Guida di amministrazione

Browser WorkSpaces sicuro Amazon

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

Browser WorkSpaces sicuro Amazon: Guida di amministrazione

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è Amazon WorkSpaces Secure Browser? 1
Cronologia delle versioni 1
Termini da conoscere 2
Servizi correlati 4
Architecture 5
Accesso 5
Configurazione 6
Registrazione e creazione di un utente 6
Registrati per un Account AWS 6
Concessione dell'accesso programmatico 6
Rete 8
Configurazione VPC 9
Connessioni utente 23
Nozioni di base 26
Creazione di un portale Web 26
Impostazioni di rete 27
Impostazioni del portale 27
Impostazioni utente 30
Configurazione del provider di identità 32
Avvia 42
Test del portale Web 43
Distribuzione su portali Web 44
Gestione del portale web 45
Visualizzazione dei dettagli del portale Web 46
Modifica di un portale Web 46
Eliminazione di un portale Web 46
Gestione delle quote di servizio 47
Richiesta di un aumento delle quote di servizio 48
Richiedere un aumento del portale 49
Richiesta di un aumento massimo delle sessioni simultanee 49
Esempio di limite 50
Altre quote di servizio 50
Riautenticazione di un token IdP SAML 51
Configurazione della registrazione delle attività degli utenti 52

Configurazione di Session Logger ... 53
Configurazione della registrazione degli accessi degli utenti ... 56
Gestione della politica del browser ... 57
Tutorial: impostazione di una politica del browser personalizzata ... 58
Modifica della politica di base del browser ... 64
Configurazione dell'Input Method Editor ... 65
Configurazione della localizzazione durante la sessione ... 67
Codici di lingua supportati ... 68
Impostazioni del browser utente ... 70
Gestione dei controlli di accesso IP ... 70
Creazione di un gruppo di controllo degli accessi IP ... 72
Associazione di un'impostazione di accesso IP ... 72
Modifica di un gruppo di controllo degli accessi IP ... 73
Eliminazione di un gruppo di controllo degli accessi IP ... 74
Gestione dell'estensione Single Sign-On ... 74
Identificazione dei domini per l'estensione Single Sign-On ... 75
Aggiungere l'estensione Single Sign-On a un nuovo portale web ... 76
Aggiungere l'estensione Single Sign-On a un portale Web esistente ... 76
Modifica o rimozione dell'estensione Single Sign-On ... 77
Filtraggio dei contenuti Web ... 77
Limitazione della navigazione a elementi specifici URLs ... 78
Blocco specifico URLs ... 78
Categorie di blocco ... 79
Esempio di URLs ... 82
Trasferimento delle politiche di Chrome ... 82
Deep link ... 82
Configurazione di link diretti ... 83
Utilizzo del filtraggio degli URL per i link diretti ... 84
Dashboard di gestione delle sessioni ... 84
Accesso al pannello di controllo ... 84
Filtri del dashboard ... 84
Termina le sessioni ... 85
Cronologia delle sessioni ... 85
Protezione dei dati in transito ... 86
Impostazioni di protezione dei dati ... 86
Redazione dei dati in linea ... 87

Configurazione di redazione predefinita 89
Redazione in linea di base 90
Redazione in linea personalizzata 92
Crea impostazioni di protezione dei dati 93
Associa le impostazioni di protezione dei dati 94
Modifica le impostazioni di protezione dei dati 95
Elimina le impostazioni di protezione dei dati 96
Personalizzazione del branding 96
Configurazione della personalizzazione del marchio per il portale 97
Linee guida per la personalizzazione 100
Reindirizzamento dell'autenticazione Web 113
Abilita il WebAuthn reindirizzamento nelle impostazioni del portale 114
Configurare la politica locale del browser 114
WebAuthn utilizzo del reindirizzamento 115
WebAuthn risoluzione dei problemi di reindirizzamento 115
Controlli della barra degli strumenti 116
Dominio personalizzato 117
Configurazione di un dominio personalizzato per il portale 118
Risoluzione dei problemi relativi ai domini personalizzati 129
Sicurezza 131
Protezione dei dati 132
Crittografia dei dati 133
Inter-network privacy del traffico 142
Registrazione degli accessi utente 143
Identity and Access Management 143
Destinatari 143
Autenticazione con identità 144
Gestione dell’accesso tramite policy 145
Come funziona Amazon WorkSpaces Secure Browser con IAM 147
Esempi di policy basate su identità 153
AWS politiche gestite 156
Risoluzione dei problemi 166
Uso di ruoli collegati ai servizi 168
Risposta agli incidenti 172
Convalida della conformità 172
Resilienza 173

Sicurezza dell'infrastruttura 173
Analisi della configurazione e delle vulnerabilità 174
Interfaccia VPC endpoint ()AWS PrivateLink 174
Considerazioni per Amazon WorkSpaces Secure Browser 175
Creazione di un endpoint VPC di interfaccia per Amazon Secure Browser WorkSpaces 175
Creazione di una policy sugli endpoint per l'endpoint VPC di interfaccia 176
Risoluzione dei problemi 177
Best practice di sicurezza 177
Monitoraggio 179
Monitoraggio con CloudWatch 179
CloudTrail registri 183
Informazioni in CloudTrail 184
Voci dei file di registro 185
Registrazione delle attività degli utenti 186
Eventi di sessione in Session Logger 187
Eventi di sessione nella registrazione di User Access 195
Guida per l'utente 197
Compatibilità browser e dispositivo 197
Accesso al portale Web 198
Guida alla sessione 198
Avvio di una sessione 198
Utilizzo della barra degli strumenti 199
Utilizzo del browser 202
Terminare una sessione 202
Risoluzione dei problemi degli utenti 203
Estensione Single Sign-On 204
Compatibilità con le estensioni Single Sign-On 205
Installazione dell'estensione Single Sign-On 205
Risoluzione dei problemi relativi all'estensione Single Sign-On 206
Cronologia dei documenti 207
..... ccxii

Cos'è Amazon WorkSpaces Secure Browser?

> **Note**
>
> Amazon WorkSpaces Secure Browser era precedentemente noto come Amazon WorkSpaces Web.

Amazon WorkSpaces Secure Browser è un servizio di browser ospitato completamente gestito, nativo del cloud, utilizzato per accedere in modo sicuro a siti Web privati e applicazioni Web (software-as-a-serviceSaaS), interagire con le risorse online e navigare in Internet da un contenitore usa e getta. WorkSpaces Secure Browser funziona con i browser Web esistenti dell'utente, senza sovraccaricare l'IT con la gestione di appliance, infrastrutture, software client specializzato o connessioni di rete privata virtuale (VPN). I contenuti Web vengono trasmessi in streaming al browser Web dell'utente, mentre il browser e il contenuto Web effettivi vengono isolati. AWS Utilizzando le stesse tecnologie di base su cui si basano i servizi di AWS End User Computing come Amazon WorkSpaces e Amazon WorkSpaces Applications, WorkSpaces Secure Browser può essere più conveniente rispetto ai desktop virtuali tradizionali e ridurre la complessità rispetto alla fornitura di software di gestione ai dispositivi di proprietà dell'azienda. WorkSpaces Secure Browser riduce il rischio di esfiltrazione dei dati mediante lo streaming di contenuti web. Nessun codice HTML, Document Object Model (DOM) o dati aziendali sensibili viene trasmesso al computer locale. Isolando il dispositivo, la rete aziendale e Internet l'uno dall'altro, la superficie di attacco del browser viene praticamente eliminata.

È possibile applicare la politica del browser aziendale (incluso l'consentimento/blocco degli URL) a tutte le sessioni e include controlli a livello di sessione per appunti, trasferimento di file e stampante. È inoltre possibile limitare l'accesso a reti o dispositivi affidabili utilizzando i controlli di accesso IP. WorkSpaces Secure Browser è facile da configurare e utilizzare. Ogni sessione viene avviata con una versione nuova e completamente aggiornata del browser Chrome, con le politiche e le impostazioni aziendali applicate.

Cronologia di pubblicazione di Amazon WorkSpaces Secure Browser

Il 20 maggio 2024, Amazon WorkSpaces Web è stato rinominato Amazon WorkSpaces Secure Browser. Per i clienti esistenti, non è stata apportata alcuna modifica al modo in cui gestiscono gli

utenti o le risorse con il servizio. L'elenco seguente descrive gli aggiornamenti applicabili che hanno avuto luogo anche in seguito a questa ridenominazione.

Lo spazio dei nomi dell'API workspaces-web rimane invariato per motivi di compatibilità con le versioni precedenti. Di conseguenza, le seguenti risorse sono sempre le stesse:

- Comandi CLI.
- CloudWatch Metriche di Amazon. Per ulteriori informazioni, consulta the section called “Monitoraggio con CloudWatch”.
- Endpoint del servizio. Per ulteriori informazioni, consulta Endpoint e quote di Amazon WorkSpaces Secure Browser.
- AWS CloudFormation risorse. Per ulteriori informazioni, consulta il riferimento al tipo di risorsa Amazon WorkSpaces Secure Browser.
- Ruolo collegato al servizio contenente workspaces-web. Per ulteriori informazioni, consulta the section called “Uso di ruoli collegati ai servizi”.
- Console URLs contenente workspaces-web.
- Documentazione contenente workspaces-web URLs . Per ulteriori informazioni, consulta la documentazione di Amazon WorkSpaces Secure Browser.
- Ruolo ReadOnly gestito esistente. Per ulteriori informazioni, consulta the section called “AWS politiche gestite”.
- Nome della concessione KMS.
- Prefisso del flusso Kinesis UAL (User-Activity Logging).

Inoltre, il portale URLs esistente rimane lo stesso. URLs <UUID>per i portali creati prima del 20 maggio 2024 ha utilizzato il formato .workspaces-web.com. WorkSpaces I portali Secure Browser continuano a utilizzare questo formato e il dominio workspaces-web.com.

Termini da conoscere per l'utilizzo di Amazon WorkSpaces Secure Browser

Per aiutarti a iniziare a usare WorkSpaces Secure Browser, dovresti acquisire familiarità con i seguenti concetti.

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. Puoi configurare il tuo IdP esistente per funzionare con WorkSpaces Secure Browser.

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. Devi inoltre concedere l'accesso ai tuoi utenti per utilizzare WorkSpaces Secure Browser nel tuo IdP.

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

WorkSpaces Secure Browser richiede metadati specifici dal tuo provider di identità (IdP) per stabilire la fiducia. Puoi aggiungere questi metadati a WorkSpaces Secure Browser 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 Secure Browser 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)

Puoi utilizzare un VPC nuovo o esistente, le sottoreti corrispondenti e i gruppi di sicurezza per collegare i tuoi contenuti a Secure Browser. WorkSpaces

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.

Le VPCs sottoreti e i gruppi di sicurezza elencati provengono dalla stessa regione della console Secure Browser. WorkSpaces

Trust store (Archivio trust)

Se un utente che accede a un sito Web tramite WorkSpaces Secure Browser 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 aggiungerlo o modificarlo nel proprio trust store. PCAs 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 Secure Browser.

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.

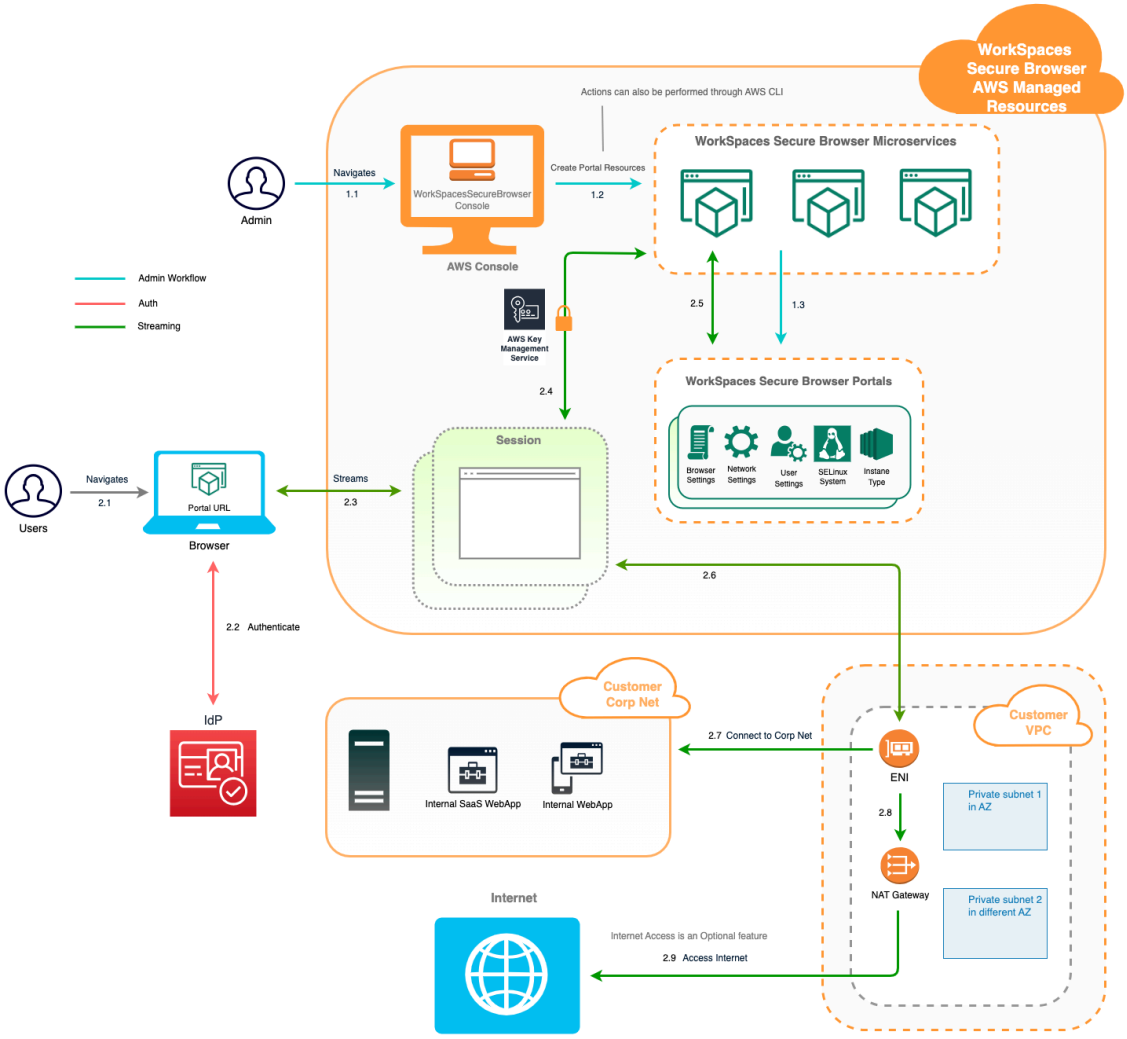
AWS servizi relativi ad Amazon WorkSpaces Secure Browser

Esistono diversi AWS servizi correlati a WorkSpaces Secure Browser.

WorkSpaces Secure Browser è una funzionalità di Amazon WorkSpaces nel portafoglio AWS End User Computing. Rispetto a WorkSpaces e AppStream 2.0, WorkSpaces Secure Browser è progettato specificamente per facilitare carichi di lavoro sicuri basati sul Web. WorkSpaces Secure Browser 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 WorkSpaces Secure Browser agli utenti del contact center che devono accedere solo a una manciata di siti Web interni e SaaS (compresi quelli ospitati all'esterno della rete) su computer desktop.

Architettura di Amazon WorkSpaces Secure Browser

Il diagramma seguente mostra l'architettura di WorkSpaces Secure Browser.



Accesso ad Amazon WorkSpaces Secure Browser

Puoi accedere a WorkSpaces Secure Browser in diversi modi.

Gli amministratori accedono a WorkSpaces Secure Browser tramite WorkSpaces Secure Browser Console, SDK, CLI o API. I tuoi utenti vi accedono tramite l'endpoint WorkSpaces Secure Browser.

Configurazione di Amazon WorkSpaces Secure Browser

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

Argomenti

- Registrazione e creazione di un utente
- Concessione dell'accesso programmatico
- Rete per Amazon WorkSpaces Secure Browser

Registrazione e creazione di un utente

Registrati per un Account AWS

Per iniziare AWS, hai bisogno di un Account AWS. Per informazioni sulla creazione di un Account AWS, vedi Guida introduttiva a un Account AWS nella Guida Gestione dell'account AWS di riferimento.

Concessione dell'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS Console di gestione AWS esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

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

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza le credenziali della console come credenziali temporanee per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Login for AWS local development nella Guida

Quale utente necessita dell'accesso programmatico?	Per	Come
		per l'utente.AWS Command Line Interface • Per gli AWS SDK, consulta Login per lo sviluppo AWS locale nella Guida di riferimento agli AWS SDK e agli strumenti.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS SDK o alle AWS CLI API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso Centro identità AWS IAM nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Rete per Amazon WorkSpaces Secure Browser

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

Argomenti

- Configurazione di un VPC per Amazon Secure Browser WorkSpaces
- Abilitazione delle connessioni utente per Amazon WorkSpaces Secure Browser

Configurazione di un VPC per Amazon Secure Browser WorkSpaces

Per impostare e configurare un VPC per WorkSpaces Secure Browser, completa i seguenti passaggi.

Argomenti

- Requisiti VPC per Amazon Secure Browser WorkSpaces
- Creazione di un nuovo VPC per Amazon Secure Browser WorkSpaces
- Abilitazione della navigazione in Internet per Amazon WorkSpaces Secure Browser
- Le migliori pratiche VPC per WorkSpaces Secure Browser
- Zone di disponibilità supportate per Amazon WorkSpaces Secure Browser

Requisiti VPC per Amazon Secure Browser WorkSpaces

Durante la creazione del portale WorkSpaces Secure Browser, 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 tue sottoreti devono avere indirizzi IP sufficienti per supportare il traffico WorkSpaces Secure Browser previsto. 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 di un nuovo VPC per Amazon Secure Browser WorkSpaces.
- 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 con Secure Browser. WorkSpaces

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

WorkSpaces Secure Browser 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 Secure Browser abbia accesso sia ai contenuti Internet

pubblici che ai contenuti VPC privati, completa i passaggi seguenti. Attivazione della navigazione Internet senza restrizioni per Amazon WorkSpaces Secure Browser (consigliato)

Creazione di un nuovo VPC per Amazon Secure Browser WorkSpaces

Questa sezione descrive come utilizzare la procedura guidata VPC per creare rapidamente un VPC con sottoreti pubbliche e private. La procedura guidata crea automaticamente un gateway Internet, un gateway NAT e configura le tabelle di routing per le sottoreti.

Per ulteriori informazioni su questa configurazione, consulta VPC con sottoreti pubbliche e private (NAT).

Argomenti

- Configurazione rapida del VPC (1 minuto)
- Verifica delle tabelle di routing della sottorete (opzionale)

Configurazione rapida del VPC (1 minuto)

Completa i seguenti passaggi per creare rapidamente un VPC dedicato per WorkSpaces Secure Browser con sottoreti pubbliche e private per l'accesso a Internet. Se desideri utilizzare un VPC esistente, consulta Requisiti VPC per Amazon Secure Browser WorkSpaces per verificare che soddisfi i requisiti.

> **Note**
>
> Assicurati di essere nella posizione desiderata. Regione AWS Se necessario, puoi cambiare la regione nella console.

Per configurare rapidamente un VPC

1. Apri la procedura guidata per la creazione di VPC: crea VPC con risorse. Mantieni tutte le impostazioni come predefinite, a meno che non sia specificato di seguito:
   - Per Risorsa da creare, seleziona VPC e altro.
   - Per Tag nome, seleziona la generazione automatica e inserisci un nome descrittivo per il tuo VPC (ad esempio,). **`WSB-VPC`**
   - Per il blocco CIDR IPv4, per impostazione predefinita, il VPC utilizza. **`10.0.0.0/16`** È possibile specificare un blocco CIDR IPv4 diverso, se necessario.

- Per Tenancy, seleziona Predefinito (i VPC con tenancy dedicata non sono supportati).
- Per Numero di zone di disponibilità (AZ), seleziona 2.
  - Espandi Personalizza le AZ e seleziona 2 diverse zone di disponibilità supportate da WorkSpaces Secure Browser. Per l'elenco delle AZ supportate, consulta. Zone di disponibilità supportate per Amazon WorkSpaces Secure Browser
- Per Numero di sottoreti pubbliche, selezionare 2.
- Per Numero di sottoreti private, selezionare 2.
- Per i blocchi CIDR di sottorete, se è necessario personalizzare i blocchi CIDR nelle sottoreti, espandi Personalizza sottoreti (blocchi CIDR). Assicurati che ogni sottorete abbia indirizzi IP sufficienti per il traffico previsto.
- Per i gateway NAT, seleziona Regionale per abilitare l'accesso a Internet per le sottoreti private in tutte le zone di disponibilità.
- Per gli endpoint VPC, seleziona Nessuno. Se hai bisogno di un accesso diretto a S3 senza passare dal gateway NAT, seleziona S3 Gateway.
- Per quanto riguarda le opzioni DNS, mantieni le opzioni DNS abilitate (impostazione predefinita) per garantire la corretta risoluzione dei nomi all'interno del tuo VPC.

2. Esamina il riquadro di anteprima, quindi scegli Crea VPC.

> **Note**
>
> Sono previsti costi aggiuntivi per i gateway NAT e gli endpoint VPC. Per ulteriori informazioni, consulta la pagina dei prezzi del VPC.

Verifica delle tabelle di routing della sottorete (opzionale)

La procedura guidata VPC configura automaticamente le tabelle di routing per te. Se hai creato il tuo VPC manualmente o desideri confermare la configurazione, puoi 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 pannello di navigazione, scegli Subnet, quindi seleziona una sottorete pubblica. Ad esempio, WSB-VPC-subnet-public1-us-east-1a.
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	Description
Subnet pubblica (blocco CIDR) IPv4 (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 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 riquadro di navigazione, seleziona Sottoreti. Quindi, seleziona una sottorete privata (ad esempio,**`WSB-VPC-subnet-private1-us-east-1a`**).

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 **`WSB-VPC-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	Description
Blocco CIDR IPv4 di 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) [pl-ID (com.amazonaws.region.s3)]	Archiviazione (vpce-ID)	Il traffico destinato ai bucket S3 viene instradato all'endpoint S3 (identificato da vpce-ID).

9. Nel riquadro di navigazione, seleziona Sottoreti. Quindi seleziona la seconda sottorete privata che hai creato (ad esempio, **`WorkSpaces Secure Browser 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.

Abilitazione della navigazione in Internet per Amazon WorkSpaces Secure Browser

È possibile scegliere di abilitare la navigazione Internet senza restrizioni (l'opzione consigliata) o la navigazione Internet con restrizioni.

Argomenti

- Attivazione della navigazione Internet senza restrizioni per Amazon WorkSpaces Secure Browser (consigliato)
- Attivazione della navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser
- Porte di connettività Internet per Amazon WorkSpaces Secure Browser

Attivazione della navigazione Internet senza restrizioni per Amazon WorkSpaces Secure Browser (consigliato)

Per configurare un VPC con un gateway NAT per una navigazione Internet senza restrizioni, segui la procedura illustrata qui. Ciò garantisce l'accesso tramite WorkSpaces Secure Browser ai siti su Internet pubblico 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 Secure Browser 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 di un nuovo VPC per Amazon Secure Browser WorkSpaces.

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 un VPC con sottoreti private, vedere. the section called “Configurazione rapida VPC”

   > **Note**
   >
   > Per assicurarti che ogni istanza di streaming abbia accesso a Internet, non collegare una sottorete pubblica al tuo WorkSpaces portale Secure Browser.

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 Configurare le tabelle di routing.

Attivazione della navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser

La configurazione di rete consigliata di un portale WorkSpaces Secure Browser prevede l'utilizzo di 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 “Navigazione Internet senza restrizioni”. Tuttavia, potrebbe essere necessario controllare le comunicazioni in uscita da un portale WorkSpaces Secure Browser verso 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 dimestichezza 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 Secure Browser, puoi configurare le impostazioni proxy utilizzando i criteri di Chrome integrati nel browser web. Puoi farlo configurando un proxy HTTP in uscita per WorkSpaces Secure Browser.

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 Secure Browser per configurare il portale WorkSpaces Secure Browser 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.

