per il Portale B fino a una sessione simultanea massima di 50 utenti.

Puoi richiedere un aumento di uno di questi limiti di quota di servizio. Per ulteriori informazioni, consulta la sezione Richiesta di un aumento di quota.

Richiedi un aumento della quota di servizio.

1. Apri la dashboard del Supporto AWS.
2. Seleziona Aumento limiti del servizio.

> **Important**
>
> WorkSpaces Le quote dei servizi Web influiscono su una regione alla volta. Devi richiedere aumenti delle quote di servizio in ogni regione AWS in cui hai bisogno di più risorse. Per ulteriori informazioni, consulta Endpoint del servizio AWS.

3. Nella sezione Descrizione del caso d'uso, inserisci le seguenti informazioni:

   - Se richiedi un aumento del numero di portali Web, specifica questo tipo di risorsa e includi l'ID del tuo account AWS, la regione in cui desideri l’aumento e il nuovo valore limite.

- Se richiedi un aumento del numero massimo di sessioni simultanee, specifica questo tipo di risorsa e includi l'ID del tuo account AWS, la regione in cui desideri l'aumento, l'ARN del portale web e il nuovo valore limite.

4. (Facoltativo) Per richiedere più aumenti della quota di servizio contemporaneamente, completa una richiesta di aumento della quota nella sezione Richieste, quindi scegli Aggiungi un'altra richiesta.

Controlla l'intervallo per la riautenticazione di un token IdP SAML

Quando un utente visita un portale WorkSpaces Web, può accedere per avviare una sessione di streaming. Ogni sessione inizia dalla pagina iniziale, a meno che non abbia effettuato l'accesso meno di 5 minuti prima. Il portale verifica la presenza di token di identity provider (IdP) per determinare se richiedere all'utente le credenziali all'avvio di una sessione. Un utente senza un token IdP valido deve inserire un nome utente, una password e (facoltativamente) l'autenticazione a più fattori (MFA) per avviare una sessione di streaming. Se un utente ha già generato un token SAML IdP accedendo al proprio IdP o a un'app protetta dallo stesso IdP, non gli verranno richieste le credenziali di accesso.

Se un utente dispone di un token SAML IdP valido, può WorkSpaces accedere al Web. Controlla l'intervallo per la riautenticazione di un token IdP SAML

Controlla l'intervallo per la riautenticazione di un token IdP SAML

1. Imposta la durata del timeout dell'IdP con il tuo provider IdP SAML. Ti consigliamo di configurare la durata del timeout IdP con il tempo più breve necessario a un utente per completare le proprie attività.

   - Per ulteriori informazioni su Okta, consulta Applicare una durata di sessione limitata per tutte le policy.
   - Per ulteriori informazioni su Azure AD, vedere Configurazione dei controlli delle sessioni di autenticazione.
   - Per ulteriori informazioni su Ping, consulta Sessioni.
   - Per ulteriori informazioni su AWS IAM Identity Center, consulta Impostare la durata della sessione.

2. Imposta i valori di inattività e di timeout di inattività del tuo portale WorkSpaces Web. Questi valori controllano la quantità di tempo tra l'ultima interazione di un utente e il termine di una sessione WorkSpaces Web per inattività. Al termine di una sessione, un utente perderà lo stato della sessione (comprese le schede aperte, i contenuti Web non salvati e la cronologia) e tornerà

a uno stato nuovo all'inizio della sessione successiva. Per ulteriori informazioni, consulta la fase 5 in the section called “Fase 1: creazione di un portale Web”.

> **Note**
>
> Se la sessione di un utente scade ma l'utente ha ancora un token SAML IdP valido, non è necessario inserire il nome utente e la password per iniziare una WorkSpaces nuova sessione Web. Per controllare come i token vengono riautenticati, segui le guide nel passaggio precedente.

Configurazione della registrazione degli accessi utente

È possibile configurare la registrazione degli accessi degli utenti per avere i log dei seguenti eventi degli utenti:

- Inizio sessione: segna l'inizio di una sessione WorkSpaces Web.
- Fine sessione: segna la fine di una sessione WorkSpaces Web.
- Navigazione URL: registra l'URL caricato da un utente.

> **Note**
>
> I log di navigazione degli URL vengono registrati dalla cronologia del browser. Gli URL non registrati nella cronologia del browser (visitati in modalità di navigazione in incognito o eliminati dalla cronologia del browser) non vengono registrati nei log. Spetta ai clienti decidere se disattivare la modalità di navigazione in incognito o l'eliminazione della cronologia in base alla policy del browser.

Inoltre, per ogni evento sono incluse le seguenti informazioni:

- Event time (Ora evento)
- Username
- ARN portale web

I clienti hanno la responsabilità di comprendere i potenziali problemi legali derivanti dall'uso del WorkSpaces Web e di garantire che l'uso del WorkSpaces Web sia conforme a tutte le leggi e i

regolamenti applicabili. Queste includono le leggi che regolano la capacità del datore di lavoro di monitorare l'uso del WorkSpaces Web da parte di un dipendente, comprese le attività eseguite all'interno dell'applicazione.

L'attivazione dei log di accesso degli utenti sul tuo portale WorkSpaces Web potrebbe comportare addebiti da parte di Amazon Kinesis Data Streams. Per i dettagli sui prezzi, consulta Prezzi del flusso di dati Amazon Kinesis.

Per attivare la registrazione degli accessi degli utenti nella console WorkSpaces Web, in Registrazione degli accessi degli utenti, seleziona l'ID Kinesis Stream che desideri utilizzare per ricevere i dati. I dati registrati verranno inviati direttamente a quel flusso.

Per ulteriori informazioni su come creare un flusso di dati Amazon Kinesisi, consulta Che cos'è il flusso di dati Amazon Kinesis?

> **Note**
>
> Per ricevere i log dal WorkSpaces Web, è necessario disporre di un Amazon Kinesis Data Stream che inizi con amazon-workspaces-web "-*». Il flusso di dati di Amazon Kinesis deve avere la crittografia lato server disattivata o deve essere utilizzata Chiavi gestite da AWS per la crittografia lato server.
> Per ulteriori informazioni sull'impostazione della crittografia lato server in Amazon Kinesis, consulta Cosa devo fare per iniziare a usare la crittografia lato server?.

Registri dei log di esempio

Di seguito è riportato un esempio di ogni evento disponibile, tra cui Validation,, e. StartSessionVisitPageEndSession

I seguenti campi sono sempre inclusi per ogni evento:

- timestamp è incluso come ora del momento specifico in millisecondi.
- eventType è incluso come stringa.
- details è incluso come altro oggetto json.
- portalArn e userName sono inclusi per ogni evento ad eccezione di Validation.

```
{
```

```
  "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"
}
```

Imposta o modifica la policy del browser

Con WorkSpaces Web, puoi impostare una politica del browser personalizzata utilizzando le politiche di Chrome disponibili per l'ultima versione stabile. Esistono più di 300 policy che puoi applicare a un

portale web. Per ulteriori informazioni, consulta the section called “Imposta una policy del browser personalizzata (esempio)” e l'elenco dei criteri di Chrome Enterprise.

Utilizzando la visualizzazione della console per creare un portale web, è possibile applicare le seguenti policy:

- `StartURL`
- Segnalibri e cartelle di segnalibri
- Attivazione e disattivazione della navigazione privata
- Eliminazione della cronologia
- Filtraggio degli URL con `AllowURL` e `BlockURL`

Per ulteriori informazioni sull'utilizzo delle policy di visualizzazione della console, consulta Guida introduttiva ad Amazon WorkSpaces Web.

WorkSpaces Web applica una configurazione di base dei criteri del browser a tutti i portali insieme a tutte le politiche specificate. Puoi modificare alcune di queste policy con il tuo file JSON personalizzato. Per ulteriori informazioni, consulta the section called “Modifica la policy di base del browser”.

Argomenti

- Imposta una policy del browser personalizzata (esempio)
- Modifica la policy di base del browser

Imposta una policy del browser personalizzata (esempio)

Puoi impostare qualsiasi policy Chrome supportata per Linux caricando un file JSON. Per ulteriori informazioni sulle policy di Chrome, consulta l'elenco delle policy di Chrome Enterprise e seleziona la piattaforma Linux. Quindi, cerca e rivedi le policy per la versione stabile più recente.

Nell'esempio seguente, si crea un portale web con i seguenti controlli delle policy:

- Imposta i segnalibri
- Configura pagine di avvio predefinite
- Impedisci all'utente di installare altre estensioni
- Impedisci all'utente di eliminare la cronologia

- Impedisci all'utente di accedere alla modalità di navigazione in incognito
- Preinstalla l'estensione del plug-in Okta per tutte le sessioni.

Argomenti

Fase 1: creazione di un portale web

Per caricare il file JSON delle policy di Chrome, devi creare un WorkSpaces portale Web. Per ulteriori informazioni, consulta the section called “Fase 1: creazione di un portale Web”.

Fase 2: raccolta delle policy

Cerca e individua le policy che desideri nella sezione Chrome Policy. Puoi quindi utilizzare le policy per creare un file JSON nel passaggio successivo.

1. Vai all'elenco delle policy di Chrome Enterprise.
2. Scegli la piattaforma Linux, quindi scegli la versione di Chrome più recente.
3. Cerca le policy che desideri impostare. Per questo esempio, cerca le estensioni per trovare le policy per la gestione. Ogni policy include una descrizione, un nome di preferenza Linux e un valore di esempio.
4. Dai risultati della ricerca, ci sono 3 policy che soddisfano i requisiti aziendali se utilizzate insieme:
   - ExtensionSettings: installa un'estensione all'avvio del browser.
   - ExtensionInstallBlocklist: impedisce l'installazione di estensioni specifiche.
   - ExtensionInstallAllowlist— Consente l'installazione di determinate estensioni.
5. Le policy aggiuntive soddisfano i requisiti rimanenti;
   - ManagedBookmarks— Aggiunge segnalibri alle pagine Web.
   - RestoreOnStartupURL: configura quali pagine Web vengono aperte ogni volta che viene aperta una nuova finestra del browser.

- AllowDeletingBrowserHistory— Configura se gli utenti possono eliminare la cronologia di navigazione.
- IncognitoModeAvailability— Configura se gli utenti possono accedere alla modalità di navigazione in incognito.

Passaggio 3: creazione di un file di policy JSON personalizzato

Crea un file JSON utilizzando un editor di testo, un modello e le policy trovate nel passaggio precedente.

1. Aprire un editor di testo.
2. Copia il seguente modello e incollalo in un editor di testo:

```
{
  "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
        }
    }
}
```

Fase 4: aggiunta delle policy al modello

Aggiungi le tue policy personalizzate al modello per ogni requisito aziendale.

1. Configura gli URL dei segnalibri.

a. Sotto la chiave `value`, aggiungi coppie di chiavi `name` e `url` per ogni segnalibro che desideri aggiungere.

b. Imposta `bookmark-url-1` su `https://www.amazon.com`.

c. Imposta `bookmark-url-2` su `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. Impostazione degli URL di avvio. Questa policy consente agli amministratori di impostare le pagine Web visualizzate quando un utente apre una nuova finestra del browser.

   a. Imposta `RestoreOnStartup` su `4`. Questo imposta l'azione `RestoreOnStartup` per aprire un elenco di URL. È possibile anche utilizzare altre operazioni negli URL di avvio. Per ulteriori informazioni, consulta l'elenco delle policy di Chrome Enterprise.

   b. Imposta `RestoreOnStartupURLs` su https://www.aboutamazon.com/news.

```
    "RestoreOnStartup":
       {
           "value": 4
       },
   "RestoreOnStartupURLs":
       {
           "value":
           [
```

```
            "https://www.aboutamazon.com/news"
        ]
    },
```

3. Per impedire all'utente di eliminare la cronologia del browser, imposta `AllowDeletingBrowserHistory` su `false`.

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

4. Per disattivare l'accesso alla modalità di navigazione in incognito per i tuoi utenti, imposta `IncognitoModeAvailability` su `1`.

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

5. Imposta e applica il plug-in Okta con le seguenti policy:

   - `ExtensionSettings`: installa un'estensione all'avvio del browser. Il valore dell'estensione è disponibile nella pagina di aiuto del plug-in Okta.
   - `ExtensionInstallBlocklist`: impedisce l'installazione di estensioni specifiche. Utilizza un valore * per impedire tutte le estensioni per impostazione predefinita. Gli amministratori possono controllare quali estensioni consentire su `ExtensionInstallAllowlist`.
   - `ExtensionInstallAllowlist` consente di installare determinate estensioni. Poiché `ExtensionInstallBlocklist` è impostato su *, aggiungi qui il valore del plug-in Okta per consentirlo.

   Di seguito viene mostrato un esempio di policy per attivare il plug-in Okta:

```
    "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"
            }
        }
```

Passaggio 5: carica il file JSON della policy sul tuo portale web

1. Aprire la console WorkSpaces Web all'indirizzo. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. Scegli WorkSpaces Web, quindi scegli Portali Web.
3. Scegli il tuo portale web, quindi scegli Modifica.
4. Scegli Impostazioni delle policy, quindi scegli Caricamento file JSON.
5. Seleziona Scegli file. Naviga verso, seleziona e carica il tuo file JSON.
6. Selezionare Salva.

Modifica la policy di base del browser

Per fornire il servizio, WorkSpaces Web applica una policy di base relativa ai browser a tutti i portali. Questa policy di base viene applicata in aggiunta a quelle specificate nella visualizzazione della console o nel caricamento JSON. Di seguito è riportato l'elenco delle policy applicate dal servizio in formato JSON:

```
{
    "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",
            ]
        }
    }
}
```

I clienti non possono apportare modifiche alle seguenti policy:

- `DefaultDownloadDirectory`: questa policy non può essere modificata. Il servizio sovrascrive qualsiasi modifica a questa policy.
- `DownloadDirectory`: questa policy non può essere modificata. Il servizio sovrascrive qualsiasi modifica a questa policy.

I clienti possono aggiornare le seguenti policy per il proprio portale web:

- `DownloadRestrictions`: l'impostazione predefinita è quella di impostare su `1` per evitare i download identificati come dannosi da Chrome Safe Browsing. Per ulteriori informazioni, consulta Impedire agli utenti di scaricare file dannosi. Puoi impostare il valore da `0` a `4`.
- Le policy `URLAllowlist` e `URLBlocklist` possono essere estese utilizzando la funzionalità di filtraggio degli URL di visualizzazione della console o il caricamento JSON. Tuttavia, gli URL di base non possono essere sovrascritti. Queste policy non sono visibili in un file JSON scaricato

dal tuo portale web. Tuttavia, se visiti “chrome://policy” durante una sessione, il browser remoto visualizza le policy applicate.

Configurare l'Input Method Editor (IME)

Un Input Method Editor (IME) è un'utilità che fornisce all'utente finale la possibilità di inserire testo in lingue che utilizzano un layout di tastiera diverso da una tastiera QWERTY. Gli IME consentono agli utenti di inserire testo in lingue con set di lingue più ampi e complessi, come giapponese, cinese e coreano. WorkSpaces Le sessioni Web includono il supporto IME per impostazione predefinita. Gli utenti possono selezionare lingue alternative dalla barra degli strumenti IME nella sessione o utilizzando le scorciatoie da tastiera.

Le seguenti lingue sono attualmente supportate dall'IME di WorkSpaces Web:

- Italiano
- Cinese semplificato (Pinyin)
- Cinese tradizionale (Bopomofo)
- Giapponese
- Coreano

Per selezionare una lingua dalla barra degli strumenti IME, procedi nel seguente modo:

1. Seleziona il menu a discesa del selettore della lingua situato sul lato destro della barra nera del pannello superiore. Per impostazione predefinita, il selettore mostrerà en, per l'inglese.
2. Dal menu a discesa scegli la lingua desiderata.
3. Nel sottomenu che appare dopo aver scelto una lingua, scegli dettagli aggiuntivi sulla lingua.

Per selezionare una lingua utilizzando le scorciatoie da tastiera, procedi come segue:

- Tutti gli IME
  - Per spostare l'IME in avanti (o passare al layout di tastiera destro), premi Shift+Control+Left Alt.
- Giapponese
  - Per scegliere Hiragana, premi F6.
  - Per scegliere Katakana, premi F7.
  - Per scegliere caratteri latini, premi F10.

  - Per scegliere caratteri latini grandi, premi F9.
  - Per scegliere Direct Input, premete ALT +, ALT+@, Zenkaku Hankaku.
- Coreano
  - Per scegliere Hangul, premi Shift+Space.
  - Per scegliere Hanja, premi F9.

Per rimuovere la barra degli strumenti e il menu IME o per disattivare la tastiera su schermo dalle sessioni WorkSpaces Web, contatta. AWS Support

Configura la localizzazione durante la sessione

Quando un utente avvia una sessione, WorkSpaces Web rileva le impostazioni della lingua e del fuso orario del browser locale dell'utente e le applica alla sessione. Ciò influisce sulla lingua di visualizzazione durante la sessione e aiuta a garantire che l'ora visualizzata corrisponda all'ora corrente nella posizione dell'utente.

L'elenco seguente mostra i codici di lingua attualmente supportati dal WorkSpaces Web. Se il browser locale dell'utente è impostato per utilizzare un codice di lingua non supportato, per impostazione predefinita la sessione è l'inglese (en-US).

- Tedesco
  - de — Tedesco
  - de-AT — Tedesco (Austria)
  - de-DE — Tedesco (Germania)
  - de-CH — Tedesco (Svizzera)
  - de-LI — Tedesco (Liechtenstein)
- Italiano
  - Inglese (en)
  - Inglese (Australia) (en-AU)
  - Inglese (Canada) (en-CA)
  - Inglese (India) (en-IN)
  - Inglese, Nuova Zelanda (en-NZ)
  - Inglese (Africa meridionale) (en-ZA)

  - Inglese (Regno Unito) (en-GB)
  - Inglese (Stati Uniti) (en-US)
- Spagnolo
  - Spagnolo (es)
  - Spagnolo (Argentina) (es-AR)
  - Spagnolo (Cile) (es-CL)
  - Spagnolo (Colombia) (es-CO)
  - Spagnolo (Costa Rica) (es-CR)
  - Spagnolo (Honduras) (es-HN)
  - Spagnolo (America Latina) (es-419)
  - Spagnolo (Messico) (es-MX)
  - Spagnolo (Perù) (es-PE)
  - Spagnolo (Spagna) (es-ES)
  - Spagnolo (Stati Uniti) (es-US)
  - Spagnolo (Uruguay) (es-UY)
  - Spagnolo (Venezuela) (es-VE)
- Francese
  - Francese (fr)
  - Francese (Canada) (fr-CA)
  - Francese (Francia) (fr-FR)
  - Francese (Svizzera) (fr-CH)
- Indonesiano
  - Indonesiano (id)
  - Indonesiano (Indonesia) (id-ID)
- Italiano
  - Italiano (it)
  - Italiano (Italia) (it-IT)
  - Italiano (Svizzera) (it-CH)
- Giapponese
  - Giapponese (ja)

  - Giapponese (Giappone) (ja-JP)
- Coreano
  - Coreano (ko)
  - Coreano (Corea) (ko-KR)
- Portoghese
  - Portoghese (pt)
  - Portoghese (Brasile) (pt-BR)
  - Portoghese (Portogallo) (pt-PT)
- Cinese
  - Cinese (zh)
  - Cinese (Cina) (zh-CN)
  - Cinese (Hong Kong) (zh-HK)
  - Cinese (Taiwan) (zh-TW)

La lingua della sessione è determinata nel seguente ordine di priorità:

1. La ForcedLanguagespolitica nelle impostazioni del browser del portale web. Per ulteriori informazioni, vedere ForcedLanguages.
2. L'impostazione della lingua locale del browser dell'utente finale.
3. Il valore predefinito è l'inglese (en-US).