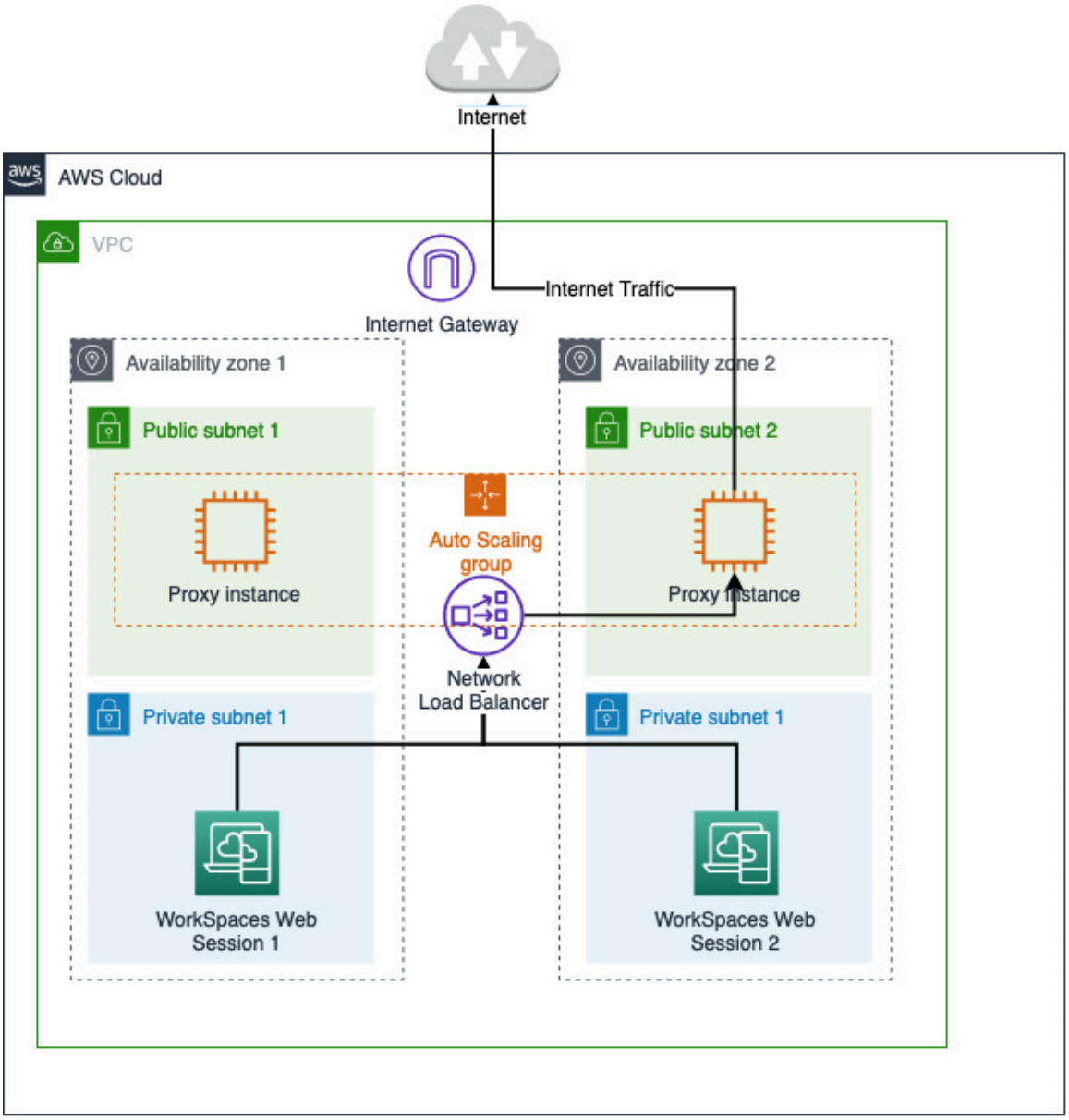
- Un portale WorkSpaces Secure Browser distribuito su sottoreti private. Non è necessario configurare il gateway NAT per abilitare l'accesso a Internet. È invece necessario configurare la politica del browser, in modo che tutto il traffico Internet passi attraverso il proxy in uscita. Se desideri utilizzare il tuo proxy, la configurazione del portale WorkSpaces Secure Browser sarà simile.

Argomenti

- Architettura di navigazione Internet limitata per Amazon WorkSpaces Secure Browser
- Prerequisiti di navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser
- Proxy HTTP in uscita per Amazon WorkSpaces Secure Browser
- Risoluzione dei problemi di navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser

Architettura di navigazione Internet limitata per Amazon WorkSpaces Secure Browser

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 di Secure Browser. WorkSpaces



Prerequisiti di navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser

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, dove risiedono le sessioni di WorkSpaces Secure Browser (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.

Proxy HTTP in uscita per Amazon WorkSpaces Secure Browser

Per configurare un proxy HTTP in uscita per WorkSpaces Secure Browser, 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 Secure Browser, 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 di WorkSpaces Secure Browser, vedrai che il proxy viene applicato all'impostazione Chrome che utilizza le impostazioni proxy dell'amministratore.
4. Vai a chrome: //policy e alla scheda Chrome policy per confermare che la policy sia applicata.

5. Verifica che la tua sessione WorkSpaces Secure Browser sia in grado di navigare correttamente nei contenuti Internet senza il gateway NAT. Nei CloudWatch registri, verifica che i log di accesso al proxy Squid siano registrati.

Risoluzione dei problemi di navigazione Internet con restrizioni per Amazon WorkSpaces Secure Browser

Dopo aver applicato i criteri di Chrome, se la sessione del WorkSpaces Secure Browser continua a non riuscire 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 portale WorkSpaces Secure Browser. 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 Secure Browser, usa Chrome per accedere a chrome: //policy e assicurati che il ProxySettings criterio sia applicato correttamente.

Porte di connettività Internet per Amazon WorkSpaces Secure Browser

Ogni istanza di streaming WorkSpaces Secure Browser 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

Le migliori pratiche VPC per WorkSpaces Secure Browser

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 Secure Browser (note anche come limiti) siano sufficienti a soddisfare la tua domanda prevista. Per richiedere un aumento della quota, puoi utilizzare la console Service Quotas all'indirizzo. https://console.aws.amazon.com/servicequotas/ Per informazioni sulle quote predefinite di WorkSpaces Secure Browser, vedere. the section called “Gestione delle quote 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 di WorkSpaces Secure Browser richiede la propria interfaccia di rete elastica per tutta la durata dello streaming. WorkSpaces Secure Browser 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

- Mentre sviluppate il vostro piano di ampliamento degli utenti, tenete presente che ogni sessione di WorkSpaces Secure Browser 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.

- Ti consigliamo di configurare una sottorete in ogni zona di disponibilità unica supportata da WorkSpaces Secure Browser nella regione desiderata per tenere conto della disponibilità e della scalabilità. Per ulteriori informazioni, consulta the section called “Creare 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 Secure Browser 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 per Amazon WorkSpaces Secure Browser

Quando crei un cloud privato virtuale (VPC) da utilizzare con WorkSpaces Secure Browser, le sottoreti del tuo VPC devono risiedere in diverse zone di disponibilità nella regione in cui stai avviando Secure Browser. 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 `us-east-1` regione 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 Secure Browser 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 della Regione	Codice regione	ID AZ supportati
Stati Uniti orientali (Virginia settentrionale)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
Stati Uniti occidentali (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asia Pacifico (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-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`

Nome della Regione	Codice regione	ID AZ supportati
Europa (Londra)	`eu-west-2`	`euw2-az1`, `euw2-az2`

Per ulteriori informazioni su Availability Zones e AZ ID, consulta Regions, Availability Zones and Local Zones nella Amazon EC2 User Guide.

Abilitazione delle connessioni utente per Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser 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 necessarie per il funzionamento di WorkSpaces Secure Browser. Per consentire questo traffico, è necessario autorizzare i domini elencati in Domini consentiti per Amazon WorkSpaces Secure Browser.

I seguenti argomenti forniscono informazioni su come abilitare le connessioni degli utenti a WorkSpaces Secure Browser.

Argomenti

- Requisiti relativi all'indirizzo IP e alla porta per Amazon WorkSpaces Secure Browser
- Domini consentiti per Amazon WorkSpaces Secure Browser

Requisiti relativi all'indirizzo IP e alla porta per Amazon WorkSpaces Secure Browser

Per accedere alle istanze WorkSpaces Secure Browser, 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 per Amazon WorkSpaces Secure Browser.

  - AWS pubblica 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 utilizza AWS 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 Amazon WorkSpaces Secure Browser

Affinché gli utenti possano accedere ai portali Web dal browser locale, è necessario aggiungere i seguenti domini all'elenco dei domini consentiti sulla rete da cui l'utente sta tentando di accedere al servizio.

Nella tabella seguente, sostituiscilo *{region}* con il codice della regione del portale web operativo. Ad esempio, s3. *{region}*.amazonaws.com dovrebbe essere s3.eu-west-1.amazonaws.com per un portale web nella regione Europa (Irlanda). Per un elenco dei codici regionali, consulta Endpoint e quote di Amazon WorkSpaces Secure Browser.

Categoria	Dominio o indirizzo IP
WorkSpaces Risorse di streaming Secure Browser	s3. *{region}*.amazonaws.com s3.amazonaws.com appstream 2. *{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Risorse statiche Secure Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net

Categoria	Dominio o indirizzo IP
WorkSpaces Autenticazione sicura del browser	*.auth. *{region}*.amazoncognito.com identità cognitiva. *{region}*.amazonaws.com cognito-idp. *{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Metriche e report sicuri del browser	*.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 elencare per consentire a WorkSpaces Secure Browser di utilizzare quel provider. Se utilizzi IAM Identity Center, consulta i prerequisiti di IAM Identity Center per ulteriori informazioni.

Guida introduttiva ad Amazon WorkSpaces Secure Browser

Segui questi passaggi per creare un portale web WorkSpaces Secure Browser 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 Secure Browser offre pay-as-you-go prezzi, tra cui 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 Secure Browser.

Argomenti

- Creazione di un portale Web per Amazon WorkSpaces Secure Browser
- Verifica del tuo portale web in Amazon WorkSpaces Secure Browser
- Distribuzione del tuo portale web in Amazon WorkSpaces Secure Browser

Creazione di un portale Web per Amazon WorkSpaces Secure Browser

Per creare un portale web, segui queste fasi:

Argomenti

- Configurazione delle impostazioni di rete per Amazon WorkSpaces Secure Browser
- Configurazione delle impostazioni del portale per Amazon WorkSpaces Secure Browser
- Configurazione delle impostazioni utente per Amazon WorkSpaces Secure Browser
- Configurazione del tuo provider di identità per Amazon WorkSpaces Secure Browser
- Avvio di un portale Web con Amazon WorkSpaces Secure Browser

Configurazione delle impostazioni di rete per Amazon WorkSpaces Secure Browser

Per configurare le impostazioni di rete per WorkSpaces Secure Browser, segui questi passaggi.

1. Apri la console WorkSpaces Secure Browser a https://console.aws.amazon.com/workspaces-web/casa.
2. Scegli WorkSpaces Secure Browser, 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 con WorkSpaces Secure Browser.
    2. Scegli fino a tre sottoreti private che soddisfino i seguenti requisiti. Per ulteriori informazioni, consulta Rete per Amazon WorkSpaces Secure Browser.
        - 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.

Configurazione delle impostazioni del portale per Amazon WorkSpaces Secure Browser

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 Tipo di istanza, seleziona il tipo di istanza per il tuo portale web dal menu a discesa. Quindi, inserisci il limite massimo di utenti simultanei per il portale web. Per ulteriori informazioni, consulta the section called “Gestione delle quote di servizio”.

   > **Note**
   >
   > La selezione di un nuovo tipo di istanza modificherà il costo per ogni utente attivo mensile. Per ulteriori informazioni, consulta i prezzi di Amazon WorkSpaces Secure Browser.

3. In Dominio personalizzato, puoi configurare un dominio personalizzato per il tuo portale per consentire l'accesso tramite il tuo nome di dominio anziché l'endpoint predefinito del portale. Per ulteriori informazioni, consulta the section called “Dominio personalizzato”. Questo è facoltativo.
4. In Session Logger, puoi specificare un bucket S3 per archiviare i file di registro delle sessioni. Per ulteriori informazioni, consulta the section called “Configurazione di Session Logger”. Questo è facoltativo.
5. In Registrazione degli accessi utente, per Kinesis stream ID, seleziona il flusso di dati Amazon Kinesis a cui desideri inviare i file di log. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione delle attività degli utenti”. Questo è facoltativo.
6. In Controllo dell'accesso IP, scegli se limitare l'accesso a reti affidabili. Per ulteriori informazioni, consulta the section called “Gestione dei controlli di accesso IP”. Questa operazione è facoltativa.
7. In Impostazioni di protezione dei dati, puoi creare politiche per WorkSpaces Secure Browser per oscurare le informazioni sensibili. Per ulteriori informazioni, consulta the section called “Impostazioni di protezione dei dati”. Questo è facoltativo.
8. Nel filtro URL, puoi specificare a quali utenti URLs finali è consentito accedere o bloccare categorie specifiche URLs o di dominio per limitare l'accesso. Per ulteriori informazioni, consulta the section called “Filtraggio dei contenuti Web”. Questo è facoltativo.

   1. Per limitare la navigazione della sessione a pochi domini selezionati, attiva l'opzione Blocca tutto URLs e fai clic su aggiungi URL per visualizzare l'elenco degli utenti finali a cui è consentito URLs l'accesso.

2. Per creare un elenco URLs da bloccare per gli utenti finali, fai clic su Aggiungi URL per elencare il singolo URLs da bloccare o fai clic su Aggiungi categorie per selezionare le categorie di domini bloccati (ad esempio, social network).

9. In Impostazioni delle norme, puoi impostare qualsiasi criterio del browser utilizzando i criteri di Chrome disponibili per l'ultima versione stabile del portale web. Per ulteriori informazioni, consulta the section called “Gestione della politica del browser”. Questo è facoltativo.

   1. È possibile selezionare rapidamente alcune delle politiche più comuni nell'editor Visual

      - 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**
      >
      > URLs i visitatori 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 delle attività degli utenti”.

      - 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 loro 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.

   2. Puoi anche aggiungere o modificare direttamente le politiche utilizzando l'editor JSON anziché l'editor visuale. Per il formato specifico di una policy, consulta l'elenco delle policy di Chrome Enterprise.
   3. Puoi anche importare le politiche di Chrome utilizzate nella tua organizzazione caricando un file JSON nel portale web. Per i dettagli, consulta the section called “Tutorial: impostazione di una politica del browser personalizzata”

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.

10. Aggiungi tag al tuo portale. Puoi utilizzare i tag per cercare o filtrare AWS le tue risorse. I tag sono costituiti da un valore chiave e facoltativo e sono associati alla risorsa del portale. Questo è facoltativo.
11. Seleziona Successivo per continuare.

Configurazione delle impostazioni utente per Amazon WorkSpaces Secure Browser

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. Nella sezione Personalizzazione del marchio, puoi personalizzare le schermate di accesso e caricamento visualizzate dagli utenti finali modificando gli elementi visivi, il contenuto testuale e i termini di servizio. Per ulteriori informazioni, consulta the section called “Personalizzazione del branding”. Questa operazione è facoltativa.
2. In Autorizzazioni, scegli se abilitare l'estensione per il Single Sign-On. Per ulteriori informazioni, consulta the section called “Gestione dell'estensione Single Sign-On”.
3. Per Consenti agli utenti di stampare su un dispositivo locale dal loro portale web, scegli Consentita o Non consentita.
4. Per Consenti agli utenti di creare collegamenti diretti al loro portale web, scegli Consentito o Non consentito. Per ulteriori informazioni sui link diretti, consulta. the section called “Deep link”
5. Per Consenti agli utenti di utilizzare l'autenticazione locale nella sessione del portale, scegli Consentita o Non consentita. Per ulteriori informazioni sull'autenticazione web, consultathe section called “Reindirizzamento dell'autenticazione Web”.
6. In Controlli della barra degli strumenti, scegli le impostazioni che desideri in Funzionalità.
7. In Impostazioni, gestisci la visualizzazione della presentazione della barra degli strumenti all'inizio della sessione, incluso lo stato della barra degli strumenti (ancorata o scollegata), il tema (modalità scura o chiara), la visibilità delle icone e la risoluzione massima dello schermo per la sessione. Lascia queste impostazioni non configurate per concedere agli utenti finali il pieno

controllo su queste opzioni. Per ulteriori informazioni, consulta the section called “Controlli della barra degli strumenti”.

8. Per i timeout delle sessioni, 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. Altrimenti, sono 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 utilizzata dall'utente 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 vengono avvisati prima di essere disconnessi per 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 collegati 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 vengono considerati inattivi quando smettono di fornire input da tastiera o mouse durante la sessione 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 del tuo provider di identità per Amazon WorkSpaces Secure Browser

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

Argomenti

- Scelta del tipo di provider di identità per Amazon WorkSpaces Secure Browser
- Modifica del tipo di provider di identità per Amazon WorkSpaces Secure Browser

Scelta del tipo di provider di identità per Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser offre due tipi di autenticazione: Standard e Centro identità AWS IAM. 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 “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, il portale IAM Identity Center e WorkSpaces Secure Browser devono risiedere entrambi nello stesso. Regione AWS Per ulteriori informazioni, consulta the section called “Tipo di autenticazione IAM Identity Center”.

Argomenti

- Configurazione del tipo di autenticazione standard per Amazon WorkSpaces Secure Browser
- Configurazione del tipo di autenticazione IAM Identity Center per Amazon WorkSpaces Secure Browser

Configurazione del tipo di autenticazione standard per Amazon WorkSpaces Secure Browser

Il tipo di autenticazione standard è il tipo di autenticazione predefinito. Può supportare flussi di accesso avviati dal provider di servizi (iniziati da SP) e avviati dal provider di identità (avviati da IdP) con il tuo IdP conforme a SAML 2.0. Per configurare il tipo di autenticazione standard, segui i passaggi seguenti per federare il tuo IdP SAML 2.0 di terze parti (come Okta o Ping) direttamente con il tuo portale.

Argomenti

- Configurazione del tuo provider di identità su Amazon WorkSpaces Secure Browser
- Configurazione del tuo IdP sul tuo IdP
- Completamento della configurazione IdP su Amazon WorkSpaces Secure Browser
- Linee guida per l'utilizzo specifico IdPs con Amazon WorkSpaces Secure Browser

Configurazione del tuo provider di identità su Amazon WorkSpaces Secure Browser

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 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 Secure Browser. 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 dalla sessione IdP WorkSpaces che da quella di Secure Browser con un'unica azione.
   a. Scarica il certificato di firma da WorkSpaces Secure Browser 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.

Configurazione del tuo IdP sul tuo IdP

Per configurare il tuo IdP sul tuo IdP, segui questi passaggi.

1. Apri una nuova scheda nel browser.
2. 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 specifiche IdPs”Per assistenza su come aggiungere i dettagli del portale alla configurazione del tuo IdP, consulta la documentazione del tuo provider.
3. 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.
4. 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 “Configurazione IdP su WorkSpaces Secure Browser” per la tua applicazione IdP.
5. 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 “Configurazione IdP su WorkSpaces Secure Browser” 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.

6. 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.
7. Facoltativo: configura Single Logout. Se hai scelto Single Logout, segui i passaggi indicati nel passaggio 5 the section called “Configurazione IdP su WorkSpaces Secure Browser” per caricare il certificato di firma sul tuo IdP, inserire Single Logout URL e abilitare Single Logout.
8. Concedi l'accesso ai tuoi utenti nel tuo IdP per utilizzare WorkSpaces Secure Browser.
9. Scarica un file di scambio di metadati dal tuo gestore dell'identità digitale. Caricherai questi metadati su WorkSpaces Secure Browser nel passaggio successivo.

Completamento della configurazione IdP su Amazon WorkSpaces Secure Browser

Per completare la configurazione IdP su WorkSpaces Secure Browser, segui questi passaggi.

1. Torna alla console WorkSpaces Secure Browser. 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.
2. 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.
3. 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 Secure Browser e, in URL dei metadati IdP, inserisci l'URL dei metadati che hai ottenuto dal tuo IdP.
4. Al termine, seleziona Next (Avanti).
5. 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 lì.

> **Note**
>
> WorkSpaces Secure Browser 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 Secure Browser richiede che le seguenti affermazioni siano presenti nella risposta SAML. Puoi trovare *<Your SP Entity ID>* e consultare i dettagli *<Your SP ACS URL>* 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 Secure Browser 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 l'utilizzo specifico IdPs con Amazon WorkSpaces Secure Browser

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 Enterprise PingOne	PingOne For Enterprise supporta la crittografia?	Disconnessione singola SAML 2.0
Un solo accesso	Connettore personalizzato	Aggiungi utenti a Manualmen	Connettore personalizzato	Connettore personalizzato	Connettore personalizzato	Connettore personalizzato

IdP	Configurazione dell'applicazione SAML	Gestione degli utenti	Autenticazione avviata da IDP	Richiedi la firma	Crittografia delle asserzioni	Disconnessione singola
	SAML (avanzato) (4266907)	te OneLogin	SAML (avanzato) (4266907)	SAML (avanzato) (4266907)	SAML (avanzato) (4266907)	SAML (avanzato) (4266907)
Centro identità IAM	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

Configurazione del tipo di autenticazione IAM Identity Center per Amazon WorkSpaces Secure Browser

Per il tipo IAM Identity Center (avanzato), federate IAM Identity Center con il vostro 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 Secure Browser. 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 “Tipo di autenticazione standard”.
Se lo utilizzi AWS Organizations, puoi creare solo portali WorkSpaces Secure Browser integrati con IAM Identity Center utilizzando un account di gestione.

Argomenti

- Creazione di un portale web con IAM Identity Center
- Gestione del portale web con IAM Identity Center
- Aggiungere utenti e gruppi aggiuntivi a un portale web
- Visualizzazione o rimozione di utenti e gruppi per il portale web

Creazione di un portale web con IAM Identity Center

Per creare un portale web con IAM Identity Center, segui questi passaggi.

Per creare un portale web con IAM Identity Center

1. Durante la creazione del portale, allo Step 4: Configura il provider di identità, scegli Centro identità AWS IAM.
2. Scegli Continua con IAM Identity Center.
3. Nella pagina Assegna utenti e gruppi, scegli la scheda and/or Gruppi di utenti.
4. Seleziona la casella accanto agli utenti o ai gruppi che desideri aggiungere al portale.
5. Dopo aver creato il portale, gli utenti associati possono accedere a WorkSpaces Secure Browser con il nome utente e la password di IAM Identity Center.

Gestione del portale web con IAM Identity Center

Per gestire il tuo portale web con IAM Identity Center, segui questi passaggi.

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.

Aggiungere utenti e gruppi aggiuntivi a un portale web

Per aggiungere altri utenti e gruppi a un portale Web esistente, procedi nel seguente modo.

Per aggiungere altri utenti e gruppi a un portale web esistente

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

Visualizzazione o rimozione di utenti e gruppi per il portale web

Per visualizzare o rimuovere utenti e gruppi dal portale Web, utilizzate le azioni disponibili nella tabella Utenti assegnati. Per ulteriori informazioni, consulta Gestire l'accesso alle applicazioni

> **Note**
>
> Non puoi visualizzare o rimuovere utenti e gruppi dalla pagina di modifica del WorkSpaces Secure Browserportal. È necessario eseguire questa operazione dalla pagina di modifica della console IAM Identity Center.

Modifica del tipo di provider di identità per Amazon WorkSpaces Secure Browser

Puoi modificare il tipo di autenticazione del tuo portale in qualsiasi momento. Per fare ciò, segui questi passaggi.

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

Avvio di un portale Web con Amazon WorkSpaces Secure Browser

Quando hai finito di configurare il tuo portale web, puoi seguire questi passaggi per avviarlo.

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.

Verifica del tuo portale web in Amazon WorkSpaces Secure Browser

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

Se hai già completato questi passaggi in the section called “Configurazione del provider di identità”, puoi ignorare questa sezione e andare su Distribuzione del tuo portale web in Amazon WorkSpaces Secure Browser.

1. Aprire la console WorkSpaces Secure Browser a https://console.aws.amazon.com/workspaces-web/casa? region=us-east-1#/.
2. Scegli WorkSpaces Secure Browser, Web portals, 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 a WorkSpaces Secure Browser, scegli Accedi, SAML e inserisci le tue credenziali SAML.
5. Quando vedi la pagina La tua sessione è in preparazione, la sessione WorkSpaces Secure Browser 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 URLs accedendo alla barra degli indirizzi.

Distribuzione del tuo portale web in Amazon WorkSpaces Secure Browser

Quando sei pronto per consentire ai tuoi utenti di iniziare a utilizzare WorkSpaces Secure Browser, scegli 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. Puoi farlo tramite il flusso di accesso avviato dall'IdP con il tuo IdP conforme a SAML 2.0. Per ulteriori informazioni, consulta Asserzioni SAML iniziate da SP e IdP in. the section called “Tipo di autenticazione standard” In alternativa, puoi creare un'applicazione SAML personalizzata in grado di fornire esperienze di autenticazione avviate da IdP utilizzando flussi avviati da SP. Per ulteriori informazioni, 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.
- Utilizza un dominio personalizzato se ne hai configurato uno per il tuo portale anziché l'URL del portale per un'esperienza di branding più integrata per i tuoi utenti. Per ulteriori informazioni, consulta the section called “Dominio personalizzato”.

Gestione del portale Web in Amazon WorkSpaces Secure Browser

Dopo aver configurato il portale web, puoi eseguire le seguenti azioni per gestirlo.

Argomenti

- Visualizzazione dei dettagli del portale Web in Amazon WorkSpaces Secure Browser
- Modifica di un portale Web in Amazon WorkSpaces Secure Browser
- Eliminazione di un portale Web in Amazon WorkSpaces Secure Browser
- Gestione delle quote di servizio per il tuo portale in Amazon WorkSpaces Secure Browser
- Controllo dell'intervallo per la riautenticazione di un token IdP SAML in Amazon Secure Browser WorkSpaces
- Configurazione della registrazione delle attività degli utenti in Amazon WorkSpaces Secure Browser
- Gestione delle policy del browser in Amazon WorkSpaces Secure Browser
- Configurazione dell'Input Method Editor per Amazon WorkSpaces Secure Browser
- Configurazione della localizzazione in sessione per Amazon Secure Browser WorkSpaces
- Gestione dei controlli di accesso IP in Amazon WorkSpaces Secure Browser
- Gestione dell'estensione Single Sign-On in Amazon Secure Browser WorkSpaces
- Filtraggio dei contenuti Web in Amazon WorkSpaces Secure Browser
- Collegamenti diretti in Amazon WorkSpaces Secure Browser
- Utilizzo della dashboard di gestione delle sessioni in Amazon WorkSpaces Secure Browser
- Protezione dei dati in transito con endpoint FIPS e Amazon Secure Browser WorkSpaces
- Gestione delle impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser
- Personalizzazione del marchio in Amazon Secure Browser WorkSpaces
- Abilitazione del supporto WebAuthn per il reindirizzamento in Amazon WorkSpaces Secure Browser
- Gestione dei controlli della barra degli strumenti in Amazon WorkSpaces Secure Browser
- Configurazione di un dominio personalizzato per il portale

Visualizzazione dei dettagli del portale Web in Amazon WorkSpaces Secure Browser

Per visualizzare i dettagli del portale Web, procedi nel seguente modo.

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

Modifica di un portale Web in Amazon WorkSpaces Secure Browser

Per modificare un portale web, segui questi passaggi.

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Secure Browser, Web portals, scegli il tuo portale web, quindi scegli 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 in Amazon WorkSpaces Secure Browser

Per eliminare un portale web, segui questi passaggi.

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Secure Browser, Web portals, scegli il tuo portale web, quindi scegli Elimina.

Gestione delle quote di servizio per il tuo portale in Amazon WorkSpaces Secure Browser

Quando crei le tue Account AWS, impostiamo automaticamente le quote di servizio predefinite (note anche come limiti) per l'utilizzo delle risorse con. Servizi AWS Gli amministratori devono essere consapevoli dell'esistenza di due quote che potrebbero dover essere aumentate per supportare il loro caso d'uso. Queste due quote rappresentano il numero di portali Web che è possibile creare in ogni regione e il numero massimo di sessioni simultanee che è possibile supportare con ogni tipo di istanza disponibile in ogni regione. Puoi richiederne un aumento dalla pagina Service Quotas della Console. AWS

La tabella seguente elenca i limiti predefiniti delle quote di servizio.

Quote predefinite all'interno e per account Regione AWS	Valore
Portali Web	3
Numero massimo di sessioni simultanee: standard.regular	25
Numero massimo di sessioni simultanee: standard.large	10
Numero massimo di sessioni simultanee: standard.xlarge	5

Per visualizzare le quote di servizio assegnate al tuo account per ciascuna regione in qualsiasi momento, consulta la pagina Service Quotas.

> **Important**
>
> Le quote di servizio influiscono su una Regione AWS alla volta. È necessario richiedere aumenti delle quote di servizio in tutti i casi in Regione AWS cui sono necessarie più risorse. Per ulteriori informazioni, endpoint e quote Amazon WorkSpaces Secure Browser.

Argomenti

- Richiesta di un aumento della quota di servizio in Amazon WorkSpaces Secure Browser
- Richiesta di un aumento del portale in Amazon WorkSpaces Secure Browser
- Richiesta di un aumento massimo delle sessioni simultanee in Amazon Secure Browser WorkSpaces
- Esempio di limite per Amazon WorkSpaces Secure Browser
- Altre quote di servizio in Amazon WorkSpaces Secure Browser

Richiesta di un aumento della quota di servizio in Amazon WorkSpaces Secure Browser

Per richiedere un aumento della quota di servizio, segui questi passaggi.

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

   > **Important**
   >
   > WorkSpaces Le quote del servizio Secure Browser riguardano 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.

Richiesta di un aumento del portale in Amazon WorkSpaces Secure Browser

Un portale è la risorsa fondamentale del servizio. Ogni portale è un'associazione tra il tuo provider di identità SAML 2.0 e la tua connessione di rete a Internet e qualsiasi contenuto web privato. Ogni portale può avere una politica del browser del portale e impostazioni utente separate, quindi gli amministratori generalmente creano più portali nella stessa regione per affrontare diversi casi d'uso. Ad esempio, è possibile fornire al Gruppo A l'accesso a un sito Web specifico con politiche restrittive (ad esempio, Appunti e trasferimento di file disabilitati) e al Gruppo B l'accesso a Internet generale senza filtri URL. È possibile creare un portale in qualsiasi formato supportato. Regione AWS Per visualizzare la disponibilità attuale del servizio, consulta Servizi AWS per regione.

Come richiedere un aumento della quota di servizio

1. Apri la pagina Service Quotas nella regione desiderata.
2. Scegli il numero di portali Web.
3. Scegli Richiedi un aumento a livello di account.
4. In Aumenta il valore della quota, inserisci l'importo totale che desideri che sia la quota.

Richiesta di un aumento massimo delle sessioni simultanee in Amazon Secure Browser WorkSpaces

La quota massima di sessioni simultanee è il numero massimo di utenti che possono essere connessi contemporaneamente a un portale. Se il limite di quota di servizio per il numero massimo di sessioni simultanee non è impostato in modo appropriato, gli utenti potrebbero scoprire che una sessione non è disponibile al momento dell'accesso. Oltre ad aumentare questa quota di servizi, i clienti devono anche assicurarsi che il VPC e le sottoreti dispongano di spazio IP sufficiente per supportare il numero massimo di sessioni simultanee.

Per richiedere un aumento massimo della sessione simultanea

1. Apri la pagina Service Quotas nella regione desiderata.

2. Scegli il numero massimo di sessioni simultanee per portale per il tipo di istanza che desideri aumentare.
3. Scegli Richiedi un aumento a livello di account.
4. In Aumenta il valore della quota, inserisci l'importo totale che desideri che sia la quota.

> **Note**
>
> Per aumenti ingenti o urgenti, vai alla pagina della cronologia di Service Quotas, seleziona il link nella colonna di stato della richiesta, collega al tuo caso di assistenza e aggiungi una risposta con i dettagli sul tuo caso d'uso, and/or l'urgenza. Queste informazioni aiutano il team di assistenza a dare priorità alle richieste e a garantire che venga allocata una capacità sufficiente per l'account.

Esempio di limite per Amazon WorkSpaces Secure Browser

Ad esempio, supponiamo che un amministratore stia configurando due portali web negli Stati Uniti orientali (Virginia settentrionale) per un totale di 125 utenti. Prima di creare il portale Web, l'amministratore identifica il primo portale Web (Portal A) che supporterà 100 utenti. Durante il test del flusso di lavoro per questi utenti, l'amministratore stabilisce che avranno bisogno del tipo di istanza XL per supportare lo streaming di audio e video durante la sessione. Il secondo portale Web (Portal B) deve essere disponibile per un massimo di 25 utenti per supportare l'accesso a una singola pagina Web statica ospitata nel VPC del cliente. Durante il test di questo caso d'uso, l'amministratore stabilisce che il tipo di istanza standard può supportare questo caso d'uso.

Per il portale A, l'amministratore deve inviare una richiesta di aumento della quota di servizio per aumentare il limite per le istanze XL dai valori predefiniti delle regioni (ovvero 5) a 100. Una volta soddisfatta, l'amministratore può allocare la capacità modificando il portale web. Per il portale B, l'amministratore può procedere senza richiedere un aumento della quota (ad esempio, poiché la regione ha una quota predefinita di 25 per il tipo di istanza standard).

Altre quote di servizio in Amazon WorkSpaces Secure Browser

È possibile visualizzare e richiedere aumenti per altre quote elencate nella pagina Service Quotas. In pratica, per la maggior parte dei clienti non sarà necessario richiedere aumenti di questi limiti. Queste quote sono generalmente raggruppate in due tipi: Numero e Tariffa.

Per quanto riguarda le quote numeriche, quando invii un aumento della quota di servizio per Numero di portali web, riceverai automaticamente un aumento del numero di risorse secondarie necessarie per creare un portale unico. Ciò si rifletterà nella pagina Service Quotas. Ad esempio, se richiedi un aumento dei portali da 3 a 5, riceverai automaticamente un aumento della quota di servizio da 3 a 5 per entrambe le impostazioni del browser e dell'utente. Hai la possibilità di riutilizzare o creare nuove risorse secondarie come desideri.

In rare occasioni, i clienti possono trovare l'opportunità di aumentare il numero o il tasso di altre quote di risorse. Ad esempio, gli amministratori potrebbero voler aumentare il numero di impostazioni del browser per testare configurazioni aggiuntive del portale. Queste richieste di quote di servizio verranno esaminate e soddisfatte di volta in volta. case-by-case

Per le quote tariffarie, non dovrebbe essere necessario modificare i limiti di tariffa indicati nelle Service Quotas, indipendentemente dal limite del portale dell'account.

Controllo dell'intervallo per la riautenticazione di un token IdP SAML in Amazon Secure Browser WorkSpaces

Quando un utente visita un portale WorkSpaces Secure Browser, 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 a Secure Browser. 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 Centro identità AWS IAM, consulta Impostare la durata della sessione.

2. Imposta i valori di inattività e di timeout di inattività del portale WorkSpaces Secure Browser. Questi valori controllano la quantità di tempo tra l'ultima interazione di un utente e il termine di una sessione di WorkSpaces Secure Browser 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 “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 di Secure Browser. Per controllare come i token vengono riautenticati, segui le guide nel passaggio precedente.

Configurazione della registrazione delle attività degli utenti in Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser offre due opzioni per la registrazione delle attività degli utenti e degli eventi relativi alla sicurezza:

- Session Logger acquisisce un'ampia gamma di eventi di sessione. Questi log vengono inviati a un bucket Amazon S3 nel tuo account, per una facile integrazione con la tua piattaforma SIEM preferita.
- La registrazione degli accessi degli utenti acquisisce gli eventi di sessione più critici. Questi log vengono trasmessi in streaming a un flusso Amazon Kinesis per l'elaborazione e l'analisi in tempo reale.

Entrambe le opzioni di registrazione sono configurate a livello di portale. È necessario configurare ogni opzione singolarmente per ogni portale in cui si desidera che la registrazione sia attiva. È possibile abilitare una delle due opzioni o entrambe, a seconda dei requisiti per ciascun portale.

L'utente è responsabile del rispetto di tutti i requisiti applicabili alla registrazione o al monitoraggio delle attività degli utenti quando utilizza questa funzione, inclusa la registrazione o il monitoraggio delle attività dei dipendenti.

Argomenti

- Configurazione di Session Logger per Amazon WorkSpaces Secure Browser
- Configurazione della registrazione degli accessi utente per Amazon WorkSpaces Secure Browser

Configurazione di Session Logger per Amazon WorkSpaces Secure Browser

> **Warning**
>
> L'attivazione di Session Logger disabilita le seguenti funzionalità di Chrome:
>
> - modalità di navigazione in incognito
> - Strumenti per developer
> - Cambio di profilo Chrome

Per attivare il logger di sessione per un portale WorkSpaces Secure Browser, devi prima identificare il bucket Amazon S3 in cui verranno raccolti gli eventi della sessione. Puoi utilizzare un bucket esistente che già memorizza log simili o crearne uno nuovo appositamente per questo scopo.

Il bucket Amazon S3 deve avere una policy sui bucket che conceda a WorkSpaces Secure Browser l'autorizzazione a scrivere log al suo interno. Ti consigliamo di collocare il bucket Amazon S3 nella stessa Account AWS regione del tuo portale WorkSpaces Secure Browser.

Non è richiesto alcun nome per il bucket Amazon S3. Per creare un nuovo bucket, segui i passaggi seguenti o consulta la sezione Creazione di un bucket generico nella Guida per l'utente di Amazon Simple Storage Service. Per indicazioni sulla configurazione delle autorizzazioni, consulta le politiche di Bucket per Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Di seguito è riportato un esempio di policy per il tuo bucket Amazon S3. Assicurati di aggiornare la policy con il nome del tuo bucket Amazon S3. Tieni presente che il Principal è «workspaces-web.amazonaws.com».

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

L'attivazione di Session Logger sul tuo portale WorkSpaces Secure Browser potrebbe comportare addebiti da parte di Amazon S3. Per ulteriori informazioni, consulta la pagina Prezzi di Amazon S3.

Per ulteriori informazioni sugli eventi relativi alla sessione acquisiti da Session Logger, consulta. the section called “Eventi di sessione in Session Logger”

Bucket S3 con crittografia KMS (opzionale)

WorkSpaces Secure Browser Session Logger supporta completamente i bucket AWS KMS Amazon S3 con crittografia abilitata. Per garantire una corretta funzionalità di registrazione con il tuo bucket Amazon S3 crittografato, devi concedere a Session Logger le autorizzazioni necessarie per utilizzare la tua chiave. AWS KMS

Aggiungi la seguente politica alla configurazione delle chiavi: AWS KMS

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

Nella AWS console, seleziona il portale WorkSpaces Secure Browser da cui raccoglierai gli eventi, quindi scegli la scheda Session logger e Modifica.

Inserisci le seguenti informazioni per configurare Session Logger per il portale:

- S3 Location (obbligatorio): il nome del bucket Amazon S3 in cui verranno distribuiti gli eventi.
- Prefisso chiave (opzionale): la cartella in cui vengono consegnati gli eventi. Se la cartella non esiste, verrà creata. Se il campo viene lasciato vuoto, Session Logger scriverà gli eventi nella radice del bucket Amazon S3.

In Advanced, puoi configurare i seguenti campi:

- Filtro eventi: questo è l'elenco degli eventi monitorati da Session Logger.
  - Tutti: la selezione di questa opzione significa che tutti gli eventi attuali e futuri verranno monitorati
  - Includi: consente di selezionare manualmente eventi specifici da monitorare. Verranno registrati solo gli eventi selezionati in modo esplicito. I nuovi eventi introdotti nei futuri aggiornamenti non verranno monitorati, a meno che non vengano aggiunti manualmente alla selezione.
- Formato del file
  - JSON (impostazione predefinita): si tratta di un formato di file in cui ogni file di registro viene presentato come una serie di eventi. Consigliamo questo formato per la maggior parte dei casi d'uso.
  - JSONLines: si tratta di un formato di file ottimizzato per Amazon Athena.
- Struttura delle cartelle: determina come vengono archiviati i file di registro.
  - Flat (impostazione predefinita): tutti i file di registro si trovano in un'unica cartella.

- Annidati per data: i file di registro sono organizzati in cartelle per data e ora. Partizionato per Amazon Athena e ottimizzato per le query Amazon Athena.

Puoi testare la configurazione del Session Logger e assicurarti che il logger di sessione funzioni correttamente. Una volta completata la configurazione, il sistema tenta di scrivere un file di test denominato `_workspaces_secure_browser.tmp` nel bucket e nella cartella Amazon S3 specificati. Ciò serve come convalida sia della funzionalità di registrazione che della configurazione delle autorizzazioni.

È inoltre possibile eseguire una sessione di test avviando una sessione di Secure Browser nel portale e utilizzando il browser come si farebbe normalmente. Session Logger scrive i file di registro nel bucket Amazon S3 configurato ogni 15 minuti durante una sessione attiva o al termine della sessione.

Dopo aver terminato la sessione o aver atteso il prossimo intervallo di registrazione, controlla il bucket Amazon S3 per confermare che i file di registro della sessione siano stati generati e archiviati come previsto.

Configurazione della registrazione degli accessi utente per Amazon WorkSpaces Secure Browser

Per attivare la registrazione degli accessi degli utenti nella console WorkSpaces Secure Browser, 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?

Per ricevere i log da WorkSpaces Secure Browser, 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?.

Gestione delle policy del browser in Amazon WorkSpaces Secure Browser

Puoi impostare qualsiasi politica del browser personalizzata utilizzando le politiche di Chrome disponibili per l'ultima versione stabile di WorkSpaces Secure Browser. Quando imposti un criterio nel portale WorkSpaces Secure Browser, il criterio verrà applicato a tutte le sessioni gestite da quel portale web.

Esistono più di 300 policy che puoi applicare a un portale web. Per ulteriori informazioni, incluso l'elenco completo delle politiche di Chrome, consulta l'elenco dei criteri di Chrome Enterprise.

Hai tre modi per impostare una policy di Chrome:

1. Utilizzo dell'editor visivo nel portale web

   Utilizzando la visualizzazione della console per creare un portale Web, è possibile applicare alcune delle politiche più comuni dell'editor visuale:

   - `StartURL`
   - Attivazione e disattivazione della navigazione privata
   - Eliminazione della cronologia
   - Segnalibri e cartelle di segnalibri
2. Utilizzo dell'editor JSON nel portale web

   È inoltre possibile aggiungere o modificare direttamente le politiche utilizzando l'editor JSON anziché l'editor visuale.

   Per il formato specifico di una policy, consulta l'elenco delle policy di Chrome Enterprise.
3. Caricamento di un file JSON nel portale web

   Puoi anche importare le politiche di Chrome utilizzate nella tua organizzazione caricando un file JSON nel portale web.

   Per i dettagli, consulta the section called “Tutorial: impostazione di una politica del browser personalizzata”

WorkSpaces Secure Browser applica una configurazione di base dei criteri del browser a tutti i portali insieme alle politiche specificate dall'utente. Puoi modificare alcune di queste policy con il tuo file

JSON personalizzato. Per ulteriori informazioni, consulta the section called “Modifica della politica di base del browser”.

Argomenti

- Tutorial: impostazione di una politica del browser personalizzata in Amazon WorkSpaces Secure Browser
- Modifica della policy di base del browser in Amazon WorkSpaces Secure Browser

Tutorial: impostazione di una politica del browser personalizzata in Amazon WorkSpaces Secure Browser

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.

Nel seguente tutorial, creerai 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
- Fase 2: raccolta delle policy
- Passaggio 3: creazione di un file di policy JSON personalizzato
- Fase 4: aggiunta delle policy al modello
- Passaggio 5: carica il file JSON della policy sul tuo portale web

Fase 1: creazione di un portale web

Per caricare il file JSON della policy di Chrome, devi creare un portale WorkSpaces Secure Browser. Per ulteriori informazioni, consulta the section called “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.
   - RestoreOnStartupURLs— 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 segnalibro. URLs
   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. Configura l'avvio URLs. 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'`RestoreOnStartup`azione per aprire un elenco di URLs . Puoi anche utilizzare altre azioni all'avvio URLs. Per ulteriori informazioni, consulta l'elenco delle policy di Chrome Enterprise.

   b. Impostato su `RestoreOnStartupURLs` 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. Apri la console WorkSpaces Secure Browser all'indirizzo. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. Scegli WorkSpaces Secure Browser, 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. Scegli Save (Salva).

Modifica della policy di base del browser in Amazon WorkSpaces Secure Browser

Per fornire il servizio, WorkSpaces Secure Browser applica una policy di base per i 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.

La linea di base `URLAllowlist` e `URLBlocklist` le politiche non possono essere sovrascritte. Tieni presente che il file di policy del browser JSON associato al tuo portale web non conterrà queste politiche di base. Per visualizzare un elenco completo di tutte le politiche applicate e dei relativi valori, accedi a «chrome: //policy» dall'interno di una sessione di navigazione remota.

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`.

Configurazione dell'Input Method Editor per Amazon WorkSpaces Secure Browser

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. IMEs aiuta gli utenti a inserire testo in lingue con set di lingue più ampi e complessi, come giapponese, cinese e coreano. WorkSpaces Le sessioni Secure Browser 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 Secure Browser:

- 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:

- Tutte le lingue
  - Per spostare l'IME in avanti (o passare al layout di tastiera destro), premi Shift+Control+Left Alt.
  - Per accedere alle impostazioni della lingua e di input, usa il selettore della lingua nella barra del pannello superiore. Se non è visibile, abilitalo tramite Barra degli strumenti → Preferenze → Generale → Metodo di immissione da tastiera.
- Giapponese
  - Per gli utenti macOS: se utilizzi una fonte di input statunitense, potresti riscontrare problemi di input. Per risolvere questo problema:
    1. Seleziona una fonte di input giapponese (ad esempio, giapponese - Kana o giapponese - Romaji) anziché la fonte di input americana sul tuo macOS.
    2. Nella sessione WorkSpaces Secure Browser, vai su Barra degli strumenti → Preferenze → Tastiera → Impostazione dei tasti Opzione e seleziona Usa Opzione () come tasto Alt remoto (Mac) per assicurarti che le scorciatoie da tastiera funzionino correttamente.
  - Conversione dei caratteri di input
    - Per convertire i caratteri in Hiragana, premete. F6
    - Per convertire i caratteri in Katakana, premete. F7
    - Per convertire i caratteri in Hankaku Katakana (Katakana a metà larghezza), premi F8

    - Per convertire i caratteri in latino, premete. F10
    - Per convertire i caratteri in Wide Latin, premeteF9.
  - Cambio delle modalità di input
    - Per passare da Hiragana a Katakana, premere. Alt/Option+K
    - Per passare da Katakana a Hankaku Katakana, premi. Alt/Option+K
    - Per passare da Hankaku Katakana (Katakana a metà larghezza) a Hiragana, premi. Alt/Option+K
    - Per passare da una modalità giapponese o da Wide Latin a Latin, premi. Alt/Option+L
    - Per passare da Latin a Wide Latin, premereAlt/Option+L.
    - Per passare da qualsiasi modalità a Direct Input, premeteHenkaku/Zenkaku key.
    - Per passare da Direct Input a Hiragana, premete. Henkaku/Zenkaku key
- Coreano
  - Per scegliere Hangul, premi Shift+Space.
  - Per scegliere Hanja, premi F9.

Per disattivare la tastiera su schermo dalle sessioni di WorkSpaces Secure Browser, contatta. Supporto

Configurazione della localizzazione in sessione per Amazon Secure Browser WorkSpaces

Quando un utente avvia una sessione, WorkSpaces Secure Browser 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.

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

1. La ForcedLanguagespolitica nelle impostazioni del browser del portale web. Per ulteriori informazioni, consulta 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 di WorkSpaces Secure Browser supportano la localizzazione:

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

Argomenti

- Codici di lingua supportati per Amazon WorkSpaces Secure Browser
- Selezione delle lingue nelle impostazioni del browser dell'utente

Codici di lingua supportati per Amazon WorkSpaces Secure Browser

L'elenco seguente mostra i codici di lingua attualmente supportati da WorkSpaces Secure Browser. 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)

Selezione delle lingue nelle impostazioni del browser dell'utente

Per configurare le impostazioni del browser locale di un utente, segui i passaggi appropriati.

- 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.

Gestione dei controlli di accesso IP in Amazon WorkSpaces Secure Browser

> **Important**
>
> Supportano solo i controlli di accesso IP IPv4. Gli utenti che si connettono da reti IPv6 -only verranno bloccati.

WorkSpaces Secure Browser 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 Secure Browser 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 Secure Browser 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 Secure Browser rileverà e terminerà 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 di WorkSpaces Secure Browser e devono assicurarsi che l'uso di WorkSpaces Secure Browser 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 di WorkSpaces Secure Browser da parte di un dipendente, comprese le attività eseguite all'interno dell'applicazione.

Argomenti

- Creazione di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser
- Associazione di un'impostazione di accesso IP a un portale Web in Amazon WorkSpaces Secure Browser
- Modifica di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser
- Eliminazione di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser

Creazione di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser

> **Important**
>
> Supportano solo i controlli di accesso IP IPv4. Gli utenti che si connettono da reti IPv6 -only verranno bloccati.

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

1. Apri la console WorkSpaces Secure Browser 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.

Associazione di un'impostazione di accesso IP a un portale Web in Amazon WorkSpaces Secure Browser

> **Important**
>
> IPv4Supportano solo i controlli di accesso IP. Gli utenti che si connettono da reti IPv6 -only verranno bloccati.

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

1. Apri la console WorkSpaces Secure Browser 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. Scegli Save (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 “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 di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser

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. Apri la console WorkSpaces Secure Browser 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.

Eliminazione di un gruppo di controllo degli accessi IP in Amazon WorkSpaces Secure Browser

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. Apri la console WorkSpaces Secure Browser 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.

Gestione dell'estensione Single Sign-On in Amazon Secure Browser WorkSpaces

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.

Per impostazione predefinita, le estensioni non sono abilitate in Chrome nelle finestre di navigazione in incognito o nelle finestre di navigazione privata di Firefox. Gli utenti possono abilitarle manualmente. Per ulteriori informazioni su Chrome, consulta Estensioni in modalità di navigazione in incognito. Per ulteriori informazioni su Firefox, consulta Estensioni nella navigazione privata.

Agli utenti viene richiesto di installare l'estensione quando accedono a un portale. Per informazioni dettagliate sull'esperienza utente con l'estensione, consulta the section called “Estensione Single Sign-On”.

Argomenti

- Identificazione dei domini per l'estensione Single Sign-On in Amazon Secure Browser WorkSpaces
- Aggiungere l'estensione Single Sign-On a un nuovo portale Web in Amazon WorkSpaces Secure Browser
- Aggiungere l'estensione Single Sign-On a un portale Web esistente in Amazon WorkSpaces Secure Browser
- Modifica o rimozione dell'estensione Single Sign-On in Amazon Secure Browser WorkSpaces

Identificazione dei domini per l'estensione Single Sign-On in Amazon Secure Browser WorkSpaces

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	Dominio
Okta	okta.com

IdP	Dominio
Inserisci ID	microsoftonline.com
AWS Identity Center	awsapps.com
Un solo accesso	onelogin.com
Duo	duosecurity.com

Aggiungere l'estensione Single Sign-On a un nuovo portale Web in Amazon WorkSpaces Secure Browser

Per consentire l'estensione durante la creazione di un nuovo portale web, segui questi passaggi.

1. Segui i passaggi indicati in the section called “Creazione di un portale Web” fino ad arrivare a the section called “Impostazioni utente”.
2. Nel passaggio 1 di the section called “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 “Impostazioni utente” e le sezioni rimanenti in the section called “Creazione di un portale Web” per creare il tuo portale web.

Aggiungere l'estensione Single Sign-On a un portale Web esistente in Amazon WorkSpaces Secure Browser

Per aggiungere l'estensione a un portale web esistente, segui questi passaggi.

1. Apri la console WorkSpaces Secure Browser a https://console.aws.amazon.com/workspaces-web/casa.
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.

Modifica o rimozione dell'estensione Single Sign-On in Amazon Secure Browser WorkSpaces

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

1. Apri la console WorkSpaces Secure Browser a https://console.aws.amazon.com/workspaces-web/casa.
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 l'estensione WorkSpaces Secure Browser installata nel proprio browser.

Filtraggio dei contenuti Web in Amazon WorkSpaces Secure Browser

Il Web Content Filtering è una funzionalità di sicurezza e conformità che consente all'organizzazione di definire politiche e regolare l'accesso ai contenuti all'interno di WorkSpaces Secure Browser. Con Web Content Filtering, è possibile specificare a quali utenti URLs finali è consentito accedere o bloccare categorie specifiche URLs o di dominio per limitare l'accesso, soddisfacendo i requisiti critici di sicurezza e conformità normativa.

> **Note**
>
> Sebbene sia possibile configurare politiche di filtraggio degli URL tramite le politiche di Chrome per bloccare o consentire domini specifici, non consigliamo questo approccio perché le azioni delle politiche di Chrome non verranno registrate come parte delle funzionalità di registrazione del servizio. Per un monitoraggio completo e un reporting sulla conformità, utilizza le politiche di Web Content Filtering descritte in questa pagina.

Argomenti

- Limitazione della navigazione a elementi specifici URLs
- Blocco specifico URLs
- Bloccare le categorie
- Esempio di URLs
- Trasferimento delle politiche di Chrome

Limitazione della navigazione a elementi specifici URLs

È possibile implementare una politica di «negazione predefinita» in base alla quale sono accessibili solo i siti Web approvati esplicitamente. URLs È ideale per ambienti ad alta sicurezza in cui l'accesso a Internet deve essere strettamente controllato e ogni sito consentito è stato verificato per esigenze aziendali e conformità alla sicurezza.