Il fuso orario è determinato dalle impostazioni del fuso orario locale specificate nel browser dell'utente finale. Se l'impostazione del fuso orario non è valida, viene utilizzato UTC.

I seguenti componenti della localizzazione del supporto WorkSpaces Web:

- WorkSpaces Pagina di accesso Web
- WorkSpaces Messaggi di stato del portale Web (inclusi messaggi ed errori di caricamento)
- Browser Chrome
- Menu contestuale del sistema e finestra Salva con nome

Per configurare le impostazioni del browser locale di un utente, effettua una delle seguenti operazioni:

- In Chrome, scegli Impostazioni, scegli Lingue, quindi ordina le lingue in base alle preferenze.
- In Firefox, scegli Impostazioni, Generali, Lingua e seleziona la lingua dal menu a discesa.
- In Edge, scegli Impostazioni, scegli Lingue, quindi ordina le lingue in base alle preferenze.

Configura i controlli di accesso IP (opzionale)

WorkSpaces Il Web consente di controllare da quali indirizzi IP è possibile accedere al portale Web. Utilizzando le impostazioni di accesso degli indirizzi IP, è possibile definire e gestire gruppi di indirizzi IP affidabili e consentire agli utenti di accedere al proprio portale solo se sono connessi a una rete affidabile.

Per impostazione predefinita, WorkSpaces Web consente agli utenti di accedere al proprio portale Web da qualsiasi luogo. Un gruppo di controllo degli accessi IP funge da firewall virtuale che filtra l'indirizzo IP che un utente può utilizzare per connettersi al portale web. Se associate al portale web, le impostazioni di accesso IP rileveranno l'IP dell'utente prima dell'autenticazione per determinare se è idoneo alla connessione. Una volta connesso, WorkSpaces Web monitora continuamente l'indirizzo IP di un utente per garantire che rimanga connesso da una rete affidabile. Se l'IP di un utente cambia, WorkSpaces Web rileverà e interromperà la sessione.

Per specificare gli intervalli di indirizzi CIDR, aggiungi regole al gruppo di controllo degli accessi IP, quindi associa il gruppo al portale web. È possibile associare ogni impostazione di accesso IP a uno o più portali Web. Per specificare gli indirizzi IP pubblici e gli intervalli di indirizzi IP per le reti attendibili, aggiungi regole ai tuoi gruppi di controllo degli accessi IP. Se gli utenti accedono al proprio portale web tramite un gateway NAT o una VPN, è necessario creare regole che consentano il traffico proveniente dagli indirizzi IP pubblici per il gateway NAT o la VPN.

> **Note**
>
> I clienti hanno la responsabilità di comprendere i potenziali problemi legali derivanti dall'uso del WorkSpaces Web e devono assicurarsi che l'uso del WorkSpaces Web sia conforme a tutte le leggi e i regolamenti applicabili. Ciò include le leggi che regolano la capacità del datore di lavoro di monitorare l'uso del WorkSpaces Web da parte di un dipendente, comprese le attività eseguite all'interno dell'applicazione.

Creazione di un gruppo di controllo degli accessi IP

Per creare un gruppo di controllo degli accessi IP, seguire i seguenti passaggi.

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione, scegli Controlli degli accessi IP.
3. Scegli Creazione di un gruppo di controllo degli accessi IP.
4. Nella finestra di dialogo Crea gruppo di controllo degli accessi IP, immetti un nome (obbligatorio) e una descrizione (opzionale) per il gruppo.
5. Immetti l'indirizzo IP o l'intervallo IP CIDR che verrà associato all'origine e una descrizione (opzionale).
6. In Tag, scegli se etichettare una coppia di valori chiave per ogni gruppo di controllo degli accessi IP.
7. Una volta aggiunti tutti i tag e le regole, seleziona Salva.

Associa un'impostazione di accesso IP a un portale web

Per associare un gruppo di controllo degli accessi IP a un portale web esistente, procedi nel seguente modo.

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione scegli Portali web.
3. Seleziona il portale web e scegli Modifica.
4. In Gruppo di controllo degli accessi IP, seleziona i gruppi di controllo degli accessi IP per il portale web.
5. Selezionare Salva.

Per associare un gruppo di controllo degli accessi IP quando crei un nuovo portale web, procedi nel seguente modo.

1. Completa i passaggi da 1 a 4 in the section called “Per configurare le impostazioni del portale” per accedere a Controllo degli accessi IP (opzionale).

2. Scegli Creazione di controlli degli accessi IP.
3. Nella finestra di dialogo Crea gruppo di IP, immetti un nome (obbligatorio) e una descrizione (opzionale) per il gruppo.
4. Immetti l'indirizzo IP o l'intervallo IP CIDR che verrà associato all'origine e una descrizione (opzionale).
5. In Tag, scegli se etichettare una coppia di valori chiave per ogni gruppo di controllo degli accessi IP.
6. Quando hai finito di aggiungere regole e tag, scegli Crea controllo di accesso IP.
7. Il tuo gruppo di controllo degli accessi IP verrà associato a questo portale web una volta avviato.

Modifica un gruppo di controllo degli accessi IP

È possibile eliminare una regola da un'impostazione di controllo degli accessi IP in qualsiasi momento. Se si rimuove una regola utilizzata per consentire una connessione a un portale web, tutti gli utenti con una sessione corrente verranno disconnessi dal portale web.

Per creare un gruppo di controllo degli accessi IP, seguire i seguenti passaggi.

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione, scegli Controlli degli accessi IP.
3. Seleziona il gruppo e scegli Modifica.
4. Modifica le regole esistenti Source e Description (opzionale) o aggiungi regole aggiuntive.
5. In Tag, scegli se etichettare una coppia di valori chiave per ogni gruppo di controllo degli accessi IP.
6. Una volta aggiunti tutti i tag e le regole, seleziona Salva.
7. Se hai aggiornato un'impostazione di accesso IP esistente, attendi fino a 15 minuti affinché la regola nuova o modificata abbia effetto.

Elimina un gruppo di controllo degli accessi IP

È possibile eliminare una regola da un gruppo di controllo degli accessi IP in qualsiasi momento. Se si rimuove una regola utilizzata per consentire una connessione a un portale web, tutti gli utenti con una sessione corrente verranno disconnessi dal portale web.

Per eliminare un gruppo di controllo degli accessi IP, seguire i seguenti passaggi.

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione, scegli Gruppo di controllo degli accessi IP.
3. Seleziona il gruppo e scegli Elimina.

Abilita l’estensione per Single Sign-On (opzionale)

Puoi abilitare un'estensione per gli utenti finali per avere una migliore esperienza di accesso al portale. Ad esempio, se utilizzi Okta come gestore dell'identità digitale SAML 2.0 (IdP) del tuo portale e lo utilizzi anche come IdP per i siti web che desideri che gli utenti visitino durante una sessione, puoi passare il cookie di accesso Okta alla sessione con l'estensione. Successivamente, quando gli utenti visitano un sito web che richiede il cookie del dominio Okta, possono accedere al sito web senza dover effettuare l'accesso durante la sessione.

L'estensione è supportata nei browser Chrome e Firefox. L'estensione consente la sincronizzazione dei cookie per i domini consentiti dall'accesso degli utenti alla sessione. L'estensione non richiede l'accesso dell'utente e funziona dietro le quinte per abilitare la sincronizzazione dei cookie senza richiedere all'utente di intraprendere alcuna azione dopo l'installazione. Nessun dato viene memorizzato dall'estensione.

Gli utenti possono aggiungere l'estensione al proprio browser Chrome dal Chrome Web Store o al FireFox browser da Add-ons for FireFox.

Le estensioni non sono abilitate in Chrome in InCognito Windows. Firefox ha un'impostazione per consentire le estensioni durante la navigazione privata. Per ulteriori informazioni, consulta Utilizzo delle estensioni durante la navigazione privata.

È possibile aggiornare la configurazione delle impostazioni utente esistente di un portale o quando si crea un portale web per la prima volta. Innanzitutto, stabilisci quali domini ti servono per il tuo IdP SAML e i tuoi siti web. È possibile aggiungere fino a 10 domini.

L'utente è responsabile del test e dell'identificazione del dominio appropriato per la sincronizzazione dei cookie. Potrebbero essere necessarie modifiche a livello di IdP o di autenticazione del sito web per garantire che il Single Sign-On funzioni come previsto.

Per vedere quali domini utilizzare con gli IdP più comuni, consulta la tabella seguente:

IdP e domini

IdP	Domain
Okta	okta.com
Annuncio Azure	microsoftonline.com
AWS Identity Center	awsapps.com
Un unico accesso	onelogin.com
Duo	duosecurity.com

Successivamente, visita il tuo portale web nella console. Quindi, consenti l'estensione e aggiungi i cookie dei domini da sincronizzare. Segui i passaggi seguenti per creare un nuovo portale con l'estensione consentita o per aggiornare un portale esistente.

Per consentire l'estensione durante la creazione di un nuovo portale web, procedi nel seguente modo:

1. Segui i passaggi indicati in the section called “Fase 1: creazione di un portale Web” fino ad arrivare a the section called “Configurazione delle impostazioni utente”.
2. Nel passaggio 1 di the section called “Configurazione delle impostazioni utente”, in Autorizzazioni utente, scegli Consentita per abilitare l'estensione per il tuo portale web.
3. Inserisci il dominio per la sincronizzazione dei cookie e scegli Aggiungi nuovo dominio.
4. Completa i passaggi indicati in the section called “Configurazione delle impostazioni utente” e le sezioni rimanenti in the section called “Fase 1: creazione di un portale Web” per creare il tuo portale web.