Nella AWS console, sotto il filtro degli URL:

- Vai all'elenco dei blocchi e seleziona l'interruttore Blocca tutto URLs
- Nella sezione Elenco consentiti, fai clic su Aggiungi URL per aggiungere un URL da inserire nell'elenco degli URL consentiti per l'utente finale. Aggiungi una voce per URL.
- Fai clic su Salva

Blocco specifico URLs

È possibile bilanciare sicurezza e produttività mantenendo un accesso a Internet aperto e bloccando al contempo i siti problematici noti. È adatto alle organizzazioni che si fidano dei propri utenti ma vogliono impedire l'accesso a minacce specifiche o contenuti inappropriati senza limitare eccessivamente le attività commerciali legittime.

Nella tua AWS console, in Filtraggio URL:

- Vai a Bloccato URLs
- Seleziona Aggiungi URL e inserisci l'URL da bloccare. Aggiungi una voce per ogni URL che desideri bloccare
- Fai clic su Salva

Bloccare le categorie

Oltre a bloccare blocchi specifici URLs, puoi anche bloccare automaticamente gruppi di contenuti URLs in base a categorie di contenuti. Ciò è utile per le organizzazioni che necessitano di una copertura completa contro vari tipi di contenuti inappropriati o rischiosi senza dover identificare e bloccare manualmente i singoli siti.

Nella AWS console, in Filtraggio URL:

- Vai alle categorie bloccate e fai clic su Aggiungi categorie
- Seleziona qualsiasi categoria che desideri bloccare
- Puoi fare eccezioni a queste categorie aggiungendole URLs all'elenco Consenti. Per fare ciò, fai clic su Aggiungi URL e inserisci URLs quello che desideri consentire. entry/ies Anche se sono inclusi nelle categorie, gli utenti finali potranno visitare il URLs.
- Fai clic su Salva

È possibile selezionare le seguenti categorie. È possibile selezionare una, molte o tutte le categorie.

Categorie di filtraggio disponibili

Tema	Categoria	Description
Contenuti per adulti e inappropriati	Nudità	Siti contenenti immagini o opere d'arte di nudo non sessuali.
Contenuti per adulti e inappropriati	Pornografia	Siti con contenuti sessuali espliciti o materiale di nudo provocatorio.
Contenuti per adulti e inappropriati	Educazione sessuale	Risorse sanitarie e sessuali adeguate all'età e riviste da un medico.
Contenuti per adulti e inappropriati	Insapore	Contenuti inappropriati per bambini non compresi in altre categorie.

Tema	Categoria	Description
Comunicazione e social	Chat	Piattaforme di messaggistica privata e di gruppo in tempo reale.
Comunicazione e social	Messaggistica istantanea	Servizi di messaggistica privata.
Comunicazione e social	Rete professionale	Piattaforme per la creazione di relazioni incentrate sul business.
Comunicazione e social	Social network	Piattaforme di interazione con gli utenti per la condivisione di contenuti ed esperienze personali.
Comunicazione e social	Posta elettronica basata sul Web	Servizi di messaggistica accessibili tramite browser, tra cui cartoline elettroniche e sistemi di auguri.
Intrattenimento	Videogiochi	Risorse di gioco ricreative, inclusi videogiochi, puzzle e attività diverse dal gioco d'azzardo.
Intrattenimento	Condivisione di immagini	Piattaforme di contenuti visivi che offrono funzionalità di hosting, ricerca e condivisione.
Intrattenimento	Peer to peer	Fornitori di applicazioni per la condivisione di file e relativi strumenti software.
Contenuti dannosi e illegali	Attività criminale	Istruzioni o materiali che promuovono atti illegali.
Contenuti dannosi e illegali	Hacking	Strumenti di accesso non autorizzati al sistema e risorse di sfruttamento della rete.
Contenuti dannosi e illegali	Droga illegale	Contenuti che promuovono l'uso di droghe ricreative o l'abuso di sostanze.
Contenuti dannosi e illegali	Software illegale	Materiale non autorizzato protetto da copyright e distribuzione di software dannoso.
Contenuti dannosi e illegali	Violenza	Contenuti che promuovono danni fisici o che mostrano materiale grafico.

Tema	Categoria	Description
Contenuti dannosi e illegali	Armi	Risorse legittime per l'uso di armi da fuoco sportive e ricreative.
Comportamenti ad alto rischio	Culti	Contenuti spirituali e metafisici non tradizionali.
Comportamenti ad alto rischio	Gioco d'azzardo	Attività e informazioni relative alle scommesse.
Comportamenti ad alto rischio	Odio e intolleranza	Contenuti che promuovono pregiudizi nei confronti delle caratteristiche protette.
Comportamenti ad alto rischio	Imbrogli scolastici	Servizi di assistenza accademica e completamento dei compiti non autorizzati.
Comportamenti ad alto rischio	Autolesionismo	Contenuti che promuovono o discutono di comportamenti autodistruttivi.
Tecnologia e intelligenza artificiale	Siti di download	Piattaforme di hosting di software, applicazioni e risorse digitali.
Tecnologia e intelligenza artificiale	IA generativa	Risorse tecnologiche di intelligenza artificiale e apprendimento automatico.
Tecnologia e intelligenza artificiale	Domini parcheggiati	Domini con contenuti minimi utilizzati per la pubblicità o la vendita di domini.
Tecnologia e intelligenza artificiale	Streaming di contenuti multimediali e download	Piattaforme di contenuti audio/video tra cui musica, video e radio su Internet.

Esempio di URLs

I seguenti tipi di URLs possono essere forniti in AllowedUrls o BlockedUrls

Tipo	Esempio
Dominio	esempio.com
Sottodominio	login.example.com
Path	example.com/myvideos
Parametro di query	example.com/? parameter=123

Trasferimento delle politiche di Chrome

Se hai già impostato le politiche di Chrome per consentire o bloccare domini specifici, ti consigliamo di trasferirle alla funzione Web Content Filtering.

La funzionalità Web Content Filtering rileverà tutte URLAllow URLBlock le policy applicabili a una sessione WorkSpaces Secure Browser e le segnalerà nella Console. AWS

Per trasferire le politiche di Chrome per URLAllowlist e/o URLBlocklist:

- Nella tua AWS Console, in Filtraggio URL, fai clic su Verifica le politiche di Chrome (se non vedi il pulsante Rivedi le norme di Chrome, significa che al momento non si applicano le politiche di Chrome per URL Allow o URLBlock)
- Sotto l'overlay, consulta le politiche di Chrome
- Fai clic su Trasferisci

Le politiche di Chrome verranno rimosse dall'editor JSON in Impostazioni dei criteri e le nuove URLs verranno aggiunte automaticamente alla funzionalità Web Content Filtering.

Collegamenti diretti in Amazon WorkSpaces Secure Browser

Quando un utente accede a WorkSpaces Secure Browser, avvia la sessione su una home page impostata dall'amministratore. Puoi anche consentire ai portali di ricevere link diretti che collegano

gli utenti a un sito Web specifico durante una sessione. Quando viene selezionato un collegamento diretto, il portale visualizza l'URL specificato nel collegamento diretto. Il link viene visualizzato accanto alle home page configurate per l'inizio della sessione o da solo se una sessione è già in corso. Questa funzionalità consente agli amministratori di creare esperienze utente più dinamiche con WorkSpaces Secure Browser.

I link diretti aprono pagine in una sessione di WorkSpaces Secure Browser. Se una sessione è già in esecuzione, aprirà il collegamento diretto in una nuova scheda. Se una sessione non è già in esecuzione, aprirà l'URL del collegamento diretto in una nuova scheda e la home page predefinita del portale in una scheda separata. Se un collegamento diretto contiene più di un URL, mostrerà l'URL del collegamento diretto elencato per primo, con ogni URL successivo (inclusa la home page predefinita) aperto in schede separate.

Argomenti

- Configurazione di collegamenti diretti in Amazon WorkSpaces Secure Browser
- Utilizzo del filtro URL per i link diretti in Amazon WorkSpaces Secure Browser

Configurazione di collegamenti diretti in Amazon WorkSpaces Secure Browser

Per consentire l'autorizzazione per i link diretti, scegli Consentito durante la creazione delle impostazioni utente. Il sito a cui desideri creare un collegamento diretto deve avere una codifica URL. Ad esempio, per collegare un utente a «/? https://www.example.com query=true», aggiorna il link a %2F%3Fquery%3Dtrue. https%3A%2F%2Fwww.example.com

Un deeplink può contenerne fino URLs a 10, delineati da una virgola. Esempio:

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

Per ulteriori informazioni sull'autorizzazione dei link diretti, consulta. the section called “Impostazioni utente”

Utilizzo del filtro URL per i link diretti in Amazon WorkSpaces Secure Browser

Qualsiasi utente con cui condividi questo link al portale può manipolare il valore del deep link per visitare un sito web, se quel dominio è raggiungibile dal portale e non è presente nella lista di blocco degli URL. Per creare una lista consentita o una lista di blocco restrittiva per impedire agli utenti di visitare domini indesiderati con il tuo portale, utilizza il filtro degli URL.

La lista consentita e la lista bloccata per un portale possono essere modificate con il filtro degli URL nelle impostazioni del browser del portale. <uuid>A tale scopo, aggiungi l'URL a un URL del portale nella lista consentita nel seguente formato, dove UUID è l'ID del portale: https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue https%3A%2F%2Fwww.example.com

Per ulteriori the section called “Filtraggio dei contenuti Web” informazioni, consulta Consentire o bloccare l'accesso ai siti Web.

Utilizzo della dashboard di gestione delle sessioni in Amazon WorkSpaces Secure Browser

Utilizza la dashboard di gestione delle sessioni sulla console WorkSpaces Secure Browser per monitorare e gestire sessioni attive e complete.

Accesso alla dashboard

Per accedere alla dashboard, segui questi passaggi.

Per accedere alla dashboard

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Secure Browser, Portali Web e scegli il tuo portale web.
3. Scegli la scheda Sessione o scegli Visualizza sessioni per aprire la dashboard in un pannello diviso sottostante.

Filtri della dashboard

Nel pannello delle sessioni, puoi filtrare le sessioni in base alle seguenti proprietà o valori:

- Stato
  - Attiva: indica che una sessione è attualmente in esecuzione. Per terminare la sessione, vedi sotto.
  - Terminata: indica che una sessione non è più attiva.
- ID della sessione
- Nome utente
- Ora di inizio della sessione

Termina le sessioni

Per terminare una sessione, segui questi passaggi.

Per terminare una sessione

1. Nella dashboard delle sessioni, seleziona la sessione che desideri interrompere.
2. Scegliere Terminate (Termina).
3. Gli utenti disconnessi perdono tutto lo stato della sessione. Tutte le schede aperte, la cronologia del browser e i file scaricati nel browser sicuro vengono riciclati.

Cronologia delle sessioni

La dashboard contiene le sessioni degli ultimi 35 giorni. È possibile utilizzare la CLI per elencare le sessioni, con o senza filtro. La cronologia delle sessioni viene fornita in formato JSON, che gli amministratori possono elaborare, gestire e archiviare in un repository separato.

Di seguito sono riportati alcuni esempi di comandi CLI per la gestione delle sessioni nella regione US-West-2 (Oregon).

Per elencare tutte le sessioni per un portale Web, esegui il comando seguente:

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

Per elencare tutte le sessioni per un utente specifico di un portale Web, esegui il comando seguente:

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

Protezione dei dati in transito con endpoint FIPS e Amazon Secure Browser WorkSpaces

Per impostazione predefinita, quando comunichi con il servizio WorkSpaces Secure Browser come amministratore utilizzando la console, l'interfaccia a riga di AWS comando (AWS CLI) o un AWS SDK o durante una sessione utente, tutti i dati in transito vengono crittografati utilizzando TLS 1.2.

Se necessiti di moduli crittografici convalidati FIPS 140-3 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Quando si utilizza un endpoint FIPS, tutti i dati in transito vengono crittografati utilizzando standard crittografici conformi al Federal Information Processing Standard (FIPS) 140-3. Per informazioni sugli endpoint FIPS, incluso un elenco di endpoint Secure Browser, vedere. WorkSpaces https://aws.amazon.com/compliance/fips

Dopo la creazione di un portale con endpoint FIPS, tutte le sessioni utente e le modifiche amministrative vengono apportate automaticamente utilizzando gli endpoint FIPS 140-3. È possibile utilizzare la variabile di `AWS_USE_FIPS_ENDPOINT=true` ambiente per individuare gli endpoint FIPS e inviare richieste con l'SDK. Di seguito è riportato un esempio di :

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

È inoltre possibile utilizzare l'`–endpoint-url`opzione per inviare richieste direttamente agli endpoint FIPS. Di seguito è riportato un esempio di portali con elenchi di chiamate nella regione US-West-2 (Oregon):

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

Gestione delle impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

Le impostazioni di protezione dei dati vengono utilizzate per proteggere i dati dalla condivisione durante una sessione. Le impostazioni possono essere create e applicate a più portali.

Argomenti

- Redazione dei dati in linea in Amazon Secure Browser WorkSpaces
- Configurazione di redazione predefinita in Amazon WorkSpaces Secure Browser
- Redazione in linea di base in Amazon Secure Browser WorkSpaces
- Redazione in linea personalizzata in Amazon Secure Browser WorkSpaces
- Crea impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser
- Associa le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser
- Modifica le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser
- Eliminare le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

Redazione dei dati in linea in Amazon Secure Browser WorkSpaces

Aggiungendo la redazione dei dati in linea a un portale, è possibile prevedere e oscurare automaticamente determinati dati da una stringa di testo visualizzata nelle pagine Web. È possibile creare politiche di redazione scegliendo tra modelli predefiniti (ad esempio numeri di previdenza sociale o numeri di carte di credito) oppure creare tipi di dati personalizzati utilizzando espressioni regolari e parole chiave. Le politiche includono livelli configurabili di applicazione e controlli per stabilire URLs dove applicare la redazione.

I seguenti componenti determinano quando i dati vengono oscurati:

- Impostazioni di protezione dei dati: le impostazioni di protezione dei dati sono il nome della risorsa che include i tipi di dati e i criteri di applicazione. Per utilizzare questa risorsa, devi prima creare le tue impostazioni, quindi associarle a un portale. Quando gli utenti avviano una sessione, le impostazioni vengono applicate durante la sessione.
- Estensione del browser in sessione: quando si associano le impostazioni di redazione al portale, il browser di sessione viene avviato con un'estensione del browser applicata dal sistema che applica le impostazioni dell'utente. Le impostazioni di protezione dei dati applicano la redazione tramite il pattern matching (espressioni regolari) e la ricerca di parole chiave in base al livello di confidenza e alla configurazione di applicazione degli URL. Il contenuto viene previsto dalle stringhe di testo e oscurato prima di essere visualizzato sullo schermo. L'estensione imposta anche le relative politiche del browser che regolano la capacità degli utenti di aggirare la redazione (come la navigazione privata disabilitata, l'accesso agli strumenti di sviluppo e l'ispezione della rete).

Le seguenti modifiche alle norme del browser Chrome vengono applicate dall'estensione del browser integrata nella sessione. Per ulteriori informazioni, consulta l'elenco delle policy di Chrome Enterprise.

- Applica la politica del browser per impedire agli utenti di visualizzare la sessione senza redazione:
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled= falso
  - BrowserGuestModeEnabled= falso
- L'estensione impedisce inoltre agli utenti di scaricare file HTML da URLs cui vengono applicate le impostazioni di protezione dei dati annullando l'evento di download.

In generale, è consigliabile utilizzare la redazione con siti Web privati e strutturati (come gli strumenti di gestione dei clienti, i sistemi di ticketing o i wiki) e non per la navigazione pubblica non strutturata (come Facebook o Google). Puoi scegliere tra i tipi di dati predefiniti (vedi sotto per l'elenco completo) o definire tipi di dati personalizzati utilizzando i tuoi valori di espressione regolare e le tue parole chiave. Gli amministratori hanno la responsabilità di verificare e convalidare che ogni tipo di dati, livello di confidenza e applicazione degli URL funzioni come previsto. AWS non può garantire la compatibilità con siti Web o applicazioni personalizzati forniti da terze parti.

WorkSpaces Secure Browser attualmente non supporta la redazione di tipi di dati supportati o personalizzati in formati non testuali, incluso il testo nei seguenti formati:

- Immagini, come JPEG, PNG o GIF
- Pagine Web che consentono agli utenti di utilizzare l'elaborazione o la modifica dinamica di testi, come Google Docs o Sheets
- Stream audio o video a cui si accede nel browser, ad esempio video YouTube
- PDFs visualizzati dal browser Chrome

Non utilizzare la redazione per i contenuti in un formato non supportato. Gli amministratori sono responsabili della convalida della compatibilità del sito e dei contenuti prima di concedere agli utenti l'accesso ai contenuti che intendono oscurare.

Configurazione di redazione predefinita in Amazon WorkSpaces Secure Browser

La configurazione di redazione predefinita applicherà automaticamente un livello di confidenza e l'applicazione degli URL per tutti i tipi di dati incorporati nelle impostazioni di protezione dei dati. È possibile sovrascrivere la configurazione predefinita quando si aggiunge un tipo di dati integrato.

I livelli di confidenza consentono di ottimizzare la logica di redazione per i tipi di dati incorporati utilizzando una combinazione di formato, parole chiave e testo non formattato. Scegli il livello di rigore con cui applicare la redazione, tra cui Alto, Medio o Basso. Il valore predefinito verrà applicato a tutti i tipi di dati, a meno che non venga applicata un'eccezione a livello di tipo di dati. In generale, iniziate con una configurazione predefinita di Medium e perfezionatela verificando che la redazione venga applicata come previsto sui vostri siti.

Livello di confidenza	Description	Esempio
Elevata	Richiede una corrispon denza dello schema di testo formattato per poter oscurare il contenuto.	Il SSN 123-45-6798 verrebbe oscurato, mentre 123456789 no.
Media	La redazione considera sia il testo formattato che quello non formattato e aggiunge parole chiave associate alla logica.	Il SSN 123-45-6798 verrebbe oscurato. 123456789 verrebbe oscurato se rilevato accanto a una parola chiave (ad esempio «numero di previdenz a sociale»).
Bassa	Oscurazione applicata sia per il pattern formattato che per il pattern non formattato senza parola chiave.	I SSN in entrambi i formati, 123-45-6798 e 123456789 , vengono oscurati senza richiedere una parola chiave.

È necessario impostare la configurazione di redazione predefinita per tutti i tipi di dati. Scegliere tra le seguenti opzioni:

- Tutti URLs

- Specifico URLs
- Configurazione avanzata

Il valore predefinito verrà applicato a tutti i tipi di dati, a meno che non venga applicata un'eccezione a livello di tipo di dati. L'applicazione degli URL utilizza una logica simile alla politica di Chrome per la gestione delle liste consentite e bloccate. Per indicazioni sull'utilizzo di blocchi e consenti URLs, consulta Consentire o bloccare l'accesso ai siti Web. Per ottenere risultati ottimali, aggiungili URLs a questi elenchi seguendo il formato di filtro delle liste bloccate di Chrome. Per ulteriori informazioni, consulta Formato del filtro URL blocklist.

Redazione in linea di base in Amazon Secure Browser WorkSpaces

La redazione in linea dei dati supporta modelli integrati (come i numeri di previdenza sociale e i numeri delle carte di credito), elencati nella sezione Redazione in linea di base. Scegli i tipi di dati dal menu a discesa e specifica il valore sostitutivo per ogni tipo di dati. Tutti i tipi di dati seguono lo schema di applicazione della configurazione predefinito riportato sopra, ma puoi scegliere di ignorare il livello di confidenza e ottimizzare il modello di imposizione del dominio per ogni tipo di dati.

Per inserire un valore alternativo dalla configurazione predefinita, scegli Confidence level override. Ad esempio, con la configurazione predefinita impostata su Media, durante i test potresti notare che uno dei tuoi tipi di dati non viene oscurato in modo affidabile. Puoi impostare l'override su Basso per aumentare la possibilità di redazione, senza modificare la logica utilizzata per gli altri tipi di dati.

Per ottimizzare il modo in cui viene applicata la redazione URLs senza modificare la configurazione predefinita, applica le sostituzioni di imposizione degli URL. Ad esempio, è possibile impostare l'utilizzo delle sostituzioni degli URL per imporre la redazione degli indirizzi e-mail nel sistema di gestione delle relazioni con i clienti, senza interrompere l'accesso degli utenti agli indirizzi e-mail presenti nell'elenco aziendale, nel sito Web o nelle e-mail basate sul Web.

Di seguito è riportato un elenco di tipi di dati e il relativo schema integrato: IDs

builtInPatternId	Tipo di dati
awsAccessKey:	AWS Access Key (Chiave di accesso AWS)
awsSecretKey:	AWS Secret Key (Chiave segreta AWS)
Numeri di carta:	Numeri di carte di credito

builtInPatternId	Tipo di dati
cripto:	Indirizzi di criptovalute
CuSIPNum:	Numero CUSIP
data:	Data
Decano:	Numeri DEA degli Stati Uniti
cane:	Data di nascita
Patente di guida:	Patenti di guida statunitensi
Indirizzo e-mail:	Indirizzo e-mail
Peccato:	Numero identificativo del datore di lavoro statunitense
Data di scadenza:	Data di scadenza della carta di credito
healthInsuranceNum:	Numero di reclamo dell'assicurazione sanitaria Medicare
Codice HIPAA:	Codice HIPAA ICD-10
indivTaxId:	Codice fiscale individuale statunitense
iPad Dr:	Indirizzo IP
è in:	Numeri di identificazione internazionali dei titoli
jwt:	Token Web JSON
Coord di posizione:	Coordinate della posizione
MacAddr:	Un indirizzo MAC
medicareBeneficiaryId:	Numero del beneficiario Medicare
npi:	Numero identificativo del fornitore nazionale

builtInPatternId	Tipo di dati
ndc:	Codici nazionali sulle droghe (NDC)
Numero di passaporto:	Numero di passaporto statunitense
Numero di telefono:	Numero di telefono
Numero di routing:	Numero di routing ABA
ssn:	Numero di previdenza sociale degli Stati Uniti
Codice SWIFT:	Codice SWIFT
ora:	Orario
vena:	Numero di identificazione del veicolo negli Stati Uniti

Redazione in linea personalizzata in Amazon Secure Browser WorkSpaces

I clienti possono definire i propri modelli utilizzando espressioni regolari, ad esempio un'applicazione interna personalizzata. IDs Per creare un modello di redazione in linea personalizzato, segui questi passaggi:

1. Vai alle impostazioni di protezione dei dati.
2. Scegli Redazione in linea personalizzata e aggiungi.
3. Inserisci un nome per il tipo di dati personalizzato.
4. Inserisci il valore dell'espressione regolare.
   - I valori delle espressioni regolari devono corrispondere alla sintassi letterale delle espressioni JavaScript regolari. Per ulteriori informazioni, consulta Espressioni regolari. Un esempio di espressione regolare è `/ex[am]+ple/i`.
   - Assicurati di testare i tuoi modelli personalizzati sui siti Web che intendi supportare. Se i modelli personalizzati sono scritti con errori, possono introdurre problemi di prestazioni non intenzionali.
5. Specificate il valore sostitutivo.
6. Scegli Altre opzioni per ulteriori personalizzazioni opzionali, tra cui:

- Aggiungi parole chiave per ottimizzare la logica di redazione. Le parole chiave possono aumentare la precisione dell'applicazione. Aggiungi parole chiave nella sintassi letterale delle espressioni regolari Javascript. Per ulteriori informazioni, consulta Espressioni regolari.

  Ad esempio, se state creando un modello di redazione personalizzato per un client IDs utilizzato in un sistema interno, potete aggiungerlo `/client name/i` al campo delle parole chiave per definire la logica di scansione e rilevamento.
- Applica le sostituzioni di imposizione degli URL per ottimizzare il modo in cui viene applicata la redazione URLs, senza modificare la configurazione predefinita.

  Ad esempio, è possibile impostare l'utilizzo delle sostituzioni degli URL per imporre la redazione degli indirizzi e-mail nel sistema di gestione delle relazioni con i clienti, senza interrompere l'accesso degli utenti agli indirizzi e-mail presenti nell'elenco aziendale o nelle e-mail basate sul Web.
- Inserisci una descrizione (opzionale) per il tipo di dati.

Crea impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

È possibile creare impostazioni di protezione dei dati in WorkSpaces Secure Browser.

Per creare impostazioni di protezione dei dati

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni di protezione dei dati.
3. Scegli Crea impostazioni di protezione dei dati.
4. Inserisci un nome visualizzato (obbligatorio) e una descrizione (opzionale) per l'impostazione.
5. Seleziona le impostazioni predefinite per la redazione in linea. È possibile impostare quanto segue:

   - Il livello di rigore di tutti i tipi di dati
   - I domini su cui deve essere applicata la redazione
6. Scegli i tipi di dati di redazione in linea di base tra quelli supportati o crea un tipo di dati personalizzato. Puoi impostare sostituzioni per ogni tipo di dati, incluso il livello di rigore e le eccezioni di dominio.

7. Aggiungi eventuali tag (facoltativo) per la segnalazione.
8. Al termine, scegliere Save (Salva).

Associa le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

È possibile associare le impostazioni di protezione dei dati in WorkSpaces Secure Browser.

Per associare un'impostazione di protezione dei dati a un portale esistente

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Nel riquadro di navigazione a sinistra, scegli Portali Web.
3. Seleziona il portale web e scegli Modifica.
4. In Impostazioni di protezione dei dati, seleziona l'impostazione per il tuo portale.
5. Scegli Save (Salva).

Per associare un'impostazione di protezione dei dati alla creazione di un nuovo portale, procedi nel seguente modo.

Per associare un'impostazione di protezione dei dati durante la creazione di un nuovo portale

1. Segui le istruzioni the section called “Creazione di un portale Web” per creare un portale, fino ad arrivare alle impostazioni di protezione dei dati.
2. Scegli l'impostazione di protezione dei dati dal menu a discesa.
3. Completa i passaggi indicati the section called “Creazione di un portale Web” per completare la creazione del portale.

Per creare un'impostazione di protezione dei dati durante la creazione di un nuovo portale, segui questi passaggi.

Per creare un'impostazione di protezione dei dati durante la creazione di un nuovo portale

1. Segui le istruzioni the section called “Creazione di un portale Web” per creare un portale, fino ad arrivare alle impostazioni di protezione dei dati.
2. Scegli le impostazioni di protezione dei dati dal menu a discesa.