Per aggiungere l'estensione a un portale web esistente, procedi nel seguente modo:

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Seleziona il portale web da modificare.
3. Seleziona Impostazioni utente, Autorizzazioni utente e Consentite per abilitare l’estensione per il tuo portale web.

4. Inserisci il dominio per la sincronizzazione dei cookie e scegli Aggiungi nuovo dominio.
5. Salva le modifiche al portale. I portali chiederanno agli utenti di installare l'estensione entro 15 minuti.

Per modificare i domini o rimuovere l'estensione, segui questi passaggi:

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Seleziona il portale web da modificare.
3. Seleziona Impostazioni utente, Autorizzazioni utente e Non consentita per rimuovere l'estensione per il tuo portale web.
4. Rimuovi o modifica singoli domini.
5. Una volta rimosse, le sessioni non sincronizzeranno più i cookie, anche se l'utente ha installato l'estensione WorkSpaces Web nel browser.

Per informazioni dettagliate sull'esperienza utente con l'estensione, consulta the section called "Estensione per Single Sign-On".

Imposta il filtraggio degli URL

Puoi utilizzare Chrome Policy per filtrare gli URL a cui gli utenti possono accedere dal proprio browser remoto. Chrome Policy offre due meccanismi per filtrare gli URL: URLAllowList e URLBlocklist. È possibile utilizzare l'interfaccia della console WorkSpaces Web per configurare il filtro degli URL come impostazione del portale oppure aggiungerlo come parte dell'istruzione JSON personalizzata (nell'editor in linea o come caricamento di file JSON).

Per configurare il filtraggio degli URL utilizzando la console

1. Aprire la console WorkSpaces Web all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Web, Portali Web, scegli il tuo portale Web, quindi scegli Visualizza dettagli.
3. Per il filtraggio degli URL, scegli una delle seguenti opzioni:

   - Consenti l'accesso a tutti gli URL: per impostazione predefinita, un portale web consente l'accesso a tutti gli URL. È possibile aggiungere siti Web specifici all'elenco BlockURL per impedire agli utenti di visitare tali siti durante una sessione. Ad esempio, l'aggiunta di

www.anycorp.com all'elenco BlockURL impedirà all'utente di navigare su www.anycorp.com durante la sessione.

- Blocca l'accesso a tutti gli URL: per impostazione predefinita, il portale web blocca l'accesso a tutti gli URL. Puoi aggiungere siti Web specifici all'elenco degli URL consentiti per creare un elenco di siti Web che gli utenti possono visitare e bloccare il traffico verso qualsiasi altro sito Web. Valuta la possibilità di aggiungere ogni URL come segnalibro per consentire l'accesso con 1 clic agli utenti durante la sessione.
- Configurazione avanzata: scegli questa opzione per creare elenchi AllowURL e blockURL in parallelo. La lista degli URL consentiti ha la priorità sulla lista di blocco degli URL. Questa opzione abilita il filtraggio degli URL per percorso. Ad esempio, puoi aggiungere www.anycorp.com alla lista dei blocchi e quindi aggiungere www.anycorp.com/hr all'elenco degli indirizzi consentiti. Ciò consente agli utenti di visitare www.anycorp.com/hr, ma non saranno in grado di accedere ad altri percorsi URL, come www.anycorp.com/finance.

Per ulteriori indicazioni sull'utilizzo degli URL bloccati e consentiti, consulta Consentire o bloccare l'accesso ai siti Web. Aggiungi gli URL a questi elenchi seguendo il formato di filtro degli elenchi bloccati di Chrome per ottenere risultati ottimali. Per ulteriori informazioni, consulta Formato di filtro della lista bloccata degli URL.

Per configurare il filtraggio degli URL utilizzando l'editor JSON o il caricamento di file

1. Dal modulo delle impostazioni delle politiche, scegli JSON Editor e ignora il modulo dell'interfaccia utente della console per la visualizzazione Editor o File Upload.

   - L'editor consente ai clienti di creare dichiarazioni politiche personalizzate in linea nella console. L'editor evidenzia gli errori nell'istruzione JSON durante la creazione delle policy.
   - Il caricamento dei file consente ai clienti di aggiungere un file JSON creato all'esterno della console (ad esempio esportato da un browser Chrome esistente).
2. Consulta i dettagli delle norme di Chrome per URLAllowList e URLBlocklist per formattare correttamente un elenco Allow/DenyURL per il tuo portale web. Per ulteriori informazioni, consulta URLAllowlist e URLBlocklist.

Sicurezza in Amazon WorkSpaces Web

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili ad Amazon WorkSpaces Web, consulta Servizi AWS coperti dal programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili ai dati.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Amazon WorkSpaces Web. Viene illustrato come configurare Amazon WorkSpaces Web per soddisfare gli obiettivi di sicurezza e conformità. Vengono inoltre fornite informazioni su come utilizzare altri servizi AWS che consentono di monitorare e proteggere le risorse di Amazon WorkSpaces Web.

Indice

Protezione dei dati in Amazon WorkSpaces Web

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in Amazon WorkSpaces Web. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con WorkSpaces Web o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

Amazon WorkSpaces Web raccoglie dati di personalizzazione del portale, come impostazioni del browser, impostazioni utente, impostazioni di rete, informazioni sul provider di identità, dati di trust store e dati del certificato Trust Store. WorkSpaces Web raccoglie anche i dati sulle politiche del browser, le preferenze dell'utente (per le impostazioni del browser) e i registri delle sessioni. I dati raccolti vengono archiviati in Amazon DynamoDB e Amazon S3. WorkSpaces Usi Web per la crittografiaAWS Key Management Service.

Per proteggere i tuoi contenuti, segui le linee guida riportate di seguito:

- Implementa l'accesso con privilegi minimi e crea ruoli specifici da utilizzare per le azioni WorkSpaces Web. Utilizza i modelli IAM per creare un ruolo con accesso completo o di sola lettura. Per ulteriori informazioni, consulta Politiche gestite AWS per WorkSpaces Web.
- Proteggi i dati dall'inizio alla fine fornendo una chiave gestita dal cliente, in modo che WorkSpaces Web possa crittografare i dati archiviati con le chiavi fornite.
- Fai attenzione a condividere i domini del portale e le credenziali degli utenti.
  - Gli amministratori devono accedere alla WorkSpaces console Amazon e gli utenti devono accedere al WorkSpaces portale Web.
  - Chiunque su Internet può accedere al portale Web, ma non può avviare una sessione a meno che non disponga di credenziali utente valida per il portale.
- Gli utenti possono terminare esplicitamente le sessioni selezionando Termina sessione. Ciò elimina l'istanza che ospita la sessione del browser e determina l'isolamento del browser.

WorkSpaces Il Web protegge contenuti e metadati per impostazione predefinita crittografando tutti i dati sensibili con. AWS KMS Raccoglie i criteri del browser e le preferenze dell'utente per applicare criteri e impostazioni durante le sessioni Web. WorkSpaces Se si verifica un errore durante l'applicazione delle impostazioni esistenti, un utente non può accedere alle nuove sessioni e ai siti interni dell'azienda e alle applicazioni SaaS.

Crittografia a riposo

La crittografia a riposo è configurata per impostazione predefinita. I dati specifici del cliente utilizzati nel WorkSpaces Web vengono crittografati utilizzando. AWS KMS WorkSpaces Il Web fornisce la crittografia inattiva per le risorse create. Il servizio accetta una chiave gestita AWS KMS dal cliente al momento della creazione delle risorse e, se non ne viene fornita una, verrà utilizzata una chiave AWS

proprietaria per crittografare le risorse inutilizzate. Il servizio crittografa il documento Browser Policy che puoi fornire per personalizzare le sessioni del browser, nonché la configurazione del tuo gestore dell'identità digitale e i nomi visualizzati per i tuoi portali. Queste informazioni rimarranno crittografate utilizzando la chiave gestita dal cliente o la chiave AWS di proprietà, mentre sono archiviate nel nostro backend.

È possibile decidere quale chiave verrà utilizzata quando si crea una risorsa WorkSpaces Web. Se i dati che fanno parte di quella risorsa sono crittografati, WorkSpaces Web accetta il `customerManagedKeyArn` campo come parte dell'`create`API. La chiave fornita deve essere una chiave simmetrica AWS KMS e l'amministratore che crea la risorsa utilizzando questa chiave deve disporre delle autorizzazioni `kms:Decrypt`, `kms:GenerateDataKey` e `kms:CreateGrant`. Dopo aver creato una risorsa con la chiave, la chiave non può essere rimossa o modificata. Se hai utilizzato una chiave gestita dal cliente, l'amministratore che accede alla risorsa deve disporre delle autorizzazioni `kms:Decrypt` e `kms:GenerateDataKey`. Se visualizzi un errore relativo al rifiuto dell'accesso durante l'utilizzo della console, assicurati che l'utente che utilizza la console disponga di queste autorizzazioni con la chiave utilizzata.

Puoi risolvere i problemi e controllare l'utilizzo delle chiavi controllando lo stato delle concessioni AWS KMS. Per ulteriori informazioni, consulta Gestione delle concessioni. Durante la creazione del portale, WorkSpaces Web crea una concessione per consentire al servizio di accedere alla chiave in modo asincrono. Puoi controllare lo stato dell'utilizzo delle nostre chiavi controllando la concessione, nonché il contesto di crittografia fornito quando viene utilizzata la concessione. Il contesto di crittografia contiene sempre una voce con la chiave `aws:workspaces-web:portal:id` e un valore uguale all'ID del portale. Per le altre risorse, il contesto di crittografia conterrà sempre una voce nel formato `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` e l'ID della risorsa corrispondente.