3. Inserisci un nome visualizzato (obbligatorio) e una descrizione (opzionale) per l'impostazione.
4. Seleziona le impostazioni predefinite per la redazione in linea. È possibile impostare quanto segue:
   - Il livello di rigore di tutti i tipi di dati
   - I domini su cui deve essere applicata la redazione
5. Scegli i tipi di dati di redazione in linea di base tra quelli supportati o crea un tipo di dati personalizzato. Puoi impostare sostituzioni per ogni tipo di dati, incluso il livello di rigore e le eccezioni di dominio.
6. Aggiungi eventuali tag (facoltativo) per la segnalazione.
7. Al termine, scegliere Save (Salva).
8. Seleziona il pulsante di aggiornamento nelle impostazioni di protezione dei dati, quindi scegli l'impostazione di protezione dei dati dal menu a discesa.
9. Continua a seguire le istruzioni per la creazione del portale per completare la creazione del portale.

Modifica le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

È possibile modificare le impostazioni di protezione dei dati in WorkSpaces Secure Browser.

Per modificare le impostazioni di protezione dei dati

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli le impostazioni di protezione dei dati e l'impostazione di protezione dei dati che desideri modificare dalla visualizzazione a elenco.
3. Puoi aggiornare il nome, la descrizione, le impostazioni predefinite, i tipi di dati (supportati o personalizzati) e applicare modifiche al livello di confidenza o al dominio.
4. Scegli Save (Salva).

Eliminare le impostazioni di protezione dei dati in Amazon WorkSpaces Secure Browser

È possibile eliminare le impostazioni di protezione dei dati in WorkSpaces Secure Browser.

Per eliminare le impostazioni di protezione dei dati

1. Se si dispone di un portale associato a un'impostazione di protezione dei dati, è necessario rimuovere l'associazione prima di eliminare l'impostazione di protezione dei dati.
2. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
3. Scegli le impostazioni di protezione dei dati e l'impostazione di protezione dei dati che desideri eliminare dalla visualizzazione a elenco.
4. Scegli Elimina.

Personalizzazione del marchio in Amazon Secure Browser WorkSpaces

Puoi personalizzare le schermate di accesso e caricamento visualizzate dagli utenti finali modificando gli elementi visivi, il contenuto del testo e i termini di servizio. La personalizzazione del marchio aiuta a creare un'esperienza coerente in linea con l'identità dell'organizzazione.

Panoramica

La personalizzazione del marchio consente di personalizzare i seguenti aspetti dell'esperienza utente:

- Elementi visivi: carica logo, favicon e sfondo e seleziona i temi di colore in base all'identità del tuo marchio.
- Contenuto testuale: personalizza i messaggi di benvenuto, il titolo della scheda del browser e altri campi di testo opzionali per mantenere la voce del tuo marchio durante tutto il flusso di accesso. Se non specifichi testo personalizzato per determinati campi, verrà utilizzato il testo predefinito. Per informazioni dettagliate, vedi the section called “Linee guida per la personalizzazione”.
- Termini di servizio (facoltativo): aggiungi i termini di servizio della tua organizzazione che gli utenti devono confermare prima di iniziare una sessione.

> **Note**
>
> Puoi anche personalizzare il nome di dominio per il tuo portale. Per informazioni dettagliate, vedi the section called “Dominio personalizzato”.

Argomenti

- Configurazione della personalizzazione del marchio per il portale
- Linee guida per la personalizzazione

Configurazione della personalizzazione del marchio per il portale

Come funziona

Quando configuri la personalizzazione del marchio:

- Gli elementi visivi e testuali vengono applicati sia alla schermata di accesso che alla schermata di caricamento.
- La scheda del browser mostra la favicon e il titolo personalizzati.
- Gli utenti finali vedranno le modifiche alla personalizzazione all'inizio di una nuova sessione. In alcuni casi, potrebbero essere necessari alcuni minuti prima che le modifiche siano visibili.
- Se i termini di servizio sono configurati, gli utenti finali devono accettarli prima di iniziare la sessione di streaming. Tieni presente che verranno chiesti all'inizio di ogni sessione.

Prerequisiti

Prima di iniziare:

- Assicurati di disporre delle autorizzazioni necessarie per modificare le impostazioni del portale, vedithe section called “AWS politiche gestite”.
- Prepara le tue risorse di branding (logo, favicon, sfondo) in base alle specifiche riportate in. the section called “Linee guida per la personalizzazione”

Nozioni di base

Per configurare la personalizzazione del marchio, segui questi passaggi.

1. Apri la console WorkSpaces Secure Browser all'indirizzo. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. Scegli WorkSpaces Secure Browser, Portali Web e scegli il tuo portale web.
3. Seleziona il tuo portale e scegli la scheda Impostazioni utente.
4. Nella sezione Personalizzazione del marchio, scegli Modifica.
5. Configura le seguenti sezioni in base alle esigenze:
   - Nell'editor dei contenuti: carica tutti gli elementi visivi (il logo della tua azienda, la tua favicon e uno sfondo opzionale) e seleziona il tema del colore. Puoi caricare i file dal tuo computer locale o da un bucket S3. Per informazioni sulla configurazione delle autorizzazioni del bucket S3, consulta. the section called “Configurazione delle autorizzazioni per i bucket S3”
   - Nell'editor di testo: personalizza il testo che appare nella schermata di accesso.
   - Nell'editor dei Termini di servizio: facoltativamente, aggiungi termini che gli utenti devono riconoscere.
6. Scegli Save changes (Salva modifiche).

Per istruzioni dettagliate su ciascuna opzione di personalizzazione, consulta. the section called “Linee guida per la personalizzazione”

Configurazione delle autorizzazioni per i bucket S3

Puoi caricare i file di branding direttamente dal tuo computer o selezionare oggetti esistenti dai tuoi bucket S3. Se scegli di caricare i file per gli elementi visivi (il logo della tua azienda, la tua favicon e uno sfondo) da un bucket S3, assicurati di impostare le autorizzazioni appropriate per il bucket S3.

Selezione di oggetti S3 nello stesso account

Se il tuo utente o ruolo IAM dispone già dell'`s3:GetObject`autorizzazione per il bucket contenente le tue risorse di branding, non è richiesta alcuna configurazione aggiuntiva.

Selezione di oggetti S3 in un altro account

Per selezionare un bucket S3 in un AWS account diverso, devi configurare sia la policy del bucket nell'account di origine che la policy IAM nel tuo account amministratore.

Esempio di bucket policy (nell'account di origine):

Applica questa politica al bucket S3 nell'account di origine. *123456789012*Sostituiscilo con l'ID del tuo account amministratore e *source-account-bucket-name* con il nome effettivo del bucket.

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

Esempio di policy IAM (nel tuo account amministratore):

Allega questa policy all'utente o al ruolo IAM nel tuo account amministratore. Sostituiscila *source-account-bucket-name* con il nome effettivo del bucket dall'account di origine.

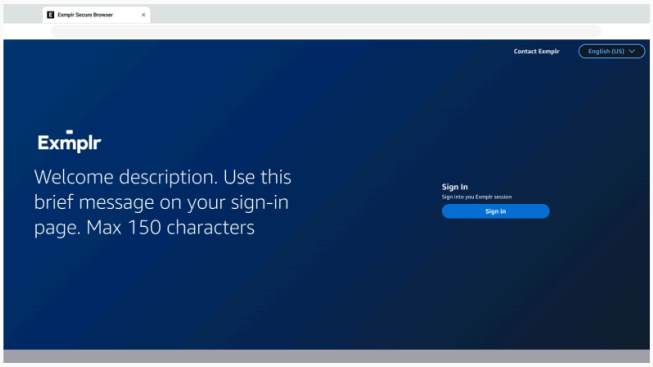
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
    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

```
}
```

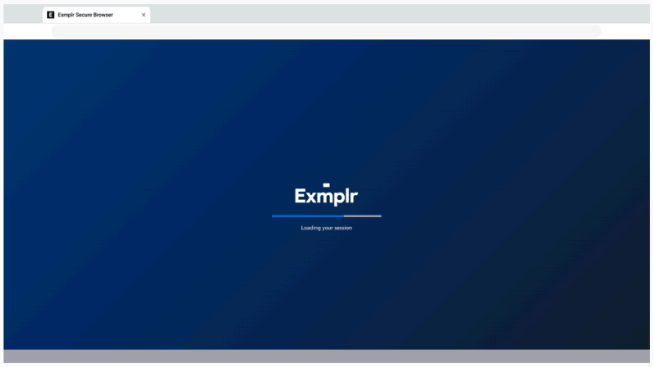
Per informazioni dettagliate sull'accesso tra account, consulta S3 Access concede l'accesso su più account.

Linee guida per la personalizzazione

Personalizza l'esperienza di accesso e caricamento per i tuoi utenti finali aggiornando gli elementi di branding e il testo nelle pagine di accesso e caricamento. Puoi modificare elementi visivi come loghi e sfondi, modificare elementi di testo come messaggi di benvenuto e intestazioni e, facoltativamente, configurare un accordo sui Termini di servizio che gli utenti devono accettare prima di iniziare la sessione.



Sign in Page

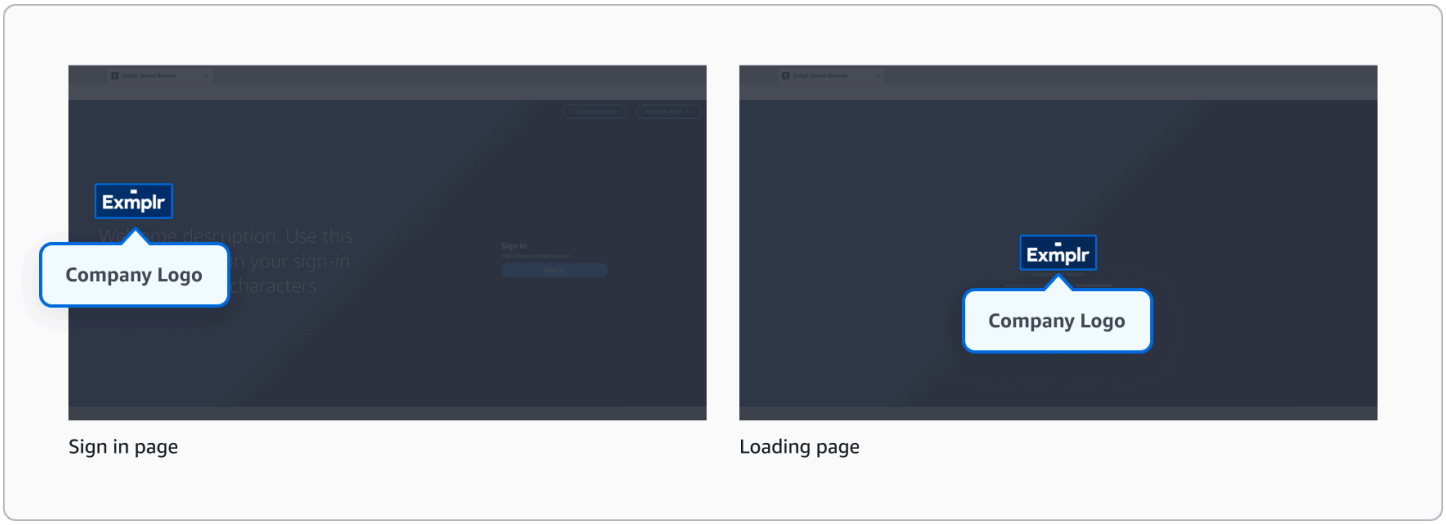


Loading Page

Editor di contenuti

Logo dell'azienda

Il logo viene visualizzato nella schermata di accesso e nella schermata di caricamento, fornendo un branding coerente per tutta l’esperienza utente.

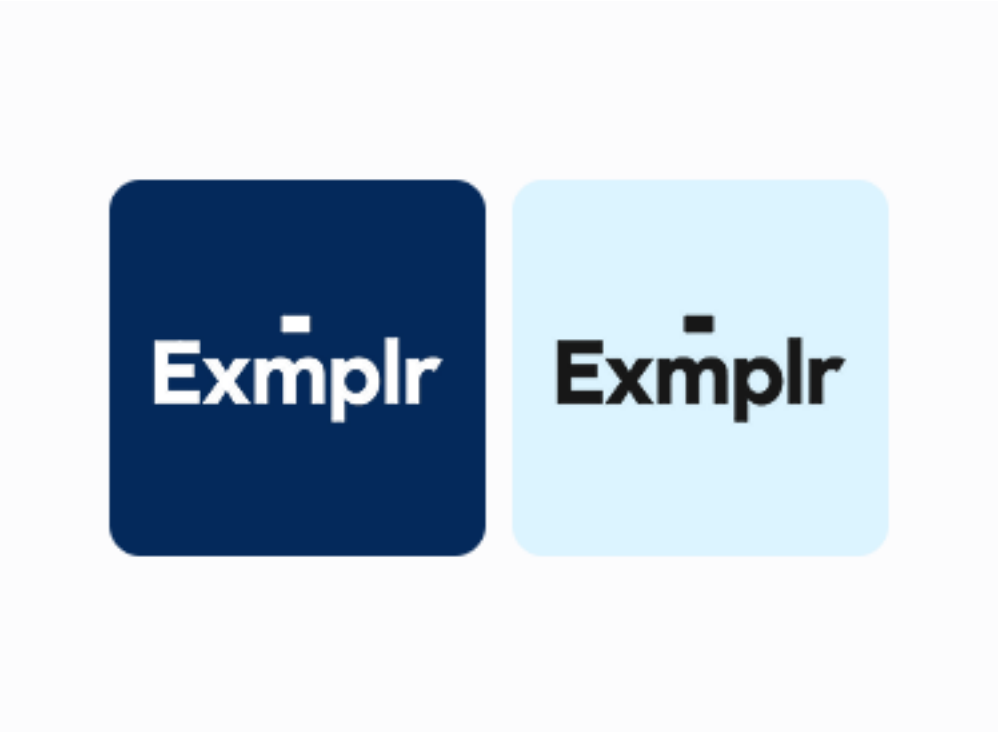


Sign in page

Loading page

- Formati supportati: JPEG, ICO o PNG
- Dimensione massima del file: 100 KB

Fare



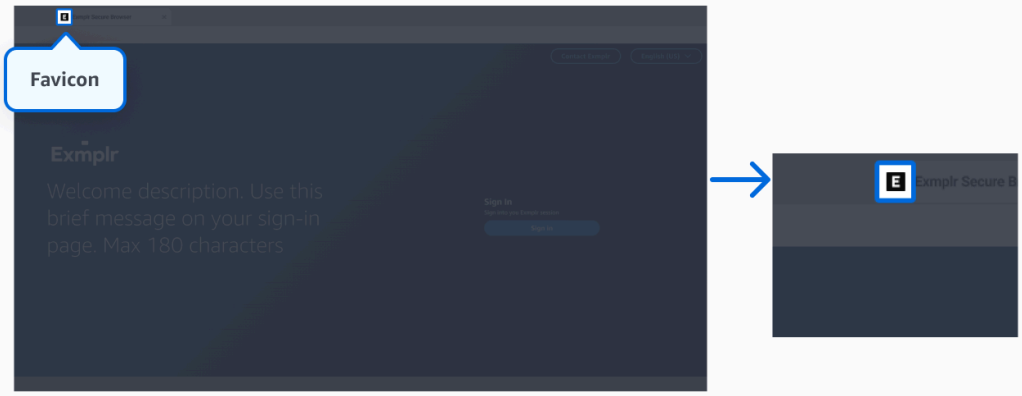
- Se hai diverse varianti del logo (ad esempio colori o stili diversi), scegli quella che offre il miglior contrasto con lo sfondo dello sfondo selezionato.

Non

- Non ignorate le proporzioni quando ridimensionate il logo.
- Non utilizzare in precedenza loghi non dimensionati correttamente in quanto potrebbero apparire distorti.

Favicon

Una favicon è una piccola icona che appare nelle schede del browser e aiuta gli utenti a identificare l'applicazione tra le diverse schede aperte.



- Formati supportati: JPEG, ICO o PNG
- Dimensione massima del file: 100 KB
- Proporzioni consigliate: 1:1

Sfondo: opzionale

Lo sfondo funge da immagine di sfondo su tutti gli schermi, creando un'esperienza visiva coerente. Se non carichi uno sfondo personalizzato, verrà utilizzato lo sfondo predefinito mostrato di seguito. Scegli un'immagine che integri il tuo branding senza interferire con la leggibilità dei contenuti.

Wallpaper will be the same across all pages

- Formati supportati: JPEG o PNG
- Dimensione massima del file: 5 MB
- Proporzioni consigliate: 16:9

- Risoluzione minima consigliata: 1920 x 1080

Fate

- Usa sfondi sottili e a basso contrasto o immagini sfocate che non interferiscano con i contenuti in primo piano.
- Prendi in considerazione il posizionamento preimpostato del testo per evitare aree affollate dietro il testo.
- Utilizza i colori del marchio e le sovrapposizioni per creare contrasto e leggibilità migliori.

Non

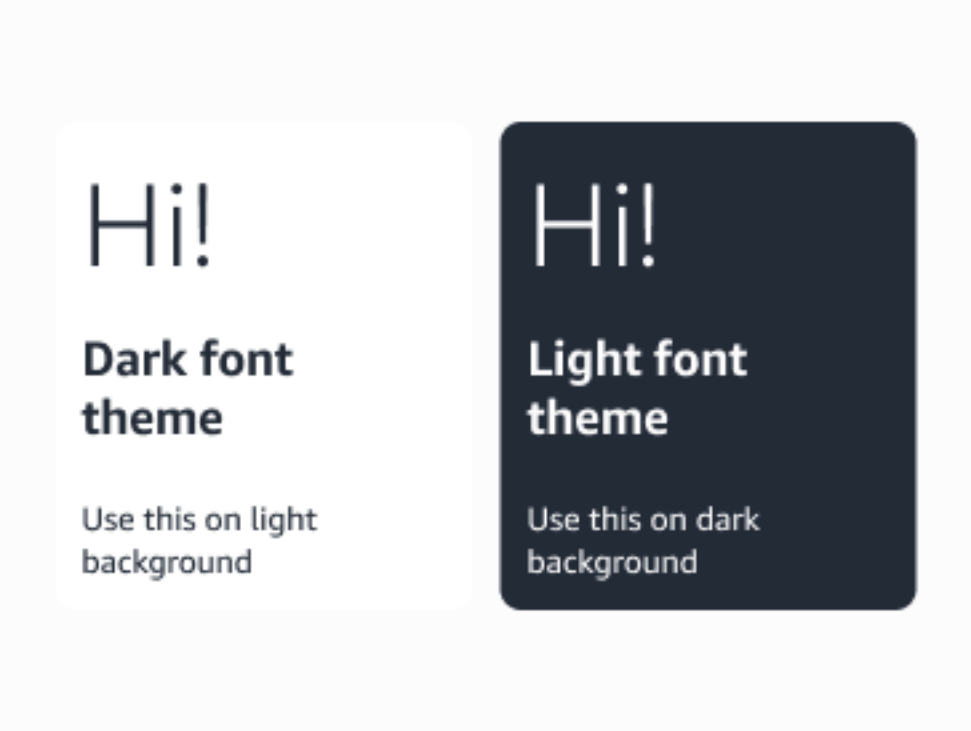
- Non utilizzare immagini affollate, sature o ricche di dettagli direttamente dietro a un testo importante.
- Non utilizzare immagini visivamente complesse o immagini con transizioni nitide che potrebbero causare limitazioni di leggibilità con posizioni di testo preimpostate.
- Non affidatevi esclusivamente al colore per separare il testo dallo sfondo senza un contrasto sufficiente.

Tema colore

Scegli tra temi chiari o scuri che si riflettono su caratteri, pulsanti e modali.

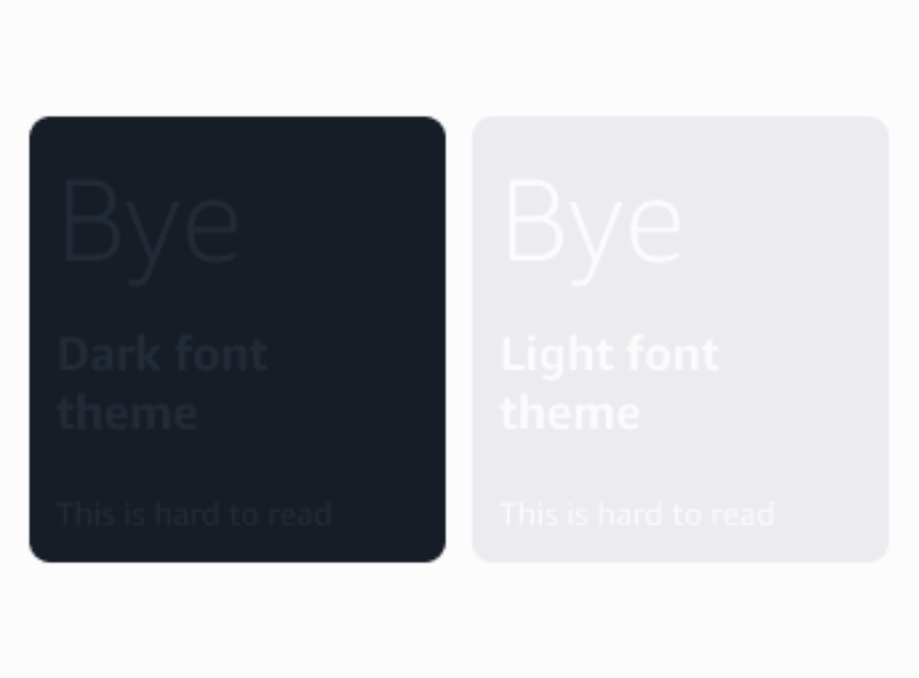
- Tema chiaro: ideale per sfondi più scuri, offre un contrasto chiaro e riduce l'affaticamento degli occhi quando si lavora in ambienti con scarsa illuminazione.
- Tema scuro: ottimale per gli sfondi chiari, offre una visione confortevole e un abbagliamento ridotto in ambienti luminosi.

Fai



- Garantisci un forte contrasto con gli elementi di sfondo/lo sfondo.
- Usa un tema di colore scuro su sfondi chiari.
- Usa un tema di colore chiaro su sfondi scuri.

Non



- Non collocate caratteri chiari o scuri su immagini o sfondi complessi.

Editor di testo

L'editor di testo consente di personalizzare il testo visualizzato nella schermata di accesso degli utenti finali. Per abilitare la personalizzazione del marchio, è necessario aggiungere almeno una lingua.

Per i nuovi utenti: rileviamo la preferenza della lingua del browser e visualizziamo la pagina del portale in quella lingua, se l'hai configurata nelle lingue del tuo branding. Se la lingua del browser non è nelle lingue configurate, l'impostazione predefinita è l'inglese (en-US), se disponibile. Se non hai configurato l'inglese, utilizziamo la prima lingua in ordine alfabetico tra le lingue configurate.

Per gli utenti abituali: memorizziamo la preferenza della lingua della sessione precedente in un cookie del browser. Se quella lingua è nelle lingue di branding configurate, la utilizziamo. Altrimenti, seguiamo la stessa logica di fallback: inglese (en-US) se disponibile o la prima lingua configurata in ordine alfabetico.

Sono supportate le seguenti impostazioni locali (codici di lingua):

- Tedesco (de-DE)
- Inglese (Stati Uniti) (en-US)
- Spagnolo (es-ES)
- Francese (fr-FR)

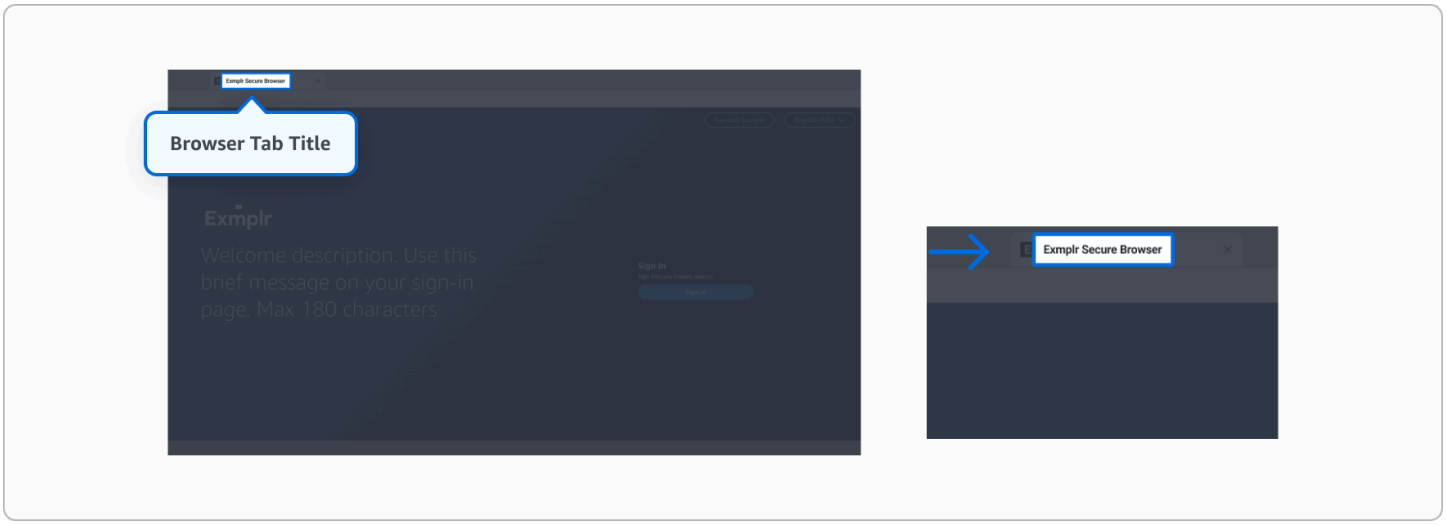
- Indonesiano (id-ID)
- Italiano (it-IT)
- Giapponese (ja-JP)
- Coreano (ko-KR)
- Portoghese (pt-BR)
- Cinese semplificato (zh-CN)
- Cinese tradizionale (zh-TW)

Per motivi di sicurezza, i seguenti caratteri sono bloccati in tutti i campi di testo:

- < (minore di)
- > (maggiore di)
- & (e commerciale)
- ’ (apostrofo dritto)
- ` (backtick/accento grave)
- ~ (tilde)
- \ (barra rovesciata).

Titolo della scheda del browser

Il testo visualizzato nella scheda del browser. Massimo 25 caratteri.

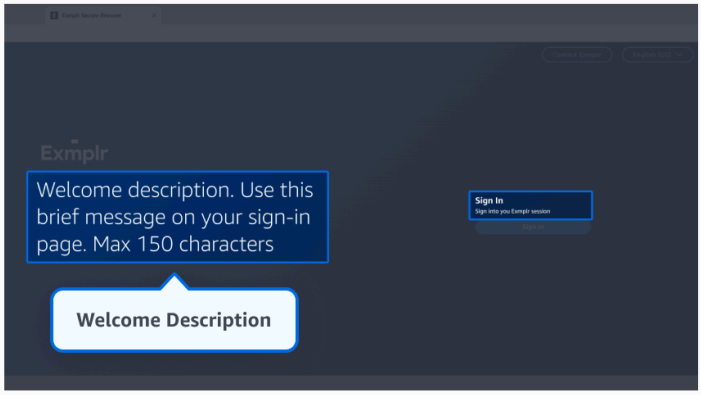


Raccomandazione

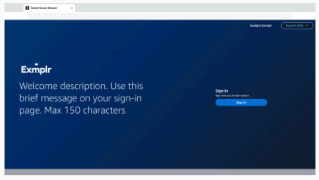
Prendi in considerazione l'utilizzo di titoli brevi e chiari in modo che rimangano leggibili anche quando sono aperte più schede.

Descrizione di benvenuto

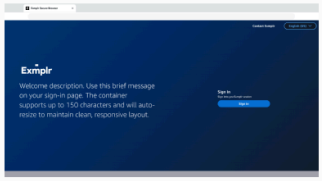
Una breve descrizione accanto al logo della tua azienda nella schermata di accesso. Massimo 150 caratteri.



Welcome description



Starting font sizing



Adapted sizing to Max characters

Raccomandazione

Mantieni il testo conciso per una migliore leggibilità. Tieni presente che il testo più lungo verrà automaticamente ridimensionato a una dimensione del carattere più piccola, mentre i messaggi più brevi vengono visualizzati in modo più evidente.

Sezione Contatti

Pulsante di contatto: opzionale

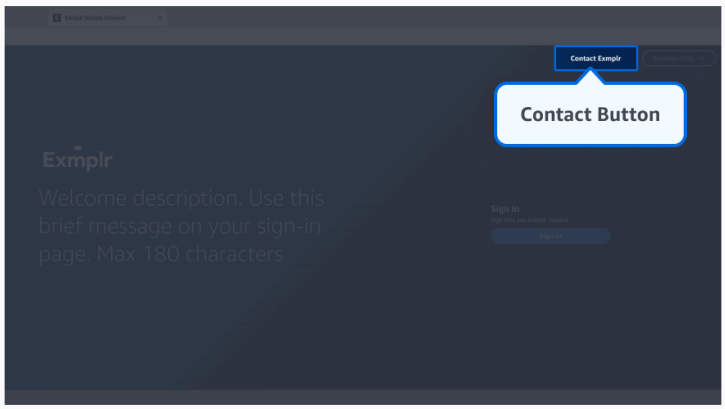
Testo del pulsante di contatto nella schermata di accesso. Se lasciato vuoto, verrà visualizzato «Contattaci». Massimo 30 caratteri.

Link di contatto: opzionale

Link del pulsante di contatto nella schermata di accesso. È possibile utilizzare:

- Un URL HTTPS per indirizzare gli utenti a una pagina Web
- Un link mailto: per aprire il client di posta elettronica dell'utente

Se lasciato vuoto, il pulsante di contatto verrà nascosto dallo schermo.



Raccomandazione

Mantieni il testo breve, idealmente 2-3 parole.

Sezione di accesso

Intestazione di accesso: opzionale

Intestazione per la sezione di accesso della pagina di accesso. Se lasciato vuoto, verrà visualizzato “Accedi”. Massimo 100 caratteri.

Descrizione dell’accesso: opzionale

Testo descrittivo per la sezione di accesso. Se lasciato vuoto, verrà visualizzato il messaggio «Accedi alla sessione WorkSpaces sicura del browser». Massimo 250 caratteri.

Pulsante di accesso: opzionale

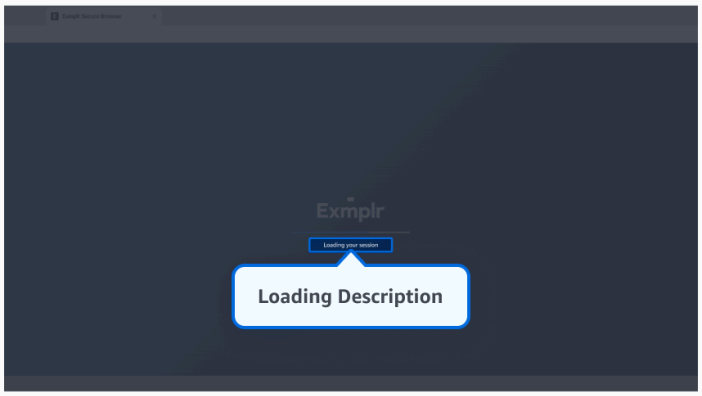
Testo visualizzato sul pulsante di accesso. Se lasciato vuoto, verrà visualizzato “Accedi”. Massimo 30 caratteri.

Raccomandazioni

- Mantieni il testo breve.
- Tieni presente che il pulsante di accesso indirizza gli utenti al provider di identità configurato per il tuo portale. Puoi personalizzare il testo del pulsante in modo che rifletta il tuo provider di identità specifico.

Caricamento della descrizione

Testo visualizzato durante la connessione nella schermata di caricamento. Se lasciato vuoto, verrà visualizzato “Contattaci”. Massimo 300 caratteri.



Loading screen

Raccomandazione

Questo messaggio viene visualizzato solo durante il caricamento della sessione, quindi gli utenti finali potrebbero non avere il tempo di leggerlo. Cercate di evitare che sia troppo lungo.

Termini di servizio: facoltativi

Puoi personalizzare i termini di servizio che gli utenti finali devono esaminare e accettare prima di iniziare una sessione di streaming. Questo contenuto può essere aggiunto caricando un file Markdown o utilizzando l'editor Markdown integrato.

Agli utenti verranno presentati i termini di servizio dopo aver effettuato correttamente l'accesso. Devono scorrere l'intero documento e fare clic sul pulsante "Accetta" per procedere alla sessione di Secure Browser. Se l'utente fa clic su "Rifiuta", verrà reindirizzato alla pagina di accesso.

Tieni presente che questa è un'impostazione facoltativa: se non aggiungi termini di servizio, gli utenti procederanno direttamente alle sessioni dopo l'accesso.

Formattazione supportata:

- Stili di testo di base (grassetto, corsivo)
- Intestazioni
- Elenchi ordinati e non ordinati
- Citazioni a blocchi
- Regole orizzontali
- Paragrafi e interruzioni di riga semplici

Per motivi di sicurezza, i seguenti elementi sono bloccati:

- Script ed esecuzione di codice
- Elementi interattivi come moduli e iframe
- Protocolli e percorsi di file non sicuri
- Attributi e stile HTML
- Link e tabelle esterni

Tieni presente che la dimensione del file dei termini di servizio non deve superare i 150 KB.

Abilitazione del supporto WebAuthn per il reindirizzamento in Amazon WorkSpaces Secure Browser

> **Warning**
>
> WebAuthn il reindirizzamento funziona solo nelle sessioni del browser con accesso a Internet abilitato. Assicurati che le impostazioni di rete del portale consentano l'accesso a Internet affinché WebAuthn le funzionalità funzionino correttamente.

WorkSpaces Secure Browser supporta WebAuthn (autenticazione Web) per i siti Web a cui si accede all'interno della sessione remota del browser. Ciò consente agli utenti di autenticarsi sui siti Web utilizzando le chiavi di FIDO2 sicurezza locali, gli autenticatori biometrici e gli autenticatori della piattaforma durante la navigazione nella sessione di Secure Browser. WorkSpaces

> **Note**
>
> WebAuthn il reindirizzamento è disponibile per gli utenti finali che utilizzano Google Chrome 136 (o successivo) o Microsoft Edge 137 (o successivo). Questa funzionalità non è disponibile per i browser diversi da Chromium come Safari o Firefox.
> Per abilitare la funzionalità di WebAuthn reindirizzamento, gli amministratori devono configurare entrambi:
>
> 1. Impostazioni utente del portale: abilita il WebAuthn reindirizzamento nelle impostazioni del portale
> 2. Criteri del browser locale dell'utente finale: configura la politica del WebAuthenticationRemoteDesktopAllowedOrigins browser sui dispositivi dell'utente per consentire il reindirizzamento WebAuthn

Argomenti

- Abilitazione del WebAuthn reindirizzamento nelle impostazioni del portale
- Configurazione della politica locale del browser per WebAuthn
- Utilizzo del WebAuthn reindirizzamento nelle sessioni remote del browser
- Risoluzione dei problemi di reindirizzamento WebAuthn

Abilitazione del WebAuthn reindirizzamento nelle impostazioni del portale

Per abilitare il WebAuthn reindirizzamento per i siti Web a cui si accede all'interno della sessione remota del browser, procedi nel seguente modo.

1. Apri la console WorkSpaces Secure Browser all'indirizzohttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Scegli WorkSpaces Secure Browser, Web portals, scegli il tuo portale web, quindi scegli Modifica.
3. Vai alla sezione Impostazioni utente.
4. In Autorizzazioni utente, imposta Consenti agli utenti di utilizzare l'autenticazione locale nella sessione del portale su Consentito.
5. Scegli Salva per applicare la configurazione.

Configurazione della politica locale del browser per WebAuthn

Oltre ad abilitare il WebAuthn reindirizzamento nelle impostazioni del portale, è necessario configurare la politica del browser locale per consentire il WebAuthn reindirizzamento tra il dispositivo locale dell'utente e la sessione remota del browser e viceversa. Questa configurazione viene in genere gestita dagli amministratori IT per gli ambienti aziendali o da singoli utenti per gli scenari BYOD.

La politica del browser deve includere il dominio di contenuto WorkSpaces Secure Browser per la tua regione. Aggiungi la seguente origine alla `WebAuthenticationRemoteDesktopAllowedOrigins` politica in base alla tua regione:

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

Ad esempio, in us-west-2: `https://us-west-2.content.workspaces-web.com`

Il metodo di configurazione specifico dipende dal fatto che si gestiscano i browser in un ambiente aziendale o si configurino singoli dispositivi per gli utenti BYOD. Per ulteriori informazioni sulla politica del browser, consulta la documentazione delle policy di Chrome Enterprise e la documentazione delle policy di Microsoft Edge.

> **Note**
>
> Potrebbe essere necessario il riavvio del browser per rendere effettiva la policy.

Utilizzo del WebAuthn reindirizzamento nelle sessioni remote del browser

Una volta abilitato il WebAuthn reindirizzamento nelle impostazioni del portale e configurata la politica locale del browser, gli utenti possono utilizzare WebAuthn l'autenticazione sui siti Web all'interno delle sessioni remote del browser WorkSpaces Secure Browser.

Gli utenti possono autenticarsi sui siti Web utilizzando:

- FIDO2 chiavi di sicurezza collegate al proprio dispositivo locale
- chiavi di accesso
- Autenticatori di piattaforme come Windows Hello o Touch ID

Il processo di WebAuthn autenticazione viene inoltrato senza problemi dalla sessione remota del browser al dispositivo locale dell'utente, fornendo un'autenticazione sicura senza password pur mantenendo i vantaggi di sicurezza dell'ambiente di navigazione remoto.

Risoluzione dei problemi di reindirizzamento WebAuthn

Se gli utenti riscontrano problemi con il WebAuthn reindirizzamento nelle sessioni remote del browser, utilizza i seguenti passaggi per identificare e risolvere i problemi più comuni.

Argomenti

- WebAuthn il reindirizzamento non funziona
- Messaggi di errore comuni

WebAuthn il reindirizzamento non funziona

Se i prompt di WebAuthn autenticazione non vengono visualizzati o non funzionano:

1. WebAuthn La verifica è abilitata nelle impostazioni del portale in Autorizzazioni utente.
2. Verifica che la politica del browser locale sia configurata correttamente accedendo `chrome://policy` o `edge://policy` confermando che `WebAuthenticationRemoteDesktopAllowedOrigins` includa l'URL del contenuto della tua regione.
3. Assicurati che la versione del browser soddisfi i requisiti: Chrome 136+ o Edge 137+.
4. Esegui il test con un altro autenticatore (chiave di sicurezza o autenticatore di piattaforma).

Messaggi di errore comuni

Di seguito sono riportati i messaggi di errore più comuni e le relative risoluzioni:

WebAuthn messaggi di errore e risoluzioni

Messaggio di errore	Risoluzione
Il WebAuthn reindirizzamento di Amazon DCV non è riuscito a completare la richiesta di registrazione: il reindirizzamento Webauthn non è supportato dal client	Verifica di utilizzare un browser e una versione supportati (Chrome 136+ o Edge 137+).
Viene visualizzato il messaggio ma non è possibile interagire con gli autenticatori locali	Verifica che l'estensione di WebAuthn reindiriz zamento Amazon DCV sia installata e abilitata nel tuo browser remoto.
Il WebAuthn reindirizzamento di Amazon DCV non è riuscito a completare la richiesta di registrazione: l'ID relying party non è un suffisso di dominio registrabile né uguale al dominio corrente. Successivamente, un tentativo di recuperare la risorsa .well-known/ webauthn dell'ID RP richiesto non è riuscito.	Ciò significa che la politica del browser locale non viene applicata. WebAuthenticationR emoteDesktopAllowedOrigins Controlla la politica e aggiorna per consentire il dominio del contenuto. Assicurati che il browser sia riavviato. Potrebbe essere necessario avviare una nuova sessione per applicare le modifiche.
L'operazione è scaduta o non è stata consentit a. Vedi: https://www.w3. org/TR/webauthn-2/#. sctn-privacy-considerations-client	Questo errore può verificarsi se: (1) L'estensi one di WebAuthn reindirizzamento DCV non è installata o abilitata, (2) l'utente annulla la richiesta di autenticazione, (3) l'utente inserisce un PIN errato per la chiave di sicurezza o (4) L'utente non interagisce con il prompt e la richiesta scade.

Gestione dei controlli della barra degli strumenti in Amazon WorkSpaces Secure Browser

Con i controlli della barra degli strumenti, puoi configurare la presentazione della barra degli strumenti per le sessioni degli utenti finali, incluse le seguenti opzioni:

- Funzionalità
  - Appunti: se abilitato, consente copy/paste controlli granulari (solo copia, solo incolla o entrambi). Quando è disattivata, nasconde l'icona e ne impedisce l'utilizzo dalla barra degli strumenti.
  - Trasferimento file: se abilitato, consente operazioni sui file con controlli granulari (solo caricamento, solo download o entrambi). Quando è disattivata, nasconde l'icona e impedisce i trasferimenti.
  - Microfono: se abilitato, consente l'utilizzo del microfono. Quando è disattivata, nasconde l'icona.
  - Webcam: se abilitata, consente l'utilizzo della fotocamera. Quando è disattivata, nasconde l'icona.
  - Doppio monitor: se abilitato, consente l'utilizzo di due monitor. Quando è disattivata, nasconde l'icona.
  - Schermo intero: se abilitata, consente la modalità a schermo intero. Quando è disattivata, nasconde l'icona.
  - Windows: se abilitato, consente lo spostamento tra le finestre. Quando è disattivata, nasconde l'icona.
- Settings (Impostazioni)
  - Tema della barra degli strumenti: controlla la visualizzazione in modalità chiara o scura. La configurazione rimuove il controllo del tema per l'utente finale.
  - Stato della barra degli strumenti: imposta lo stato ancorato o distaccato della barra degli strumenti. La configurazione rimuove il controllo dell'utente finale sullo stato della barra degli strumenti.
  - Risoluzione massima: definisce la risoluzione di visualizzazione massima consentita. Gli utenti possono selezionare solo risoluzioni fino a questo limite definito.

Configurazione di un dominio personalizzato per il portale

È possibile configurare un dominio personalizzato per un portale WorkSpaces Secure Browser per consentire l'accesso tramite il proprio nome di dominio anziché l'URL predefinito del portale. Questa funzionalità consente di fornire agli utenti un'esperienza più integrata utilizzando un dominio in linea con il marchio dell'organizzazione.

Panoramica

Il dominio personalizzato consente di personalizzare i seguenti aspetti dell'esperienza utente:

- Accesso personalizzato al portale: gli utenti accedono al portale tramite il dominio dell'organizzazione anziché l'endpoint AWS predefinito.
- Esperienza utente coerente: mantieni la coerenza del marchio utilizzando nomi di dominio familiari in linea con la tua organizzazione.

> **Note**
>
> Per personalizzare l'aspetto visivo e gli elementi di branding del portale, consulta. the section called “Personalizzazione del branding”

Argomenti

- Configurazione di un dominio personalizzato per il portale
- Risoluzione dei problemi relativi ai domini personalizzati

Configurazione di un dominio personalizzato per il portale

Come funziona

Quando configuri un dominio personalizzato:

- È possibile creare e configurare un reverse proxy con il dominio personalizzato per indirizzare il traffico verso l'endpoint del portale.
- Gli utenti accedono al portale tramite il dominio personalizzato anziché l'endpoint predefinito del portale.
- I certificati SSL garantiscono connessioni sicure durante tutto il processo.

Prerequisiti

Prima di configurare domini personalizzati, assicurati di avere:

- Un nome di dominio che gestisci tramite un provider di servizi DNS come Amazon Route53.
- Un portale WorkSpaces Secure Browser. Per ulteriori informazioni sulla creazione di un portale, vederethe section called “Creazione di un portale Web”.
- Assicurati di disporre delle autorizzazioni necessarie per gestire AWS Certificate Manager e le CloudFront configurazioni DNS.

Important

Gli utenti devono abilitare i cookie di terze parti per il dominio personalizzato nei propri browser per garantire la corretta funzionalità del portale.
Assicurati di possedere e gestire correttamente il dominio personalizzato e i relativi record DNS per mantenere la sicurezza e la funzionalità del tuo portale.

Note

Per abilitare l'estensione Single Sign-On per i domini personalizzati, gli utenti devono installare l'estensione nel proprio browser con una versione successiva alla 1.0.2505.6608. Agli utenti viene richiesto di installare l'estensione quando accedono a un portale. Per informazioni dettagliate sull'esperienza utente con l'estensione, consulta the section called “Estensione Single Sign-On”.

Nozioni di base

È possibile configurare il dominio personalizzato come attributo delle impostazioni del portale quando si crea un nuovo portale o quando si modifica un portale esistente. Questa operazione può essere eseguita utilizzando i AWS comandi Console, SDK CloudFormation o AWS CLI.

Ti consigliamo di configurare una CloudFront distribuzione Amazon come proxy inverso che indirizza il traffico dal tuo dominio personalizzato all'endpoint del portale WorkSpaces Secure Browser.

Note

Sebbene Amazon CloudFront sia consigliato come soluzione di reverse proxy, puoi utilizzare configurazioni di reverse proxy alternative. Assicurati di soddisfare le impostazioni di origine e di configurazione della cache richieste, come descritto nei passaggi di CloudFront configurazione di Amazon.

Configurazione CloudFront come proxy inverso

Per completare la configurazione di un reverse proxy, è necessario:

- Un certificato SSL tramite AWS Certificate Manager (ACM)

- Una CloudFront distribuzione Amazon
- Record DNS
- Portale configurato con il tuo dominio personalizzato

Certificato SSL

Se non ne hai già uno, segui questi passaggi per richiederne uno tramite ACM:

1. Accedi alla console ACM all'indirizzo. https://console.aws.amazon.com/acm

   > **Important**
   >
   > Utilizza la regione Stati Uniti orientali (Virginia settentrionale), poiché CloudFront richiede che i certificati vengano archiviati lì.

2. Richiedi un certificato:

   - Per i nuovi utenti ACM: scegli Inizia nella sezione Provision certificates
   - Per gli utenti ACM esistenti: scegli Richiedi un certificato

3. Scegli Richiedi un certificato pubblico, quindi scegli Richiedi un certificato.

   > **Note**
   >
   > Puoi anche importare un certificato esistente. Per ulteriori informazioni, consulta Importazione di certificati in ACM nella Guida per l'utente ACM.

4. Inserisci il tuo nome di dominio principale (ad esempio,). **`myportal.example.com`**
5. Scegli un metodo di convalida:

   - Convalida DNS (consigliata per gli utenti di Route 53): consente la creazione automatica di set di record nella zona ospitata. Per ulteriori informazioni, consulta la convalida DNS nella ACM User Guide.
   - Convalida e-mail: per ulteriori informazioni, consulta la sezione Convalida delle e-mail nella Guida per l'utente ACM.

6. Controlla le impostazioni e scegli Conferma e richiedi.

CloudFront distribuzione

Crea una CloudFront distribuzione per le richieste proxy dal tuo dominio personalizzato all'endpoint del portale.

1. Accedere alla CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront.
2. Scegliere Create Distribution (Crea distribuzione).
   - Nome della distribuzione: inserisci un nome per la distribuzione
   - Tipo di distribuzione: sito Web o app singola

   > **Note**
   >
   > Se il tuo dominio personalizzato è gestito in Route 53 nello stesso account AWS, CloudFront può gestire automaticamente il tuo DNS per te. Inserisci il tuo dominio personalizzato e fai clic su «Verifica dominio». Se hai un dominio di un altro provider DNS, salta questo passaggio e configura il dominio in un secondo momento.

3. Configura le impostazioni di origine:
   - Tipo di origine: Altro
   - Origine personalizzata: inserisci l'endpoint del portale .workspaces-web.com *<portalId>*
   - Percorso di origine: lascia vuoto (impostazione predefinita)
4. Personalizza le impostazioni di origine:
   - Aggiunta di intestazioni personalizzate

     > **Important**
     >
     > L'accesso al portale tramite dominio personalizzato funzionerà solo se questa intestazione è presente nelle richieste proxy. Assicurati che il nome e il valore dell'intestazione siano specificati esattamente come indicato.

     - Nome dell'intestazione: workspacessecurebrowser-custom-domain
     - Valore: il tuo dominio personalizzato (ad esempio,**`myportal.example.com`**)
   - Protocollo: solo HTTPS
   - Porta HTTPS: 443 (mantieni l'impostazione predefinita)

- Protocollo SSL originale minimo: TLSv1 .2 (impostazione predefinita)
- Tipo di indirizzo IP di origine: IPv4 solo (Amazon WorkSpaces Secure Browser non è supportato IPv6 al momento della stesura di questa guida amministrativa).

5. Personalizza le impostazioni della cache:

   - Politica del protocollo Viewer: reindirizza HTTP a HTTPS
   - Metodi HTTP consentiti: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Politica sulla cache: CachingDisabled
   - Politica di richiesta Origin: AllViewerExceptHostHeader

   > **Important**
   >
   > L'accesso al portale tramite un dominio personalizzato funzionerà solo se la policy di richiesta di origine è impostata su AllViewerExceptHostHeader. Come suggerisce il nome, questa politica filtra solo l'intestazione dell'host dalle intestazioni della richiesta e trasmette tutte le intestazioni rimanenti all'origine.

6. È possibile configurare WAF se lo si desidera, ma non è necessario ai fini di questa configurazione.
7. In Ottieni certificato TLS, seleziona il certificato TLS creato nel passaggio 1.
8. Controlla le impostazioni e scegli Crea distribuzione.

Record DNS

Cloudfront può aggiornare i record DNS in Route 53 per indirizzare il traffico dai domini specificati alla distribuzione creata nella Fase 2, se la zona ospitata si trova nello stesso account AWS.

1. Vai alle impostazioni CloudFront
2. Fai clic su «Indirizza i domini verso CloudFront»
3. Fai clic su «Configura il routing automaticamente»

Se hai configurato il DNS per il dominio personalizzato in un altro provider di servizi o in un altro account AWS, configura il provider DNS per indirizzare il traffico dal tuo dominio alla distribuzione. I passaggi seguenti descrivono come eseguire questa operazione utilizzando Route 53.

1. Apri la console Amazon Route 53 all'indirizzohttps://console.aws.amazon.com/route53.

2. Accedi alla gestione DNS:
   - Se non conosci Route 53 con questo AWS account, si apre la pagina di panoramica di Amazon Route 53. In Gestione DNS, scegli Inizia subito.
   - Se hai già utilizzato Route 53 con questo AWS account, procedi al passaggio successivo.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Crea una zona ospitata se non ne hai già una:
   - Per indirizzare il traffico Internet verso le tue risorse, consulta Creazione di una zona ospitata pubblica nella Amazon Route 53 Developer Guide.
   - Per indirizzare il traffico nel tuo VPC, consulta Creazione di una zona ospitata privata nella Amazon Route 53 Developer Guide.
5. Nella pagina Hosted Zones, scegli il nome della zona ospitata che desideri amministrare.
6. Scegliere Create Record Set (Crea set di record).
7. Crea una voce per il tuo dominio (ad esempio,**`myportal.example.com`**):
   - Tipo: A — IPv4 indirizzo
   - Alias: Yes (Sì)
   - Alias Target: URL CloudFront di distribuzione

   Mantieni i valori predefiniti per tutte le altre impostazioni.

> **Note**
>
> Se non utilizzi Route 53 per gestire il DNS per il tuo dominio, usa il tuo provider di servizi DNS e aggiungi voci DNS che puntano al tuo dominio all'URL della tua distribuzione. CloudFront

In alternativa, puoi utilizzare il seguente CloudFormation modello per creare la tua distribuzione: CloudFront

Questo CloudFormation modello crea automaticamente la CloudFront distribuzione, configura le impostazioni del reverse proxy e, facoltativamente, crea i record DNS di Route53:

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

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

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'

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

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

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

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

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

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
 ${CustomDomainName}'
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

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

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
```

```
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
 policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
          MinimumProtocolVersion: TLSv1.2_2021

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

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

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

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

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

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

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

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

Per utilizzare questo modello:

1. Salva il modello qui sopra come `workspaces-web-custom-domain-template.yaml`
2. Esegui la distribuzione utilizzando la AWS console, la AWS CLI AWS o l'SDK con i valori dei parametri specifici
3. Dopo la distribuzione, configura il portale con il dominio personalizzato come descritto nel passaggio 4 di seguito

Configurazione del portale

Registra il tuo dominio personalizzato come attributo delle impostazioni del portale utilizzando la AWS console, l' UpdatePortal API o il comando CLI AWS update-portal.