Crittografia in transito

WorkSpaces Web crittografa i dati in transito tramite HTTPS e TLS 1.2. Puoi inviare una richiesta a WorkSpaces utilizzando la console o chiamate API dirette. I dati della richiesta trasferiti vengono crittografati inviando tutto tramite una connessione HTTPS o TLS. I dati della richiesta possono essere trasferiti dalla AWS console o dall'AWSSDK al WorkSpaces Web. AWS Command Line Interface

La crittografia in transito è configurata per impostazione predefinita e le connessioni sicure (HTTPS, TLS) sono configurate per impostazione predefinita.

Gestione delle chiavi

È possibile fornire la propria chiave AWS KMS gestita dal cliente per crittografare le informazioni sui clienti. Se non ne fornisci uno, WorkSpaces Web utilizzerà una chiave AWS proprietaria. Puoi impostare la tua chiave utilizzando AWS SDK.

Riservatezza del traffico Internet

Per proteggere le connessioni tra il WorkSpaces Web e le applicazioni locali, utilizzi WorkSpaces Web per avviare sessioni del browser all'interno del tuo VPC. La connessione alle applicazioni locali è configurata nel tuo VPC e non è controllata dal Web. WorkSpaces

Per proteggere le connessioni tra gli account, WorkSpaces Web utilizza un ruolo collegato al servizio per connettersi in modo sicuro agli account dei clienti ed eseguire operazioni per conto del cliente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati al servizio per WorkSpaces Web.

Registrazione degli accessi utente

Gli amministratori sono in grado di registrare gli eventi delle sessioni WorkSpaces Web, tra cui avvio, interruzione e visite agli URL. Questi log sono crittografati e distribuiti in modo sicuro ai clienti tramite Amazon Kinesis Data Stream. Le informazioni di navigazione derivanti dalla registrazione degli accessi degli utenti non vengono archiviate da AWS o non sono disponibili nelle sessioni senza che la registrazione sia configurata. Le visite agli URL in modalità di navigazione in incognito o gli URL eliminati dalla cronologia del browser non vengono registrati nella registrazione degli accessi degli utenti.

Identity and Access Management per Amazon WorkSpaces Web

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Web. WorkSpaces IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Come funziona Amazon WorkSpaces Web con IAM
- Esempi di policy basate sull'identità per Amazon Web WorkSpaces
- Politiche gestite AWS per WorkSpaces Web
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Web
- Utilizzo di ruoli collegati al servizio per WorkSpaces Web

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi sul Web. WorkSpaces

Utente del servizio: se si utilizza il servizio WorkSpaces Web per svolgere il proprio lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. Man mano che si utilizzano più funzionalità WorkSpaces Web per svolgere il proprio lavoro, potrebbero essere necessarie autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non è possibile accedere a una funzionalità del WorkSpaces Web, vedereRisoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Web.

Amministratore del servizio: se sei responsabile delle risorse WorkSpaces Web della tua azienda, probabilmente hai pieno accesso al WorkSpaces Web. È compito dell'utente determinare a quali funzionalità e risorse WorkSpaces Web devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con il WorkSpaces Web, consultaCome funziona Amazon WorkSpaces Web con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso al WorkSpaces Web. Per visualizzare esempi di policy basate sull'identità WorkSpaces Web che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWS nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedi agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ai Servizi AWS

utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono agli Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un

ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona Amazon WorkSpaces Web con IAM

Prima di utilizzare IAM per gestire l'accesso al WorkSpaces Web, scopri quali funzionalità IAM sono disponibili per l'uso con WorkSpaces Web.

Funzionalità IAM che puoi utilizzare con Amazon WorkSpaces Web

Funzionalità IAM	WorkSpaces Supporto Web
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come il WorkSpaces Web e gli altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWSi servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per il Web WorkSpaces

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per il Web WorkSpaces

Per visualizzare esempi di politiche basate sull'identità WorkSpaces Web, vedere. Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Politiche basate sulle risorse all'interno del Web WorkSpaces

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per il Web WorkSpaces

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni WorkSpaces Web, consulta Actions defined by Amazon WorkSpaces Web nel Service Authorization Reference.

Le azioni politiche WorkSpaces sul Web utilizzano il seguente prefisso prima dell'azione:

```
workspaces-web
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'identità WorkSpaces Web, vedere. Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Risorse politiche per il Web WorkSpaces

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse WorkSpaces Web e dei relativi ARN, consulta Resources defined by Amazon WorkSpaces Web nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon WorkSpaces Web.

Per visualizzare esempi di politiche basate sull'identità WorkSpaces Web, consulta. Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Chiavi relative alle condizioni dei criteri per il Web WorkSpaces

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione WorkSpaces Web, consulta Condition keys for Amazon WorkSpaces Web nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon WorkSpaces Web.

Per visualizzare esempi di politiche basate sull'identità WorkSpaces Web, consulta. Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Liste di controllo degli accessi (ACL) nel Web WorkSpaces

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con Web WorkSpaces

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Web WorkSpaces

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le

credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali per più servizi per il Web WorkSpaces

Supporta sessioni di accesso diretto (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per il Web WorkSpaces

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità del WorkSpaces Web. Modifica i ruoli di servizio solo quando WorkSpaces Web fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per il Web WorkSpaces

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon Web WorkSpaces

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare WorkSpaces risorse Web. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti dal WorkSpaces Web, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon WorkSpaces Web nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Web WorkSpaces
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse WorkSpaces Web nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Web WorkSpaces

Per accedere alla console Amazon WorkSpaces Web, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse WorkSpaces Web del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console WorkSpaces Web, collega anche il WorkSpaces Web `ConsoleAccess` o la politica `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

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

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

Politiche gestite AWS per WorkSpaces Web

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere autonomamente le policy. La creazione di policy gestite dai clienti IAM che forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, utilizza le nostre policy gestite da AWS. Queste policy coprono i casi d'uso più comuni e sono disponibili nel tuo account AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente IAM.

I servizi AWS mantengono e aggiornano le policy gestite da AWS. Non è possibile modificare le autorizzazioni nelle policy gestite da AWS. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy gestita da AWS, pertanto gli aggiornamenti delle policy non interrompono le autorizzazioni esistenti.

Inoltre, AWS supporta policy gestite per le funzioni di processi che coprono più servizi. Ad esempio, la policy `ReadOnlyAccess` gestita da AWS fornisce l'accesso in sola lettura sia ai servizi AWS che a tutte le risorse. Quando un servizio avvia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente IAM.

Politica gestita AWS: AmazonWorkspacesWebServiceRolePolicy

Non è possibile allegare la policy `AmazonWorkSpacesWebServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a WorkSpaces Web di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta the section called “Utilizzo di ruoli collegati ai servizi”.

Questa policy concede autorizzazioni amministrative che consentono l'accesso ai servizi e alle risorse AWS utilizzate o gestite da Amazon WorkSpaces Web.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `WorkSpaces Web` – Consente l'accesso a servizi e risorse AWS utilizzati o gestiti da Amazon WorkSpaces Web.
- `ec2` – Consente ai principali di descrivere VPC, sottoreti e zone di disponibilità; creare, etichettare, descrivere ed eliminare interfacce di rete; associare o dissociare un indirizzo, nonché descrivere tabelle di routing, gruppi di sicurezza ed endpoint VPC.
- `CloudWatch` – Consente ai principali di inserire dati sui parametri.
- `Kinesis` – Consente ai principali di descrivere un riepilogo dei flussi di dati Kinesis e di inserire i record nei flussi di dati Kinesis per la registrazione degli accessi degli utenti. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.

```
{
    "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-*"
        }
    ]
}
```

Politica gestita AWS: AmazonWorkspacesWebReadOnly

È possibile allegare la policy `AmazonWorkSpacesWebReadOnly` alle identità IAM.

Questa policy concede autorizzazioni di sola lettura che consentono l'accesso a WorkSpaces Web e alle sue dipendenze tramite la console di gestione AWS, l'SDK e la CLI. Questa politica non include le autorizzazioni necessarie per interagire con i portali utilizzando `IAM_Identity_Center` come tipo di autenticazione. Per ottenere queste autorizzazioni, abbina questa policy a `AWSSSOReadOnly`.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `WorkSpaces Web` – Fornisce accesso in sola lettura ad Amazon WorkSpaces Web e alle sue dipendenze tramite la Console di gestione AWS, l'SDK e la CLI.
- `ec2`: consente ai principali di descrivere gruppi di sicurezza, sottoreti e VPC. Viene utilizzato nella Console di gestione AWS di WorkSpaces Web per mostrare i VPC, le sottoreti e i gruppi di sicurezza disponibili per l'uso con il servizio.
- `Kinesis`: consente ai principali di elencare i flussi di dati di Kinesis. Viene utilizzato nella Console di gestione AWS in WorkSpaces Web per mostrare i flussi di dati Kinesis disponibili per l'uso con il servizio.