1. Apri la console WorkSpaces Secure Browser all'indirizzo. https://console.aws.amazon.com/workspaces-web/home
2. Nel riquadro di navigazione scegli Portali web.
3. Seleziona il portale web che desideri configurare e scegli Modifica.
4. Nelle impostazioni del portale, aggiungi il tuo dominio personalizzato.
5. Salva la configurazione del portale.

Verifica la tua configurazione

Per testare la tua configurazione, segui questi passaggi:

1. Apri un browser Web e accedi all'URL del tuo dominio personalizzato (ad esempio,**`https://myportal.example.com`**).
2. Se tutto è configurato correttamente, dovresti vedere la pagina di accesso al tuo portale.
3. Successivamente, inserisci l'URL del portale nel tuo browser, dovresti essere reindirizzato al dominio personalizzato dopo aver effettuato l'accesso al tuo IdP.
4. Infine, accedi al tuo IdP e fai clic sul riquadro dell'applicazione relativo al tuo portale. Dovresti essere reindirizzato al dominio personalizzato.

Risoluzione dei problemi relativi ai domini personalizzati

Se gli utenti riscontrano problemi con l'accesso al portale tramite un dominio personalizzato nelle sessioni remote del browser, utilizza i seguenti passaggi per identificare e risolvere i problemi più comuni.

Argomenti

- Messaggi di errore comuni

Messaggi di errore comuni

Di seguito sono riportati i messaggi di errore più comuni e le relative risoluzioni durante la configurazione di domini personalizzati:

Errore del token CSRF non valido

Questo errore si verifica quando Secure Browser non riceve correttamente la richiesta durante la CloudFront configurazione.

Per risolvere il problema:

- Controlla le impostazioni di origine personalizzate sulla tua CloudFront distribuzione.
- Verifica che il nome dell'intestazione personalizzata corrisponda esattamente `workspacessecurebrowser-custom-domain` e che il valore corrisponda esattamente al tuo dominio personalizzato (senza https://o qualsiasi parametro di query).
- Svuota la cache del browser locale.
- Invalida la cache su. CloudFront

Errore 502 Bad Gateway

Questo errore indica in genere problemi di configurazione della cache.

Per risolvere il problema:

- Controlla le impostazioni della cache sulla tua CloudFront distribuzione.
- Verifica che la politica della cache sia impostata su`CachingDisabled`.
- Verifica che la policy di richiesta Origin sia impostata su`AllViewerExceptHostHeader`.
- Svuota la cache del browser locale.

- Invalida la cache su. CloudFront

Errore di accesso negato

Questo errore può verificarsi se il dominio personalizzato è configurato in modo errato.

Per risolvere il problema:

- Controlla le impostazioni di origine sulla tua CloudFront distribuzione.
- Verifica che l'origine sia impostata sull'URL del portale corretto.
- Verifica che il portale sia configurato con il dominio personalizzato corretto.
- Svuota la cache del browser locale.
- Invalida la cache su. CloudFront

Sicurezza in Amazon WorkSpaces Secure Browser

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon WorkSpaces Secure Browser, consulta AWS Services in Scope by Compliance Program .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio 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 ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon WorkSpaces Secure Browser. Ti mostra come configurare Amazon WorkSpaces Secure Browser per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon WorkSpaces Secure Browser.

Indice

- Protezione dei dati in Amazon WorkSpaces Secure Browser
- Identity and Access Management per Amazon WorkSpaces Secure Browser
- Risposta agli incidenti in Amazon WorkSpaces Secure Browser
- Convalida della conformità per Amazon WorkSpaces Secure Browser
- Resilienza in Amazon WorkSpaces Secure Browser
- Sicurezza dell'infrastruttura in Amazon WorkSpaces Secure Browser
- Analisi della configurazione e delle vulnerabilità in Amazon WorkSpaces Secure Browser
- Accesso APIs tramite un endpoint VPC di interfaccia ()AWS PrivateLink

- Best practice di sicurezza per Amazon WorkSpaces Secure Browser

Protezione dei dati in Amazon WorkSpaces Secure Browser

Il modello di si applica alla protezione dei dati in Amazon WorkSpaces Secure Browser. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati . Per informazioni sulla protezione dei dati in Europa, consulta il General Data Protection Regulation (GDPR) Center.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con Centro identità AWS IAM or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno 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 hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo 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 Secure Browser o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS 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 si fornisce un URL a un

server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Argomenti

- Crittografia dei dati in Amazon WorkSpaces Secure Browser
- Inter-network privacy del traffico in Amazon WorkSpaces Secure Browser
- Registrazione degli accessi degli utenti in Amazon WorkSpaces Secure Browser

Crittografia dei dati in Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser 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 Secure Browser raccoglie anche i dati sulle policy 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 Secure Browser utilizza AWS Key Management Service per la crittografia.

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 di WorkSpaces Secure Browser. Utilizza i modelli IAM per creare un ruolo con accesso completo o di sola lettura. Per ulteriori informazioni, consulta AWS politiche gestite per WorkSpaces Secure Browser.
- Proteggi i dati dall'inizio alla fine fornendo una chiave gestita dal cliente, in modo che WorkSpaces Secure Browser possa crittografare i dati inattivi 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 portale WorkSpaces Secure Browser.
  - 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 Secure Browser protegge contenuti e metadati per impostazione predefinita crittografando tutti i dati sensibili con. AWS KMS Raccoglie la politica del browser e le preferenze

dell'utente per applicare criteri e impostazioni durante le sessioni di Secure Browser. 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 per Amazon WorkSpaces Secure Browser

La crittografia a riposo è configurata per impostazione predefinita e tutti i dati dei clienti (ad esempio, dichiarazioni sulle politiche del browser, nomi utente, registrazione o indirizzi IP) utilizzati in WorkSpaces Secure Browser vengono crittografati utilizzando. AWS KMS Per impostazione predefinita, WorkSpaces Secure Browser abilita la crittografia con una chiave AWS di proprietà. È inoltre possibile utilizzare una chiave gestita dal cliente (CMK) specificando la propria CMK durante la creazione delle risorse. Al momento questa funzionalità è supportata solo tramite la CLI.

Se scegli di passare una CMK, la chiave fornita deve essere una chiave di crittografia AWS KMS simmetrica e tu, in qualità di amministratore, devi disporre delle seguenti autorizzazioni:

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Se si utilizza una CMK, è necessario consentire al responsabile del servizio esterno WorkSpaces Secure Browser di accedere alla chiave.
Per ulteriori informazioni, consulta Esempio di policy sulle chiavi CMK con ambito con aws: SourceAccount

Quando possibile, WorkSpaces Secure Browser utilizzerà le credenziali FAS (Forward Access Sessions) per accedere alla tua chiave. Per ulteriori informazioni su FAS, vedere Forward access sessions.
In alcuni casi WorkSpaces Secure Browser potrebbe dover accedere alla chiave in modo asincrono. Inserendo il principale servizio esterno WorkSpaces Secure Browser nella policy chiave dell'utente, WorkSpaces Secure Browser sarà in grado di eseguire l'insieme di operazioni crittografiche consentito con la chiave utilizzata.

Dopo aver creato una risorsa, la chiave non può più essere rimossa o modificata. Se hai utilizzato una CMK, in qualità di amministratore che accede alla risorsa, devi disporre delle seguenti autorizzazioni:

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

kms:ReEncryptTo
kms:ReEncryptFrom
```

Se viene visualizzato un errore di accesso negato quando si utilizza la console, è probabile che l'utente che accede alla console non disponga delle autorizzazioni necessarie per utilizzare la CMK sulla chiave utilizzata.

Principali esempi di policy e ambito di applicazione per Secure Browser WorkSpaces

Le CMK richiedono la seguente politica chiave:

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

WorkSpaces Secure Browser richiede le seguenti autorizzazioni:

- `kms:DescribeKey`— Verifica che la AWS KMS chiave fornita sia configurata correttamente.
- `kms:GenerateDataKeyWithoutPlaintext`e `kms:GenerateDataKey` — Richiesta della AWS KMS chiave per creare le chiavi dati utilizzate per crittografare gli oggetti.
- `kms:Decrypt`— Richiede la AWS KMS chiave per decrittografare le chiavi dati crittografate. Queste chiavi dati vengono utilizzate per crittografare i dati.
- `kms:ReEncryptToe` `kms:ReEncryptFrom` — Richiesta della AWS KMS chiave per consentire la ricrittografia da o verso una chiave KMS.

Ambito delle autorizzazioni di WorkSpaces Secure Browser sul tuo AWS KMS Chiave

Se il principale di una dichiarazione politica chiave è un responsabile del AWS servizio, consigliamo vivamente di utilizzare le chiavi di condizione SourceAccount globali aws: SourceArn o aws:, oltre a Encryption Context.

Il contesto di crittografia utilizzato per una risorsa conterrà sempre una voce nel formato `aws:workspaces-web:RESOURCE_TYPE:id` e l'ID della risorsa corrispondente.

L'ARN di origine e i valori dell'account di origine sono inclusi nel contesto di autorizzazione solo quando arriva una richiesta AWS KMS da un altro AWS servizio. Questa combinazione di condizioni implementa autorizzazioni meno privilegiate ed evita un potenziale scenario "confused deputy". Per ulteriori informazioni, consulta Autorizzazioni per i servizi AWS nelle politiche chiave.

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

> **Note**
>
> Prima della creazione delle risorse, la policy chiave dovrebbe utilizzare solo la `aws:SourceAccount` Condizione, poiché la risorsa arn completa non esisterà ancora. Dopo la creazione della risorsa, la politica chiave può essere aggiornata per includere le `kms:EncryptionContext` condizioni `aws:SourceArn` e.

Esempio di policy chiave Scoped CMK con aws: SourceAccount

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

Esempio di policy basata su chiavi CMK con ambito: e resource **wildcard SourceArn**

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

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

Esempio di policy sulle chiavi CMK con ambito con aws: SourceArn

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

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> Dopo aver creato la risorsa, puoi aggiornare il carattere jolly della risorsa. `SourceArn` Se utilizzi WorkSpaces Secure Browser per creare una nuova risorsa che richiede l'accesso a CMK, assicurati di aggiornare di conseguenza la politica chiave.

Esempio di policy chiave CMK mirata con **`aws`**: e specifica per le risorse SourceArn **`EncryptionContext`**

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

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

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

> **Note**
>
> Assicurati di creare dichiarazioni separate quando includi una risorsa specifica `EncryptionContext` nella stessa politica chiave. Per ulteriori informazioni, consulta la sezione Utilizzo di più coppie di contesto di crittografia in kms:EncryptionContext: context-key.

Crittografia in transito per Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser 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' AWS SDK a WorkSpaces Secure Browser. 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 per Amazon WorkSpaces Secure Browser

Puoi fornire la tua Customer Managed AWS KMS Key per crittografare le informazioni dei tuoi clienti. Se non ne fornisci una, WorkSpaces Secure Browser utilizzerà una chiave AWS proprietaria. Puoi impostare la tua chiave utilizzando AWS SDK.

Inter-network privacy del traffico in Amazon WorkSpaces Secure Browser

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

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

Registrazione degli accessi degli utenti in Amazon WorkSpaces Secure Browser

Gli amministratori possono registrare gli eventi delle sessioni di WorkSpaces Secure Browser, 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 AWS o 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 Secure Browser

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare WorkSpaces le risorse Secure Browser. IAM è un Servizio AWS software che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell’accesso tramite policy
- Come funziona Amazon WorkSpaces Secure Browser con IAM
- Esempi di policy basate sull'identità per Amazon Secure Browser WorkSpaces
- AWS politiche gestite per WorkSpaces Secure Browser
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Secure Browser
- Utilizzo di ruoli collegati ai servizi per Amazon Secure Browser WorkSpaces

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Secure Browser)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Amazon WorkSpaces Secure Browser con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon Secure Browser WorkSpaces)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Servizio di directory che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare Centro identità AWS IAM. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di Centro identità AWS IAM .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

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

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon WorkSpaces Secure Browser con IAM

Prima di utilizzare IAM per gestire l'accesso a WorkSpaces Secure Browser, scopri quali funzionalità IAM sono disponibili per l'uso con WorkSpaces Secure Browser.

Funzionalità IAM che puoi utilizzare con Amazon WorkSpaces Secure Browser

Funzionalità IAM	WorkSpaces Supporto per Secure Browser
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì

Funzionalità IAM	WorkSpaces Supporto per Secure Browser
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

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

Argomenti

- Politiche basate sull'identità per Secure Browser WorkSpaces
- Politiche basate sulle risorse all'interno di Secure Browser WorkSpaces
- Azioni politiche per Secure Browser WorkSpaces
- Risorse politiche per Secure Browser WorkSpaces
- Chiavi relative alle condizioni delle policy per Secure Browser WorkSpaces
- Accedete agli elenchi di controllo (ACLs) in Secure Browser WorkSpaces
- Controllo degli accessi basato sugli attributi (ABAC) con Secure Browser WorkSpaces
- Utilizzo di credenziali temporanee con WorkSpaces Secure Browser
- Autorizzazioni principali per diversi servizi per Secure Browser WorkSpaces
- Ruoli di servizio per Secure Browser WorkSpaces
- Ruoli collegati ai servizi per WorkSpaces Secure Browser

Politiche basate sull'identità per Secure Browser WorkSpaces

Supporta le policy basate sull’identità: sì

Le policy basate sull'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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l’utente di IAM.

Con le policy basate sull’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.

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 IAM.

Esempi di policy basate sull'identità per Secure Browser WorkSpaces

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

Politiche basate sulle risorse all'interno di Secure Browser WorkSpaces

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Secure Browser WorkSpaces

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni 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 in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni WorkSpaces Secure Browser, consulta Azioni definite da Amazon WorkSpaces Secure Browser nel Service Authorization Reference.

Le azioni politiche in WorkSpaces Secure Browser 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 di WorkSpaces Secure Browser, vedere. Esempi di policy basate sull'identità per Amazon Secure Browser WorkSpaces

Risorse politiche per Secure Browser WorkSpaces

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si 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 Secure Browser e relativi ARNs, consulta Resources defined by Amazon WorkSpaces Secure Browser nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon WorkSpaces Secure Browser.

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

Chiavi relative alle condizioni delle policy per Secure Browser WorkSpaces

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile 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. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

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

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

Accedete agli elenchi di controllo (ACLs) in Secure Browser WorkSpaces

Supporti ACLs: No

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

Controllo degli accessi basato sugli attributi (ABAC) con Secure Browser WorkSpaces

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione 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 WorkSpaces Secure Browser

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali per diversi servizi per Secure Browser WorkSpaces

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale chiamante an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Secure Browser 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

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

Ruoli collegati ai servizi per WorkSpaces Secure Browser

Supporta i ruoli collegati ai servizi: sì

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'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, 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 Secure Browser WorkSpaces

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse WorkSpaces Secure Browser. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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

Per dettagli sulle azioni e sui tipi di risorse definiti da WorkSpaces Secure Browser, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon WorkSpaces Secure Browser nel Service Authorization Reference.

Argomenti

- Best practice relative alle policy basate sull'identità per Amazon Secure Browser WorkSpaces
- Utilizzo della console Amazon WorkSpaces Secure Browser
- Consentire agli utenti di visualizzare le proprie autorizzazioni per Amazon WorkSpaces Secure Browser

Best practice relative alle policy basate sull'identità per Amazon Secure Browser WorkSpaces

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse WorkSpaces Secure Browser nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori 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 ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando

vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API 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 Amazon WorkSpaces Secure Browser

Per accedere alla console Amazon WorkSpaces Secure Browser, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse WorkSpaces Secure Browser presenti nel 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 consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

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

Consentire agli utenti di visualizzare le proprie autorizzazioni per Amazon WorkSpaces Secure Browser

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 collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per WorkSpaces Secure Browser

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite piuttosto che scriverle da soli. La creazione di policy gestite dai clienti IAM che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi possono occasionalmente aggiungere autorizzazioni aggiuntive a una policy AWS gestita 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 AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia 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, consultare la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Argomenti

- AWS politica gestita: AmazonWorkSpacesWebServiceRolePolicy
- AWS politica gestita: AmazonWorkSpacesSecureBrowserReadOnly
- AWS politica gestita: AmazonWorkSpacesWebReadOnly
- WorkSpaces Secure Browser aggiorna le policy AWS gestite

AWS politica gestita: AmazonWorkSpacesWebServiceRolePolicy

Non è possibile allegare la policy `AmazonWorkSpacesWebServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a WorkSpaces Secure Browser di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta the section called "Uso di ruoli collegati ai servizi".

Questa politica concede autorizzazioni amministrative che consentono l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da Secure Browser. WorkSpaces

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `workspaces-web`— Consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da WorkSpaces Secure Browser.
- `ec2`— Consente ai principali di descrivere VPCs, sottoreti e zone di disponibilità; creare, etichettare, descrivere ed eliminare interfacce di rete; associare o dissociare un indirizzo; e 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 delle attività degli utenti”.

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

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

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

AWS politica gestita: AmazonWorkSpacesSecureBrowserReadOnly

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

Questa politica concede autorizzazioni di sola lettura che consentono l'accesso a WorkSpaces Secure Browser e alle sue dipendenze tramite la console di AWS gestione, l'SDK e la CLI. Questa policy 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 delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `workspaces-web`— Fornisce accesso in sola lettura a WorkSpaces Secure Browser e alle sue dipendenze tramite la console di AWS gestione, l'SDK e la CLI.
- `ec2`— Consente ai principali di descrivere, sottoreti e gruppi di VPCs sicurezza. Viene utilizzato nella Console di AWS gestione di WorkSpaces Secure Browser per mostrare all'utente le VPCs 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 AWS gestione in WorkSpaces Secure Browser 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": "*"
        }
    ]
}
```

AWS politica gestita: AmazonWorkSpacesWebReadOnly

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

Questa politica concede autorizzazioni di sola lettura che consentono l'accesso a WorkSpaces Secure Browser e alle sue dipendenze tramite la console di AWS gestione, l'SDK e la CLI. Questa policy 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`.

> **Note**
>
> Se attualmente utilizzi questa politica, passa alla nuova politica. `AmazonWorkSpacesSecureBrowserReadOnly`

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `workspaces-web`— Fornisce accesso in sola lettura a WorkSpaces Secure Browser e alle sue dipendenze tramite la console di AWS gestione, l'SDK e la CLI.
- `ec2`— Consente ai principali di descrivere, sottoreti e gruppi di VPCs sicurezza. Viene utilizzato nella Console di AWS gestione di WorkSpaces Secure Browser per mostrare all'utente le VPCs 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 AWS gestione in WorkSpaces Secure Browser 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": "*"
        }
    ]
```

```
}
```

WorkSpaces Secure Browser aggiorna le policy AWS gestite

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

Modifica	Descrizione	Data
AmazonWorkSpacesSecureBrowserReadOnly: nuova policy	WorkSpaces Secure Browser ha aggiunto una nuova policy per fornire l'accesso in sola lettura a WorkSpaces Secure Browser e alle sue dipendenze tramite la Console di gestione AWS, l'SDK e la CLI.	24 giugno 2024
AmazonWorkSpacesWebServiceRolePolicy— Politica aggiornata	WorkSpaces Secure Browser ha aggiornato la politica per CreateNetworkInterface limitarsi ai tag con awsRequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged:: true.	15 dicembre 2022
AmazonWorkSpacesWebReadOnly— Politica aggiornata	WorkSpaces Secure Browser ha aggiornato la policy per includere le autorizzazioni di lettura per la registrazione	2 novembre 2022

Modifica	Descrizione	Data
	degli accessi degli utenti ed elencare i flussi di dati Kinesis. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione delle attività degli utenti”.	
AmazonWorkSpacesWebServiceRolePolicy— Politica aggiornata	WorkSpaces Secure Browser ha aggiornato la policy per descrivere un riepilogo dei flussi di dati Kinesis e 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 delle attività degli utenti”.	17 ottobre 2022
AmazonWorkSpacesWebServiceRolePolicy— Politica aggiornata	WorkSpaces Secure Browser ha aggiornato la politica per la creazione di tag durante la creazione di ENI.	6 settembre 2022
AmazonWorkSpacesWebServiceRolePolicy— Politica aggiornata	WorkSpaces Secure Browser ha aggiornato la policy per aggiungere lo spazio dei AWS/Usage nomi alle autorizzazioni PutMetricData API.	6 aprile 2022

Modifica	Descrizione	Data
AmazonWorkSpacesWebReadOnly: nuova policy	WorkSpaces Secure Browser ha aggiunto una nuova policy per fornire l'accesso in sola lettura a WorkSpaces Secure Browser e alle sue dipendenze tramite la Console di gestione AWS, l'SDK e la CLI.	30 novembre 2021
AmazonWorkSpacesWebServiceRolePolicy: nuova policy	WorkSpaces Secure Browser ha aggiunto una nuova policy per consentire l'accesso ai servizi e alle risorse AWS utilizzati o gestiti da WorkSpaces Secure Browser.	30 novembre 2021
WorkSpaces Secure Browser ha iniziato a tracciare le modifiche	WorkSpaces Secure Browser ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	30 novembre 2021

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

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

Argomenti

- Non sono autorizzato a eseguire un'azione in WorkSpaces Secure Browser
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere alle risorse del mio WorkSpaces Secure Browser

Non sono autorizzato a eseguire un'azione in WorkSpaces Secure Browser

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`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. 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 Secure Browser.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. 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 in WorkSpaces Secure Browser. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere 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`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. 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 risorse del mio WorkSpaces Secure Browser

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se WorkSpaces Secure Browser supporta queste funzionalità, consulta. Come funziona Amazon WorkSpaces Secure Browser con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti 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 IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Utilizzo di ruoli collegati ai servizi per Amazon Secure Browser WorkSpaces

Amazon WorkSpaces Secure Browser utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Secure Browser. WorkSpaces I ruoli collegati ai servizi sono predefiniti da WorkSpaces Secure Browser e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di WorkSpaces Secure Browser perché non è necessario aggiungere manualmente le autorizzazioni necessarie. WorkSpaces Secure Browser definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito,

solo WorkSpaces Secure Browser può assumerne i 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. Ciò protegge le risorse di WorkSpaces Secure Browser perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

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

Argomenti

- Autorizzazioni di ruolo collegate al servizio per Secure Browser WorkSpaces
- Creazione di un ruolo collegato al servizio per Secure Browser WorkSpaces
- Modifica di un ruolo collegato al servizio per Secure Browser WorkSpaces
- Eliminazione di un ruolo collegato al servizio per Secure Browser WorkSpaces
- Regioni supportate per i ruoli collegati WorkSpaces al servizio Secure Browser

Autorizzazioni di ruolo collegate al servizio per Secure Browser WorkSpaces

WorkSpaces Secure Browser utilizza il ruolo collegato al servizio denominato`AWSServiceRoleForAmazonWorkSpacesWeb`: WorkSpaces Secure Browser utilizza questo ruolo collegato al servizio per accedere alle risorse Amazon EC2 degli account dei clienti per lo streaming di istanze e parametri. CloudWatch

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

- `workspaces-web.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AmazonWorkSpacesWebServiceRolePolicy` consente a WorkSpaces Secure Browser di completare le seguenti azioni 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 al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato al servizio per Secure Browser WorkSpaces

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei il tuo primo portale nella Console di gestione AWS, o nell' AWS API AWS CLI, WorkSpaces Secure Browser 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 tuo primo portale, WorkSpaces Secure Browser crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato al servizio con lo use case WorkSpaces Secure Browser. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del 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, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato al servizio per Secure Browser WorkSpaces

WorkSpaces Secure Browser non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonWorkSpacesWeb` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile 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.

Eliminazione di un ruolo collegato al servizio per Secure Browser WorkSpaces

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, 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 al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio WorkSpaces Secure Browser utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l’operazione.

Per eliminare le risorse WorkSpaces Secure Browser utilizzate da AWSService RoleForAmazonWorkSpacesWeb

- 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 mediante IAM

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

Regioni supportate per i ruoli collegati WorkSpaces al servizio Secure Browser

WorkSpaces Secure Browser supporta l'utilizzo di ruoli collegati al servizio 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 Secure Browser

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

Convalida della conformità per Amazon WorkSpaces Secure Browser

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

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

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta AWS la documentazione sulla sicurezza.

Resilienza in Amazon WorkSpaces Secure Browser

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Le seguenti opzioni non sono attualmente supportate da WorkSpaces Secure Browser:

- Backup dei contenuti tra le nostre AZs regioni
- Backup crittografati
- Crittografia dei contenuti in transito tra o regioni AZs
- 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 Secure Browser

In quanto servizio gestito, Amazon WorkSpaces Secure Browser è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad Amazon WorkSpaces Secure Browser attraverso la rete. I client 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.

WorkSpaces Secure Browser isola il traffico di servizio applicando l'autenticazione e l'autorizzazione AWS SigV4 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 Secure Browser

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

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

Accesso APIs tramite un endpoint VPC di interfaccia ()AWS PrivateLink

Puoi chiamare direttamente l'endpoint dell'API Amazon WorkSpaces Secure Browser dall'interno di un cloud privato (VPC), anziché connetterti tramite Internet. Puoi farlo senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect

Stabilisci questa connessione privata creando un endpoint VPC di interfaccia alimentato da. AWS PrivateLink Per ogni sottorete specificata dal VPC, creiamo un'interfaccia di rete endpoint nella sottorete. Un'interfaccia di rete endpoint è un'interfaccia di rete gestita dal richiedente che funge da punto di ingresso per il traffico dell'API Amazon WorkSpaces Secure Browser.

Per ulteriori informazioni, consulta Accedere ai servizi tramite AWS. AWS PrivateLink

Argomenti

- Considerazioni per Amazon WorkSpaces Secure Browser
- Creazione di un endpoint VPC di interfaccia per Amazon Secure Browser WorkSpaces
- Creazione di una policy sugli endpoint per l'endpoint VPC di interfaccia
- Risoluzione dei problemi

Considerazioni per Amazon WorkSpaces Secure Browser

Prima di configurare un endpoint VPC di interfaccia per Amazon WorkSpaces Secure Browser APIs, assicurati di esaminare i «Prerequisiti» nei servizi di Access tramite. AWSAWS PrivateLink Amazon WorkSpaces Secure Browser supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint VPC dell'interfaccia.

Per impostazione predefinita, l'accesso completo ad Amazon WorkSpaces Secure Browser è consentito tramite l'endpoint. Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Creazione di un endpoint VPC di interfaccia per Amazon Secure Browser WorkSpaces

Puoi creare un endpoint VPC di interfaccia per il servizio Amazon WorkSpaces Secure Browser utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consultare Creazione di un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC di interfaccia per Amazon WorkSpaces Secure Browser utilizzando il seguente nome di servizio:

- com.amazonaws. *region*.workspaces-web

Per le regioni supportate da FIPS, crea un endpoint VPC di interfaccia per WorkSpaces Amazon Secure Browser utilizzando il seguente nome di servizio:

- com.amazonaws. *region*. workspaces-web-fips

Creazione di una policy sugli endpoint per l'endpoint VPC di interfaccia

Una policy per gli endpoint è una risorsa IAM che puoi collegare a un endpoint VPC di interfaccia. La policy predefinita per gli endpoint ti offre l'accesso completo ad Amazon WorkSpaces Secure Browser APIs tramite l'interfaccia VPC endpoint. Per controllare l'accesso concesso ad Amazon WorkSpaces Secure Browser dal tuo VPC, collega una policy personalizzata per gli endpoint all'endpoint VPC dell'interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

Esempio: policy sugli endpoint VPC per le azioni di Amazon Secure Browser WorkSpaces

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando colleghi questa policy all'endpoint VPC dell'interfaccia, concede l'accesso alle azioni elencate di Amazon WorkSpaces Secure Browser per tutti i principali su tutte le risorse.

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

Risoluzione dei problemi

Se le chiamate ad Amazon WorkSpaces Secure Browser APIs sono bloccate, è probabile che si tratti di un'errata configurazione nel gruppo di sicurezza VPC Endpoint Service o nella configurazione del ruolo IAM. Per risolvere il problema, prova quanto segue:

- Durante la creazione dell'endpoint VPC di interfaccia, potrebbe essere stato collegato automaticamente al gruppo di sicurezza predefinito Account AWS del tuo. Prova a utilizzare un gruppo di sicurezza diverso e assicurati che le autorizzazioni in entrata e in uscita ti consentano di trasferire i dati in modo appropriato.
- Assicurati di utilizzare un ruolo IAM che ti consenta di chiamare Amazon WorkSpaces Secure Browser APIs.

Per ulteriori informazioni, consulta Cos'è AWS PrivateLink? nella Guida per l'utente di Amazon VPC.

Best practice di sicurezza per Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser offre una serie di funzionalità di sicurezza che puoi utilizzare per sviluppare e implementare le tue politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Le best practice per Amazon WorkSpaces Secure Browser includono quanto segue:

- Per rilevare potenziali eventi di sicurezza associati all'utilizzo di WorkSpaces Secure Browser, 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 Secure Browser con Amazon CloudWatch e Registrazione delle chiamate API di WorkSpaces Secure Browser utilizzando AWS CloudTrail.
- Per implementare i controlli investigativi e identificare le anomalie, utilizza CloudTrail log e metriche. CloudWatch Per ulteriori informazioni, consulta Monitoraggio di Amazon WorkSpaces Secure Browser con Amazon CloudWatch e Registrazione delle chiamate API di WorkSpaces Secure Browser utilizzando AWS CloudTrail.

- È possibile configurare la registrazione degli accessi degli utenti per tenere traccia degli eventi degli utenti. Per ulteriori informazioni, consulta the section called “Configurazione della registrazione delle attività degli utenti”.

Per prevenire potenziali eventi di sicurezza associati all'uso di WorkSpaces Secure Browser, segui queste best practice:

- Implementa l'accesso con privilegi minimi e crea ruoli specifici da utilizzare per le azioni di WorkSpaces Secure Browser. Utilizza i modelli IAM per creare un ruolo con accesso completo o di sola lettura. Per ulteriori informazioni, consulta AWS politiche gestite per WorkSpaces Secure Browser.
- 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 Secure Browser

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon WorkSpaces Secure Browser e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare i portali WorkSpaces Secure Browser 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 tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri per le tue EC2 istanze Amazon 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 registro da EC2 istanze Amazon e altre fonti. CloudTrail 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 di .

Argomenti

- Monitoraggio di Amazon WorkSpaces Secure Browser con Amazon CloudWatch
- Registrazione delle chiamate API di WorkSpaces Secure Browser utilizzando AWS CloudTrail
- Registrazione delle attività degli utenti in Amazon WorkSpaces Secure Browser

Monitoraggio di Amazon WorkSpaces Secure Browser con Amazon CloudWatch

Puoi monitorare Amazon WorkSpaces Secure Browser 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 WorkSpaces Secure Browser

Parametro	Descrizione	Dimensioni	Statistiche	Unità
`SessionAttempt`	Il numero di tentativi di sessione di Amazon WorkSpaces Secure Browser.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio
`SessionSuccess`	Il numero di sessioni Amazon WorkSpaces Secure Browser avviate con successo.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio
`SessionFailure`	Il numero di sessioni non riuscite di Amazon WorkSpaces Secure Browser.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio
`SessionIdleDisconnect`	Il numero di connessioni chiuse a causa dell'inattività dell'utente.	`[PortalId]`	Media	Conteggio

Parametro	Descrizione	Dimensioni	Statistiche	Unità
`ActiveSession`	Il numero di sessioni attive su un portale.	`[PortalId]`	Media	Conteggio
`GlobalCpuPercent`	L'utilizzo della CPU dell'istanza di sessione Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Media, Somma, Massimo, Minimo	Percentuale
`GlobalMemoryPercent`	L'utilizzo della memoria (RAM) dell'istanza di sessione di Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Media, Somma, Massimo, Minimo	Percentuale
`DisplayLatency`	Il tempo medio in millisecondi tra l'acquisizione del fotogramma e la presentazione.	`[PortalId]` `[PortalId, UserName]`	Media, massima, minima	Millisecondi
`InputLatency`	La latenza di input tra client e server. Ad esempio, la latenza tra il clic del mouse del client e il clic del mouse del server.	`[PortalId]` `[PortalId, UserName]`	Media, massima, minima	Millisecondi

Parametro	Descrizione	Dimensioni	Statistiche	Unità
`SessionLoggerEventDelivered`	Il numero di eventi di ogni file Session Logger consegnato.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio
`SessionLoggerTargetNotFoundError`	Il numero di consegne di file di registro che hanno comportato l'impossibilità di trovare il bucket.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio
`SessionLoggerAccessDeniedError`	Il numero di consegne di file di registro che hanno comportato il rifiuto delle autorizzazioni.	`[PortalId]`	Media, Somma, Massimo, Minimo	Conteggio

> **Note**
>
> I punti dati metrici vengono raccolti da ogni sessione una volta al minuto e pubblicati una CloudWatch volta ogni 5 minuti. Le metriche del Session Logger vengono emesse immediatamente, per ogni consegna del file di registro.

Dimensioni per i parametri di Amazon WorkSpaces Secure Browser

Dimensione	Descrizione
PortalId	Filtra i dati metrici per Amazon WorkSpaces Secure Browser per un portale specifico.

Dimensione	Descrizione
UserName	Filtra i dati metrici per Amazon WorkSpace s Secure Browser per un portale e un utente specifici.

Puoi utilizzare la SessionLoggerEventDeliveredmetrica per monitorare il numero aggregato di eventi dal tuo portale o visualizzare il numero di file di log forniti contando il numero di punti dati anziché sommando i valori. Ti consigliamo di configurare gli allarmi sulle SessionLoggerAccessDeniedErrormetriche SessionLoggerTargetNotFoundErrore per rilevare l'eliminazione accidentale di risorse o autorizzazioni.

Registrazione delle chiamate API di WorkSpaces Secure Browser utilizzando AWS CloudTrail

WorkSpaces Secure Browser è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon WorkSpaces Secure Browser. CloudTrail acquisisce tutte le chiamate API per Amazon WorkSpaces Secure Browser come eventi. Queste includono le chiamate dalla console Amazon WorkSpaces Secure Browser e le chiamate in codice alle operazioni dell'API Amazon WorkSpaces Secure Browser. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon WorkSpaces Secure Browser. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi identificare la richiesta effettuata ad Amazon WorkSpaces Secure Browser, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Argomenti

- WorkSpaces Informazioni su Secure Browser in CloudTrail
- Informazioni sulle voci dei file di registro di WorkSpaces Secure Browser

WorkSpaces Informazioni su Secure Browser in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon WorkSpaces Secure Browser, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Nella cronologia degli eventi, puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon WorkSpaces Secure Browser, puoi creare un percorso. Un trail consente di CloudTrail inviare file di log a 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 della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Amazon WorkSpaces Secure Browser vengono registrate CloudTrail e documentate nell'Amazon WorkSpaces API Reference. Ad esempio, le chiamate a `DeleteUserSettings` e `CreatePortal` le `ListBrowserSettings` azioni generano voci nei file di CloudTrail registro.

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 AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro di WorkSpaces Secure Browser

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e altri dettagli. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ListBrowserSettings`azione.


```
{
   "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 delle attività degli utenti in Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser consente ai clienti di registrare gli eventi di sessione relativi alle attività degli utenti nelle sessioni Secure del browser.

WorkSpaces Secure Browser offre due opzioni per la registrazione delle attività degli utenti e degli eventi relativi alla sicurezza:

- Session Logger acquisisce un'ampia gamma di eventi di sessione. Questi log vengono inviati a un bucket Amazon S3 nel tuo account, per una facile integrazione con la tua piattaforma SIEM preferita.
- La registrazione degli accessi degli utenti registra gli eventi di sessione più critici. Questi log vengono trasmessi in streaming a un flusso Amazon Kinesis per l'elaborazione e l'analisi in tempo reale.

Per ulteriori informazioni su come configurare queste opzioni, consulta e. the section called “Configurazione di Session Logger” the section called “Configurazione della registrazione degli accessi degli utenti”

Argomenti

- Eventi di sessione in Session Logger per Amazon WorkSpaces Secure Browser
- Eventi di sessione nella registrazione degli accessi utente per Amazon WorkSpaces Secure Browser

Eventi di sessione in Session Logger per Amazon WorkSpaces Secure Browser

Session Logger acquisisce vari eventi relativi alla sessione per scopi di monitoraggio e controllo.

È possibile configurare Session Logger per raccogliere tutti gli eventi della sessione o un sottoinsieme selezionato, a seconda delle esigenze del portale Secure Browser. WorkSpaces Per ulteriori informazioni sulla configurazione, vedere. the section called “Configurazione di Session Logger”

Per mantenere la privacy degli utenti, Session Logger non registra contenuti sensibili, come i dati degli appunti o il contenuto dei file caricati o scaricati.

I seguenti campi sono inclusi in tutti gli eventi:

- Time (Orario)
- Nome utente
- ID del portale

- IP del portale
- IP del cliente
- ID della sessione

Nome	Descrizione	Campi aggiuntivi inclusi nell'evento
SessionStart	È stata avviata una sessione sicura del browser, ma l'utente non si è ancora connesso.	
SessionConnect	L'utente è connesso alla sessione sicura del browser.	
TabOpen	Nella sessione sicura del browser, l'utente ha aperto una nuova scheda o ha aperto un collegamento in una nuova scheda.	Nome host, percorso, URL (se l'utente apre un link in una nuova scheda), nessuno (se l'utente apre una nuova scheda)
UrlVisit	Nella sessione del browser, l'utente ha navigato verso un URL.	Nome host, percorso, URL
WebsiteInteract	L'utente ha modificato un elemento HTML standard su un sito Web (ad esempio, fa clic su una casella di controllo , un pulsante di opzione o un pulsante o seleziona un elemento nel menu a discesa).	Nome host, percorso, URL
TabClose	Nella sessione del browser, l'utente ha chiuso una scheda.	Nome host, percorso, URL (se l'utente chiude una scheda verso cui ha navigato), nessuno (se l'utente chiude una nuova scheda)

Nome	Descrizione	Campi aggiuntivi inclusi nell'evento
ContentTransferFromLocalToRemoteClipboard	L'utente ha aggiornato gli appunti all'interno del browser sicuro utilizzando il contenuto del browser locale (al di fuori dell'ambiente sicuro). Questo aggiornamento può avvenire copiando il contenuto tramite la barra degli strumenti della sessione o trasferendo i dati tramite scorciatoie da tastiera (Ctrl+C/Ctrl+V).	
ContentCopyFromWebsite	L'utente ha aggiornato gli appunti all'interno del browser sicuro utilizzando il contenuto del browser sicuro (all'interno dell'ambiente sicuro).	Nome host, percorso, URL
ContentPasteToWebsite	Il contenuto degli appunti è stato incollato in una pagina Web all'interno del browser. (Questo evento non acquisisce i casi in cui il contenuto degli appunti viene incollato nella barra degli URL del browser.)	Nome host, percorso, URL
PrintJobSubmit	L'utente ha inviato una richiesta di lavoro alla stampante virtuale del browser («DCV Printer»). Il contenuto viene salvato come PDF sul computer locale dell'utente.	Nome, dimensione, estensione del file

Nome	Descrizione	Campi aggiuntivi inclusi nell'evento
FileDownloadFromSecureBrowserToRemoteDisk	Un file è stato salvato dalla sessione sul disco locale dell'istanza remota.	Nome host, percorso URLfilename, dimensione, estensione
FileTransferFromRemoteToLocalDisk	È stato scaricato un file dal disco dell'istanza remota sul dispositivo locale dell'utente.	Nome, dimensione, estensione del file
FileUploadFromRemoteDiskToSecureBrowser	Un file archiviato sul disco locale dell'istanza remota è stato caricato su una piattaforma SaaS per la condivisione di file (ad esempio Google Drive, Box o File.io) tramite la sessione del browser.	
FileTransferFromLocalToRemoteDisk	Un file è stato caricato dal dispositivo dell'utente nella sessione sicura del browser.	Nome, dimensione ed estensione del file
SessionDisconnection	L'utente viene disconnesso dalla sessione sicura del browser.	

Nome	Descrizione	Campi aggiuntivi inclusi nell'evento
SessionEnd	La sessione sicura del browser è terminata. L'interruzione può avvenire in tre modi: l'amministratore termina la sessione tramite User Session Manager nella console, l'utente termina manualmente la sessione utilizzando Termina sessione nella barra degli strumenti o la sessione scade dopo aver superato la durata impostata dall'amministratore.	

Ogni evento segue lo standard OCSF e include un elenco di attributi comuni a tutti gli eventi:

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
    activity_id : Integer | OCSF standard value 99 for 'others'
    category_name : "WorkSpacesSecureBrowser" | The category name where the event
 belongs to.
    category_id : 2 | Numerical identifier for category,
    metadata : link | Required {
        product : link {
            vendor_name : "wsb",
            name : "WorkSpacesSecureBrowser"
        }
        version : String | Version of the schema | eg. 1.0.0
    },
    severity_id : 1 | The severity of the event. All events will have a severity of 1,
 meaning 'Informational',
    type_id : class_uid * 100 + activity_id
    time : The time the event happened (RFC3339 format),
    observables : link [
        {
```

```
            name : "session_detail.portal_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.session_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.client_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.portal_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.username",
            type_id : 10 //Resource UID
            value : //Generated value
        }
    ],

    // New Events
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
        username : String | The logged-in username | eg. bobross
    }
}
```

Di seguito è riportato un esempio dell' URLVisit evento:

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

Di seguito è riportato un esempio dell' PrintJobSubmit evento:

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
}
```

Parametri di Session Logger per Amazon Secure WorkSpaces Browser

Session Logger emette le seguenti metriche. Amazon CloudWatch

È possibile utilizzare la SessionLoggerEventDeliveredmetrica per monitorare il numero aggregato di eventi dal portale o visualizzare il numero di file di registro forniti contando il numero di punti dati anziché sommando i valori. Ti consigliamo di configurare gli allarmi sulle SessionLoggerAccessDeniedErrormetriche SessionLoggerTargetNotFoundErrore per rilevare l'eliminazione accidentale di risorse o autorizzazioni.

> **Note**
>
> I dati metrici vengono raccolti da ogni sessione una volta al minuto e pubblicati una volta ogni 5 minuti. Amazon CloudWatch Le metriche del Session Logger vengono emesse immediatamente, per ogni consegna del file di registro.

Metriche del Session Logger

Parametro	Descrizione	Dimensione	Statistiche	Unità
SessionLoggerEventDelivered	Il numero di eventi di ogni file Session Logger consegnato.	[PortalId]	Media, Somma, Massimo, Minimo	Conteggio
SessionLoggerTargetNotFoundError	Il numero di consegne di file di registro che hanno comportato l'impossibilità di trovare il bucket.	[PortalId]	Media, Somma, Massimo, Minimo	Conteggio
SessionLoggerAccessDeniedError	Il numero di consegne di file di registro che hanno comportat	[PortalId]	Media, Somma, Massimo, Minimo	Conteggio

Parametro	Descrizione	Dimensione	Statistiche	Unità
	o il rifiuto delle autorizzazioni.			

Eventi di sessione nella registrazione degli accessi utente per Amazon WorkSpaces Secure Browser

I seguenti eventi di sessione sono disponibili per la registrazione di User Access:

- Convalida: l'evento è stato inserito correttamente nel flusso di dati Kinesis.
- StartSession: L'utente ha avviato una sessione ed è connesso alla sessione sicura del browser.
- VisitPage: L'utente sta visitando una pagina nella sessione.
- EndSession: L'utente ha terminato la sessione.

I log di navigazione degli URL vengono registrati dalla cronologia del browser. URLs 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 politica del browser.

Di seguito è riportato un esempio di ogni evento disponibile. 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"
}
```

Linee guida per gli utenti di Amazon WorkSpaces Secure Browser

Gli amministratori utilizzano WorkSpaces Secure Browser 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 a WorkSpaces Secure Browser, sull'avvio e sulla configurazione di una sessione e sull'utilizzo della barra degli strumenti e del browser Web.

Argomenti

- Compatibilità di browser e dispositivi per Amazon WorkSpaces Secure Browser
- Accesso al portale Web per Amazon WorkSpaces Secure Browser
- Guida alla sessione per Amazon WorkSpaces Secure Browser
- Risoluzione dei problemi degli utenti in Amazon WorkSpaces Secure Browser
- Estensione Single Sign-On per Amazon Secure Browser WorkSpaces

Compatibilità di browser e dispositivi per Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser è alimentato dal client del browser Web Amazon 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 per Amazon WorkSpaces Secure Browser

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 per Amazon WorkSpaces Secure Browser

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

Argomenti

- Avvio di una sessione in Amazon WorkSpaces Secure Browser
- Utilizzo della barra degli strumenti in Amazon WorkSpaces Secure Browser
- Utilizzo del browser in Amazon WorkSpaces Secure Browser
- Terminare una sessione in Amazon WorkSpaces Secure Browser

Avvio di una sessione in Amazon WorkSpaces Secure Browser

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 Secure Browser sta creando una sessione per te. Dietro le quinte, Amazon WorkSpaces Secure Browser 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 Secure Browser 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.

Utilizzo della barra degli strumenti in Amazon WorkSpaces Secure Browser

Per imparare a usare la barra degli strumenti, segui questi passaggi.

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 con la freccia rivolta verso l'alto 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 aumentare le dimensioni dello schermo, seleziona la finestra del browser e ingrandisci. Per aumentare le dimensioni di visualizzazione delle icone e del testo della barra degli strumenti, selezionate la barra degli strumenti e ingrandisci.

Per ingrandire o ridurre un dispositivo Windows, procedi nel seguente modo:

1. Seleziona la barra degli strumenti o il contenuto web.

2. Premi Ctrl + per ingrandire o premi Ctrl + - per rimpicciolire.

Per ingrandire o ridurre su un dispositivo Mac, segui questi passaggi:

1. Seleziona la barra degli strumenti o il contenuto web.
2. Premi Cmd + per ingrandire o premi Cmd + - per rimpicciolire.

Per ancorare la barra degli strumenti alla parte superiore dello schermo, scegli Preferenze, Generali e Ancorato 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. Use the down arrow to select from a list of available microphones.
	Webcam	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	Preferences	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	Profile	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	Notifications	Get one-click access to session notifications.
	Clipboard	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	Files	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.
	Functions	To add functions to your toolbar, choose **Preferences**, **Keyboard**, and choose **Functions**. Functions allows you to enter special keystrokes or key combinations.

> **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.

Utilizzo del browser in Amazon WorkSpaces Secure 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 in Amazon WorkSpaces Secure Browser

Per terminare una sessione, scegli Profilo e Termina sessione. Al termine di una sessione, Amazon WorkSpaces Secure Browser 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 degli utenti in Amazon WorkSpaces Secure Browser

Se riscontri uno dei seguenti problemi durante l'utilizzo di WorkSpaces Secure Browser, prova le seguenti risoluzioni.

Il mio portale Amazon WorkSpaces Secure Browser 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.

Amazon WorkSpaces Secure Browser reindirizza il video (AV) in tempo reale 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.

Come posso sapere quale microfono e and/or webcam è in uso e come posso cambiarlo?

Fai clic sull'icona della freccia rivolta verso il basso accanto al microfono o alla videocamera. Il menu mostra i dispositivi disponibili, con un segno di spunta che indica il dispositivo corrente. Seleziona un dispositivo diverso per cambiare il dispositivo che desideri utilizzare per la sessione.

Il mio portale web non si avvia se si accede direttamente dal dominio personalizzato dell'azienda

Se stai cercando di avviare una sessione utilizzando un nome di dominio non workspaces-web.comacme`.secureportal.mycompany.com`, assicurati che il tuo browser abbia abilitato i cookie di terze parti per il dominio aziendale a cui stai accedendo.

Estensione Single Sign-On per Amazon Secure Browser WorkSpaces

Amazon WorkSpaces Secure Browser 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 Secure Browser 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.

Argomenti

- Compatibilità delle estensioni Single Sign-On per Amazon Secure Browser WorkSpaces
- Installazione dell'estensione Single Sign-On per Amazon Secure Browser WorkSpaces
- Risoluzione dei problemi relativi all'estensione Single Sign-On per Amazon Secure Browser WorkSpaces

Compatibilità delle estensioni Single Sign-On per Amazon Secure Browser WorkSpaces

L'estensione Single Sign-On funziona con i seguenti dispositivi e browser:

- dispositivi
  - Computer portatili
  - Computer desktop
- Browser
  - Google Chrome
  - Mozilla Firefox

Installazione dell'estensione Single Sign-On per Amazon Secure Browser WorkSpaces

Per installare l'estensione Single Sign-On, segui questi passaggi.

Quando accedi al portale, segui le istruzioni per installare l'estensione per il tuo browser Chrome o Firefox. 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 finestra di navigazione, anziché in Incognito (Chrome) o Private Browsing (Firefox).

Risoluzione dei problemi relativi all'estensione Single Sign-On per Amazon Secure Browser WorkSpaces

Durante l'utilizzo dell'estensione Single Sign-On, potresti riscontrare il seguente problema.

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 Secure Browser 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 Secure Browser Administration Guide

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

Modifica	Descrizione	Data
Session Logger	Configura Session Logger per acquisire un'ampia gamma di eventi di sessione.	1 agosto 2025
CloudWatch metriche	CloudWatch Metriche aggiornate.	21 luglio 2025
Controlli della barra degli strumenti	Con i controlli della barra degli strumenti, è possibile configurare la presentazione della barra degli strumenti per le sessioni degli utenti finali.	21 febbraio 2025
Accesso APIs tramite un endpoint VPC di interfaccia ()AWS PrivateLink	Chiama direttamente l'endpoint dell'API Amazon WorkSpaces Secure Browser dall'interno di un cloud privato (VPC), anziché connetterti tramite Internet.	10 gennaio 2025
Impostazioni di protezione dei dati	Aggiungi le impostazioni di protezione dei dati per proteggere i dati dalla condivisione durante una sessione.	20 novembre 2024
Endpoint FIPS	Proteggi i dati in transito con gli endpoint FIPS.	7 ottobre 2024

Dashboard di gestione delle sessioni	Utilizza la dashboard di gestione delle sessioni per monitorare e gestire le sessioni attive e complete.	19 settembre 2024
Consenti collegamenti diretti	Consenti ai portali di ricevere link diretti che collegano gli utenti a un sito Web specifico durante una sessione.	25 giugno 2024
Aggiornamento della policy gestita	È stata aggiunta una politica AmazonWorkSpacesSecureBrowserReadOnly gestita	24 giugno 2024
Usa la barra degli strumenti per ingrandire	Puoi aumentare le dimensioni del display, delle icone e del testo con la barra degli strumenti.	1º maggio 2024
Nuove impostazioni del portale web	Ora puoi specificare il tipo di istanza e il limite massimo di utenti simultanei per il tuo portale web.	22 aprile 2024
CloudWatch metriche	Aggiunte GlobalCpuPercent e GlobalMemoryPercent metriche.	26 febbraio 2024
Configura il filtraggio degli URL	Puoi utilizzare Chrome Policy per filtrare URLs gli utenti a cui possono accedere dal 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
Guida per l'utente per Amazon WorkSpaces Secure Browser	Sono stati aggiunti contenuti per aiutare gli utenti finali a scoprire di più sull'accesso ad Amazon WorkSpaces Secure Browser, sull'avvio e la configurazione di una sessione e sull'utilizzo della barra degli strumenti e del browser Web.	17 luglio 2023
Controlli sugli accessi degli IP	WorkSpaces Secure Browser ti consente di controllare da quali indirizzi IP è possibile accedere al tuo portale web.	31 maggio 2023
Aggiornamento della policy gestita	Politica AmazonWorkSpacesWebReadOnly gestita aggiornata	15 maggio 2023
Configura l'aggiornamento del gestore dell'identità digitale	WorkSpaces Secure Browser offre due tipi di autenticazione: Standard e Centro identità AWS IAM	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	È stata aggiornata la politica AmazonWorkSpacesWebServiceRolePolicy gestita per aggiungere lo spazio dei nomi alle autorizzazioni dell'API PutMetricData AWS/Usage	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 Secure Browser 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.