```
{
    "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": "*"
        }
    ]
}
```

Aggiornamenti di WorkSpaces Web alle policy gestite AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per WorkSpaces Web da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

Modifica	Descrizione	Data
AmazonWorkspacesWebServiceRolePolicy – Policy aggiornata	WorkSpaces Web ha aggiornato la policy per limitare CreateNetworkInterface ai tag con aws:RequestTag/WorkSpacesWe	15 dicembre 2022

Modifica	Descrizione	Data
	bManaged: true e agire sulle risorse di sottorete e gruppi di sicurezza, nonché per limitare DeleteNetworkInterface agli ENI etichettati con tag aws:ResourceTag/WorkSpacesWebManaged: true.	
AmazonWorkspacesWebReadOnly – Policy aggiornata	WorkSpaces Web ha aggiornato la policy per includere le autorizzazioni di lettura per la registrazione degli accessi degli utenti e per elencare i flussi di dati Kinesis. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.	2 novembre 2022
AmazonWorkspacesWebServiceRolePolicy – Policy aggiornata	WorkSpaces Web ha aggiornato la policy per descrivere un riepilogo dei flussi di dati Kinesis e di inserire i record nei flussi di dati Kinesis per la registrazione degli accessi degli utenti. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.	17 ottobre 2022
AmazonWorkspacesWebServiceRolePolicy – Policy aggiornata	WorkSpaces Web ha aggiornato la policy per la creazione di tag durante la creazione di ENI.	6 settembre 2022

Modifica	Descrizione	Data
AmazonWorkspacesWebServiceRolePolicy – Policy aggiornata	WorkSpaces Web ha aggiornato la policy per aggiungere lo spazio dei nomi AWS/Usage alle autorizzazioni dell'API PutMetricData.	6 aprile 2022
AmazonWorkspacesWebReadOnly – Nuova policy	WorkSpaces Web ha aggiunto una nuova policy per fornire l'accesso in sola lettura ad Amazon WorkSpaces Web e alle sue dipendenze tramite la Console di gestione AWS, l'SDK e la CLI.	30 novembre 2021
AmazonWorkSpacesWebServiceRolePolicy – Nuova policy	WorkSpaces Web ha aggiunto una nuova policy per consentire l'accesso ai servizi e alle risorse AWS utilizzati o gestiti da Amazon WorkSpaces Web.	30 novembre 2021
WorkSpaces Web ha iniziato a monitorare le modifiche	WorkSpaces Web ha iniziato a monitorare le modifiche per le sue policy gestite da AWS.	30 novembre 2021

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Web

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con WorkSpaces Web e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione sul Web WorkSpaces
- Non sono autorizzato a eseguire iam: PassRole

- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse WorkSpaces Web

Non sono autorizzato a eseguire un'azione sul Web WorkSpaces

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `workspaces-web:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `workspaces-web:`*`GetWidget`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a WorkSpaces Web.

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione WorkSpaces sul Web. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse WorkSpaces Web

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se WorkSpaces Web supporta queste funzionalità, consultaCome funziona Amazon WorkSpaces Web con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati al servizio per WorkSpaces Web

WorkSpaces Web utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a WorkSpaces Web. I ruoli collegati ai servizi sono definiti automaticamente da WorkSpaces Web e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di WorkSpaces Web perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. WorkSpaces Web definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo WorkSpaces Web potrà assumere i propri ruoli. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Le policy di autorizzazioni non possono essere collegate a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di WorkSpaces Web perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni dei ruoli collegati al servizio per WorkSpaces Web

WorkSpaces Web usa il ruolo collegato ai servizi denominato `AWSServiceRoleForAmazonWorkSpacesWeb`: WorkSpaces Web usa questo ruolo collegato ai servizi per accedere alle risorse Amazon EC2 degli account dei clienti per le istanze di streaming e i parametri CloudWatch.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForAmazonWorkSpacesWeb` considera attendibili i seguenti servizi:

- `workspaces-web.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata `AmazonWorkSpacesWebServiceRolePolicy` consente a WorkSpaces Web di eseguire le seguenti operazioni sulle risorse specificate. Per ulteriori informazioni, consulta the section called “AmazonWorkSpacesWebServiceRolePolicy”.

- Operazione: `ec2:DescribeVpcs` su `all AWS resources`
- Operazione: `ec2:DescribeSubnets` su `all AWS resources`
- Operazione: `ec2:DescribeAvailabilityZones` su `all AWS resources`
- Operazione: `ec2:CreateNetworkInterface` con `aws:RequestTag/WorkSpacesWebManaged: true` su risorse del gruppo di sicurezza e della sottorete
- Operazione: `ec2:DescribeNetworkInterfaces` su `all AWS resources`

- Azione: `ec2:DeleteNetworkInterface` sulle interfacce di rete con `aws:ResourceTag/WorkSpacesWebManaged: true`
- Operazione: `ec2:DescribeSubnets` su `all AWS resources`
- Operazione: `ec2:AssociateAddress` su `all AWS resources`
- Operazione: `ec2:DisassociateAddress` su `all AWS resources`
- Operazione: `ec2:DescribeRouteTables` su `all AWS resources`
- Operazione: `ec2:DescribeSecurityGroups` su `all AWS resources`
- Operazione: `ec2:DescribeVpcEndpoints` su `all AWS resources`
- Azione: `ec2:CreateTags` su `ec2:CreateNetworkInterface` modalità Operazione con `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Operazione: `cloudwatch:PutMetricData` su `all AWS resources`
- Azione: `kinesis:PutRecord` su flussi di dati Kinesis con nomi che iniziano con `amazon-workspaces-web-`
- Azione: `kinesis:PutRecords` su flussi di dati Kinesis con nomi che iniziano con `amazon-workspaces-web-`
- Azione: `kinesis:DescribeStreamSummary` su flussi di dati Kinesis con nomi che iniziano con `amazon-workspaces-web-`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Ruoli collegati al servizio per WorkSpaces Web

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei il primo portale in AWS Management Console, AWS CLI o con l'API AWS, WorkSpaces Web crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo.

Se elimini questo ruolo collegato ai servizi e devi ricrearlo di nuovo, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando crei il primo portale, WorkSpaces Web crea di nuovo il ruolo collegato al servizio.

È possibile utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il caso d'uso WorkSpaces Web. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `workspaces-web.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato al servizio per WorkSpaces Web

WorkSpaces Web non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForAmazonWorkSpacesWeb`. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Modifica di un ruolo collegato al servizio per WorkSpaces Web

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio WorkSpaces Web utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse WorkSpaces Web utilizzate da AWSServiceRoleForAmazonWorkSpacesWeb

- Scegli una delle seguenti opzioni.
  - Se usi la console, elimina tutti i portali sulla console.
  - Se utilizzi la CLI o l'API, dissocia tutte le tue risorse (incluse le impostazioni del browser, le impostazioni di rete, le impostazioni utente, gli archivi attendibili e le impostazioni di

registrazione degli accessi degli utenti) dai tuoi portali, elimina queste risorse e quindi elimina i portali.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizzare la console IAM, AWS CLI o l'API AWS per eliminare il ruolo collegato al servizio AWSServiceRoleForAmazonWorkSpacesWeb. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati al servizio WorkSpaces Web

WorkSpaces Web supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Risposta agli incidenti in Amazon WorkSpaces Web

Puoi rilevare gli incidenti monitorando la metrica di `SessionFailure` Amazon CloudWatch. Per ricevere avvisi per incidenti, utilizza un allarme CloudWatch per la metrica `SessionFailure`. Per ulteriori informazioni, consulta Monitoraggio di Amazon WorkSpaces Web con Amazon CloudWatch.

Convalida della conformità per Amazon Web WorkSpaces

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

> **Note**
>
> Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager: questo Servizio AWSaiuta a verificare continuamente l'utilizzo di AWSper semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza in Amazon WorkSpaces Web

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità effettiva elevata. Con le Zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Attualmente WorkSpaces Web non supporta:

- Backup dei contenuti tra AZ o regioni
- Backup crittografati
- Crittografia dei contenuti in transito tra AZ o regioni
- Backup automatici o predefiniti

Per configurare l'elevata disponibilità di Internet, puoi ottimizzare la configurazione del VPC. Per un'elevata disponibilità delle API, puoi richiedere la giusta quantità di TPS.

Sicurezza dell'infrastruttura in Amazon WorkSpaces Web

In qualità di servizio gestito, Amazon WorkSpaces Web è protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere ad Amazon WorkSpaces Web tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

WorkSpaces Web isola il traffico dei servizi applicando l'autenticazione e l'autorizzazione SigV4 AWS standard a tutti i servizi. L'endpoint delle risorse per i clienti (o endpoint del portale web) è protetto dal tuo gestore dell'identità digitale. Puoi isolare ulteriormente il traffico utilizzando l'autorizzazione a più fattori e altri meccanismi di sicurezza nel tuo gestore dell'identità digitale.

Tutti gli accessi a Internet possono essere controllati configurando le impostazioni di rete, come VPC, sottorete o gruppo di sicurezza. Gli endpoint multi-tenancy e VPC (PrivateLink) non sono attualmente supportati.

Analisi della configurazione e delle vulnerabilità in Amazon WorkSpaces Web

WorkSpaces Web aggiorna e applica patch alle applicazioni e alle piattaforme secondo necessità per tuo conto, inclusi Chrome e Linux. Non è necessario applicare patch o ricostruire. Tuttavia, è responsabilità dell'utente configurare WorkSpaces Web in base a specifiche e linee guida e monitorare l'utilizzo di WorkSpaces Web da parte degli utenti. Tutte le configurazioni relative ai servizi e l'analisi delle vulnerabilità sono di competenza di WorkSpaces Web.

È possibile richiedere un aumento del limite per le risorse WorkSpaces Web, ad esempio il numero di portali Web e il numero di utenti. WorkSpaces Web garantisce la disponibilità del servizio e dello SLA.

Best practice di sicurezza per Amazon WorkSpaces Web

Amazon WorkSpaces Web fornisce una serie di caratteristiche di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché potrebbero non essere appropriate o sufficienti per il tuo ambiente, prendile come considerazioni utili più che istruzioni.

Le best practice per Amazon WorkSpaces Web includono quanto segue:

- Per rilevare potenziali eventi di sicurezza associati all'uso di WorkSpaces Web, utilizza AWS CloudTrail o Amazon CloudWatch per rilevare e tenere traccia della cronologia degli accessi e dei log di processo. Per ulteriori informazioni, consulta Monitoraggio di Amazon WorkSpaces Web con Amazon CloudWatch e Registrazione delle chiamate API di Amazon WorkSpaces Web tramite AWS CloudTrail.
- Per implementare i controlli investigativi e identificare le anomalie, utilizza i log di CloudTrail e i parametri di CloudWatch. Per ulteriori informazioni, consulta Monitoraggio di Amazon WorkSpaces Web con Amazon CloudWatch e Registrazione delle chiamate API di Amazon WorkSpaces Web tramite AWS CloudTrail.

- È possibile configurare la registrazione degli accessi degli utenti per avere i log degli eventi degli utenti. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.

Per prevenire potenziali eventi di sicurezza associati all'utilizzo di WorkSpaces Web, segui queste best practice:

- Implementa l'accesso con privilegi minimi e crea ruoli specifici da utilizzare per le azioni di WorkSpaces Web. Utilizza i modelli IAM per creare un ruolo con accesso completo o di sola lettura. Per ulteriori informazioni, consulta Politiche gestite AWS per WorkSpaces Web.
- Fai attenzione a condividere i domini del portale e le credenziali degli utenti. Chiunque su Internet può accedere al portale Web, ma non può avviare una sessione a meno che non disponga di una credenziale utente valida per il portale. Presta attenzione a come, quando e con chi condividi le credenziali del portale web.

Monitoraggio di Amazon WorkSpaces Web

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon WorkSpaces Web e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare i portali WorkSpaces Web e le relative risorse, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi CloudWatch tenere traccia dell'utilizzo della CPU o di altri parametri per le tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre CloudTrail fonti. CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente.

Argomenti

Monitoraggio di Amazon WorkSpaces Web con Amazon CloudWatch

Puoi monitorare Amazon WorkSpaces Web utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per

un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Lo spazio dei nomi `AWS/WorkSpacesWeb` include i parametri descritti di seguito.

CloudWatch metriche per Amazon Web WorkSpaces

Parametro	Descrizione	Dimensioni	Statistiche	Unità
`SessionAttempt`	Il numero di tentativi di sessione Amazon WorkSpaces Web.	`PortalId`	Media, Somma, Massimo, Minimo	Conteggio
`SessionSuccess`	Il numero di sessioni Amazon WorkSpaces Web avviate con successo.	`PortalId`	Media, Somma, Massimo, Minimo	Conteggio
`SessionFailure`	Il numero di sessioni Amazon WorkSpaces Web non riuscite.	`PortalId`	Media, Somma, Massimo, Minimo	Conteggio
`GlobalCpuPercent`	L'utilizzo della CPU dell'istanza della sessione Amazon WorkSpaces Web.	`PortalId`	Media, Somma, Massimo, Minimo	Percentuale

Parametro	Descrizione	Dimensioni	Statistiche	Unità
`GlobalMemoryPercent`	L'utilizzo della memoria (RAM) dell'istanza di sessione Amazon WorkSpaces Web.	`PortalId`	Media, Somma, Massimo, Minimo	Percentuale

> **Note**
>
> Puoi visualizzare la statistica metrica «SampleCount» per `GlobalCpuPercent` o `GlobalMemoryPercent` determinare il numero di sessioni simultanee attive sul tuo portale. I punti dati vengono emessi da ogni sessione una volta al minuto.

Registrazione delle chiamate API di Amazon WorkSpaces Web tramite AWS CloudTrail

Amazon S3 è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Amazon WorkSpaces Web. CloudTrail acquisisce tutte le chiamate API per Amazon WorkSpaces Web come eventi. Queste includono le chiamate dalla console Amazon WorkSpaces Web e le chiamate di codice alle operazioni delle API di Amazon WorkSpaces Web. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Amazon WorkSpaces Web. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi. Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad Amazon WorkSpaces Web, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni sul Amazon WorkSpaces Web in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Amazon WorkSpaces Web, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. Nella Cronologia degli eventi è possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi per Amazon WorkSpaces Web, crea un percorso. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più Regioni e Ricezione di file di registro CloudTrail da più account

Tutte le operazioni Amazon WorkSpaces Web vengono registrate da CloudTrail e sono documentate nella Documentazione di riferimento delle API di Amazon WorkSpaces. Ad esempio, le chiamate alle operazioni `CreatePortal`, `DeleteUserSettings` e `ListBrowserSettings` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del file di log di Amazon WorkSpaces Web

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e altri dettagli. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `ListBrowserSettings`.


```
{
   "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"
    }]
}
```


Registrazione degli accessi utente

Amazon WorkSpaces Web consente ai clienti di registrare gli eventi della sessione, tra cui avvio, interruzione e visite agli URL. Questi log vengono inviati a un flusso di dati Amazon Kinesis specificato per il tuo portale web. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione degli accessi utente”.

Linee guida per gli utenti di Amazon WorkSpaces Web

Gli amministratori utilizzano Amazon WorkSpaces Web per creare portali Web che si collegano a siti Web aziendali, come siti Web interni, applicazioni Web software-as-a-service (SAAS) o Internet. Gli utenti finali utilizzano i browser Web esistenti per accedere a questi portali Web al fine di avviare una sessione e accedere ai contenuti.

Il seguente contenuto aiuta a guidare gli utenti finali che desiderano saperne di più sull'accesso ad Amazon WorkSpaces Web, sull'avvio e sulla configurazione di una sessione e sull'utilizzo della barra degli strumenti e del browser Web.

Argomenti

Compatibilità browser e dispositivo

Amazon WorkSpaces Web è alimentato dal client del browser Web NICE DCV, che viene eseguito all'interno di un browser Web, quindi non è richiesta alcuna installazione. Il client del browser Web è supportato dai browser Web più comuni, come Chrome e Firefox, e dai principali sistemi operativi desktop, come Windows, macOS e Linux.

Per maggiori up-to-date dettagli sul supporto dei client per browser Web, consulta Web browser client.

> **Note**
>
> Il supporto per la webcam è attualmente disponibile solo nei browser basati su Chromium, come Google Chrome e Microsoft Edge. Attualmente, Apple Safari e Mozilla FireFox non supportano la webcam.

Accesso al portale Web

L'amministratore può fornire l'accesso al portale Web con le seguenti opzioni:

- Puoi selezionare un link da un'e-mail o da un sito Web, quindi accedere con le tue credenziali di identità SAML.
- Puoi accedere al tuo gestore dell'identità digitale SAML (come Okta, Ping o Azure) e avviare una sessione con un clic dalla home page dell'applicazione del provider SAML (come la dashboard dell'utente finale di Okta o il portale Azure Myapps).

Guida alla sessione

Dopo aver effettuato l'accesso al portale web, puoi avviare una sessione ed eseguire varie azioni durante la sessione.

Argomenti

Avvio di una sessione

Dopo aver effettuato l'accesso per avviare una sessione, verranno visualizzati il messaggio di Avvio della sessione e la barra di avanzamento. Ciò indica che Amazon WorkSpaces Web sta creando una sessione per te. Dietro le quinte, Amazon WorkSpaces Web crea l'istanza, avvia il browser Web gestito e applica le impostazioni dell'amministratore e le politiche del browser.

Se è la prima volta che accedi al tuo portale web, vedrai delle icone blu + nella barra degli strumenti. Questa icona indica che è disponibile un tutorial che illustrerà le funzionalità disponibili nella barra degli strumenti. Puoi usare queste icone per imparare a:

- Autorizzare il browser all’uso di microfono, webcam e appunti selezionando l'icona del lucchetto accanto al browser locale e impostando l'interruttore su On accanto agli appunti, al microfono e alla fotocamera.

> **Note**
>
> Quando abiliti le autorizzazioni della webcam all'inizio della prima sessione, la webcam viene abilitata brevemente e una spia sul computer lampeggerà. Ciò consente l'accesso alla webcam tramite browser locale.

- Consenti ad Amazon WorkSpaces Web di avviare finestre di monitoraggio aggiuntive selezionando l'icona a forma di lucchetto nel browser e l'impostazione Consenti sempre i popup.

Se desideri rilanciare un tutorial, puoi scegliere Profilo dalla barra degli strumenti, Guida e Avvia tutorial.

Usa la barra degli strumenti

Per spostare la barra degli strumenti, seleziona la barra più chiara nella parte superiore della barra degli strumenti, trascinala nella posizione desiderata, quindi rilasciala per eliminarla.

Per comprimere la barra degli strumenti, passaci sopra con il mouse e seleziona il pulsante freccia su, oppure fai doppio clic sulla barra più chiara nella sezione superiore. La visualizzazione compressa offre più spazio sullo schermo e l'accesso con un solo clic alle icone più utilizzate.

Per agganciare la barra degli strumenti nella parte superiore dello schermo, scegli Preferenze, Generali e Docked in modalità Barra degli strumenti.

La tabella seguente include una descrizione di tutte le icone disponibili nella barra degli strumenti:

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**
>
> Le icone degli Appunti e dei File sono nascoste per impostazione predefinita, a meno che l'amministratore non conceda tali autorizzazioni. Solo gli amministratori possono abilitare o disabilitare gli appunti e i file su un portale Web. Se queste icone sono nascoste e devi accedervi, contatta l'amministratore.

Usa il browser

All'avvio della sessione, il browser visualizza l'URL di avvio, che è un URL scelto dall'amministratore. Se l'amministratore non ha scelto un URL di avvio, vedrai la nuova esperienza predefinita con la nuova scheda di Google Chrome.

Dal browser, puoi aprire schede, avviare finestre aggiuntive del browser (dall'icona della barra degli strumenti di Windows o dal menu a tre punti del browser), inserire un URL o effettuare una ricerca nella barra degli URL oppure accedere ai siti Web dai segnalibri gestiti. Per accedere ai segnalibri per il portale web, apri la cartella Segnalibri gestiti nella barra dei preferiti (sotto la barra degli URL) o apri il gestore dei segnalibri dal menu a tre punti sul lato destro della barra degli URL.

Per ridimensionare o spostare la finestra del browser, trascina verso il basso la barra delle schede di Chrome. Ciò consente di avere più spazio sullo schermo per più finestre del browser durante la sessione.

> **Note**
>
> Le funzionalità del browser, come la modalità di navigazione in incognito, potrebbero non essere disponibili durante la sessione se l'amministratore le ha disattivate.

Terminare una sessione

Per terminare una sessione, scegli Profilo e Termina sessione. Al termine di una sessione, Amazon WorkSpaces Web elimina tutti i dati dalla sessione. Nessun dato del browser, come siti Web aperti o cronologia, o file o dati di File Explorer è disponibile al termine di una sessione.

Se chiudi una scheda durante una sessione attiva, la sessione termina dopo un periodo di tempo impostato dall'amministratore. Se chiudi la scheda e visiti nuovamente il portale web prima che

questo timeout abbia effetto, puoi partecipare alla sessione corrente e visualizzare tutti i dati della sessione precedente, ad esempio siti Web e file aperti.

Risoluzione dei problemi

Il mio portale WorkSpaces Web Amazon non mi consente di accedere. Ho ricevuto un messaggio di errore che dice "Il tuo portale web non è ancora configurato. Contactta l'amministratore IT per assistenza."

L'amministratore deve completare la creazione del portale con un gestore dell'identità digitale SAML 2.0 per consentirti di accedere. Contatta l'amministratore per assistenza.

Il mio portale non avvia una sessione. Ho ricevuto un messaggio di errore che dice "Impossibile prenotare la sessione. Si è verificato un errore interno. Riprova."

Si è verificato un problema con l'avvio della sessione del portale web. Prova ad avviare nuovamente la sessione. Se il problema persiste, contatta l'amministratore per ricevere assistenza.

Non riesco a usare gli appunti, il microfono o la webcam.

Per autorizzare il browser, seleziona l'icona del lucchetto accanto all'URL e attiva l'interruttore blu accanto a Appunti, Microfono, Fotocamera e Popup e reindirizzamenti per attivare queste funzionalità.

> **Note**
>
> Se il tuo browser web non supporta l'input video o audio, queste opzioni non verranno visualizzate sulla barra degli strumenti.

L'audio video (AV) in tempo reale di Amazon WorkSpaces Web reindirizza il video della webcam locale e l'ingresso audio del microfono alla sessione di streaming del browser. In questo modo, puoi utilizzare i dispositivi locali per conferenze video e audio all'interno della sessione di streaming con browser Web basati su Chromium, come Google Chrome o Microsoft Edge. La webcam non è attualmente supportata nei browser diversi da Chromium.

Per informazioni su come configurare Google Chrome, consulta Utilizzare fotocamera e microfono.

Il mio portale web non apre una finestra di monitoraggio aggiuntiva.

Se provi ad avviare due monitor e vedi l'icona dei Popup bloccati alla fine della barra degli indirizzi nel browser in alto, seleziona l'icona e il pulsante di opzione accanto a Consenti sempre i popup e i reindirizzamenti. Se i popup sono consentiti, seleziona l'icona Doppio monitor sulla barra degli strumenti per aprire una nuova finestra, riposiziona la finestra sul monitor e trascina una scheda del browser nella finestra.

Quando provo a scaricare file dal riquadro File, non succede nulla.

Se provi a scaricare file dal pannello File e vedi l'icona Popup bloccati alla fine della barra degli indirizzi nel browser in alto, seleziona l'icona e il pulsante di opzione accanto a Consenti sempre i popup e i reindirizzamenti. Se i popup sono consentiti, prova a scaricare nuovamente i file.

Estensione per Single Sign-On

Amazon WorkSpaces Web offre un'estensione per il single sign-on con i browser Chrome e Firefox sui computer desktop. Se l'amministratore ha abilitato l'estensione, il portale web ti chiederà di installarla al momento dell'accesso.

Amazon WorkSpaces Web ha creato l'estensione per abilitare il Single Sign-On ai siti Web durante la sessione. Ad esempio, se accedi al tuo portale web utilizzando un gestore dell'identità digitale SAML 2.0 (come Okta o Ping) e durante la sessione visiti un sito Web che utilizza lo stesso gestore dell'identità digitale, l'estensione può semplificare l'accesso al sito Web rimuovendo ulteriori richieste di accesso.

Non è necessario installare l'estensione per accedere al portale web, ma può migliorare la tua esperienza riducendo il numero di volte in cui ti viene chiesto di inserire nome utente e password.

Quando effettui l'accesso, l'estensione individua i cookie elencati dall'amministratore per la sessione. Tutti i dati localizzati dall'estensione sono crittografati quando sono inattivi e durante il transito. Nessuno di questi dati viene memorizzato nel browser locale. Al termine della sessione, tutti i dati della sessione (ad esempio schede aperte, file scaricati e cookie inviati o creati durante la sessione) vengono eliminati.

Compatibilità

L'estensione funziona con i seguenti dispositivi:

- Computer portatili
- Computer desktop

L'estensione funziona con i seguenti browser:

- Chrome
- Firefox

Installazione

Quando accedi al portale, segui le istruzioni per installare l'estensione per il browser Chrome o Firefox dal web store del browser. Devi eseguire questa operazione una sola volta per ogni browser web.

Se cambi dispositivo, passi a un altro browser sullo stesso dispositivo o elimini l'estensione dal browser locale, all'avvio della sessione successiva verrà visualizzato un messaggio che richiede di installare l'estensione.

Per assicurarti che l'estensione funzioni come previsto, utilizza l'estensione in una normale scheda di navigazione, anziché in incognito (Chrome) o nella navigazione privata (Firefox).

Risoluzione dei problemi

Se hai installato l'estensione, ma ti viene comunque chiesto di accedere durante la sessione, segui questi passaggi:

1. Assicurati di avere l'estensione Amazon WorkSpaces Web installata sul tuo browser. Se hai eliminato i dati del browser, potresti aver rimosso l'estensione per sbaglio.
2. Assicurati di non utilizzare la navigazione in incognito (Chrome) o la navigazione privata (Firefox). Queste modalità possono causare problemi con le estensioni.
3. Se il problema persiste, contatta l'amministratore del portale per ulteriore assistenza.

Cronologia dei documenti per l'Amazon WorkSpaces Web User Guide

La tabella seguente descrive le versioni della documentazione per Amazon WorkSpaces Web.

Modifica	Descrizione	Data
CloudWatch metriche	Aggiunte GlobalCpuPercent e GlobalMemoryPercent metriche.	26 febbraio 2024
Configura il filtraggio degli URL	Puoi utilizzare Chrome Policy per filtrare gli URL a cui gli utenti possono accedere dal proprio browser remoto.	21 febbraio 2024
Tipi di autenticazione IdP	Puoi scegliere il tipo di autenticazione standard o IAM Identity Center.	5 febbraio 2024
Abilita l’estensione per Single Sign-On	Puoi abilitare un'estensione per gli utenti finali per avere una migliore esperienza di accesso al portale.	28 agosto 2023
Linee guida per l'utente per Amazon WorkSpaces Web	Sono stati aggiunti contenuti per aiutare gli utenti finali a saperne di più sull'accesso ad Amazon WorkSpaces Web, sull'avvio e sulla configura zione di una sessione e sull'util izzo della barra degli strumenti e del browser Web.	17 luglio 2023
Controlli sugli accessi degli IP	WorkSpaces Il Web ti consente di controllare da	31 maggio 2023

	quali indirizzi IP è possibile accedere al tuo portale web.	
Aggiornamento della policy gestita	Politica AmazonWorkSpacesWebReadOnly gestita aggiornata	15 maggio 2023
Configura l'aggiornamento del gestore dell'identità digitale	WorkSpaces Il Web offre due tipi di autenticazione: Standard e AWS IAM Identity Center	15 marzo 2023
Aggiornamento della policy del browser	Sezione della policy del browser aggiornata e ristrutturata	31 gennaio 2023
Aggiornamento della policy gestita	Policy AmazonWorkSpacesWebServiceRolePolicy gestita aggiornata	15 dicembre 2022
Lista consentita e lista di blocco	Specifica la lista consentita e la lista di blocco per indicare un elenco di domini a cui gli utenti possono o non possono accedere.	14 novembre 2022
Aggiornamento della policy gestita	Politica AmazonWorkSpacesWebReadOnly gestita aggiornata	2 novembre 2022
Aggiornamento della policy gestita	Politica AmazonWorkSpacesWebServiceRolePolicy gestita aggiornata	24 ottobre 2022
Registrazione degli accessi utente	Puoi configurare la registrazione degli accessi degli utenti per avere i log degli eventi degli utenti.	17 ottobre 2022

Aggiornamenti di rete	Vari aggiornamenti alla sezione “Rete e accesso”	22 settembre 2022
Aggiornamento della policy gestita	Politica AmazonWorkSpacesWebServiceRolePolicy gestita aggiornata	6 settembre 2022
Configura le sessioni utente	Configura l'Input Method Editor (IME) e la localizzazione in sessione	28 luglio 2022
Aggiornamenti di rete	Vari aggiornamenti alla sezione “Rete e accesso”	7 luglio 2022
Valori timeout	Specifica il timeout di disconnessione in minuti e il timeout di disconnessione di inattività in minuti	16 maggio 2022
Policy gestite e aggiornate	Aggiornata la policy AmazonWorkSpacesWebServiceRolePolicy gestita per aggiungere lo spazio dei nomi AWS/Usage alle autorizzazioni API PutMetricData	6 aprile 2022
Ruolo collegato ai servizi	Nuovo ruolo collegato al servizio AWSServiceRoleForAmazonWorkSpacesWeb	30 novembre 2021
Policy gestita	Nuova politica AmazonWorkSpacesWebReadOnly gestita	30 novembre 2021
Policy gestita	Nuova politica AmazonWorkSpacesWebServiceRolePolicy gestita	30 novembre 2021

Versione iniziale	Versione iniziale della WorkSpaces Web Administration Guide	30 novembre 2021

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.