aws

Guida per l'amministratore

Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client: Guida per l'amministratore

Table of Contents

Cos'è la console di amministrazione di Amazon WorkSpaces Thin Client?

Con la console di amministrazione di Amazon WorkSpaces Thin Client, gli amministratori possono gestire ambienti e dispositivi WorkSpaces Thin Client tramite un portale WorkSpaces Thin Client. Da questa console Web, gli amministratori possono creare ambienti, gestire dispositivi e impostare parametri per gli utenti WorkSpaces Thin Client all'interno della propria rete.

Gli ambienti desktop virtuali utilizzati per WorkSpaces Thin Client devono essere creati o modificati all'interno della propria console.

> **Important**
>
> Affinché la console di amministrazione WorkSpaces Thin Client funzioni correttamente, il sistema deve prima soddisfare requisiti specifici. Questi requisiti sono elencati in Prerequisiti e configurazioni.

Argomenti

È il primo utilizzo?

Se utilizzi per la prima volta la console di amministrazione WorkSpaces Thin Client, ti consigliamo di iniziare leggendo le seguenti sezioni:

- Avvio della console di amministrazione WorkSpaces Thin Client
- Utilizzo della console di amministrazione WorkSpaces Thin Client

Architettura

Ogni WorkSpaces Thin Client è associato a un provider di interfaccia desktop virtuale (VDI). WorkSpaces Thin Client supporta tre provider VDI:

- Amazon WorkSpaces
- AppStream 2.0
- Browser WorkSpaces sicuro Amazon

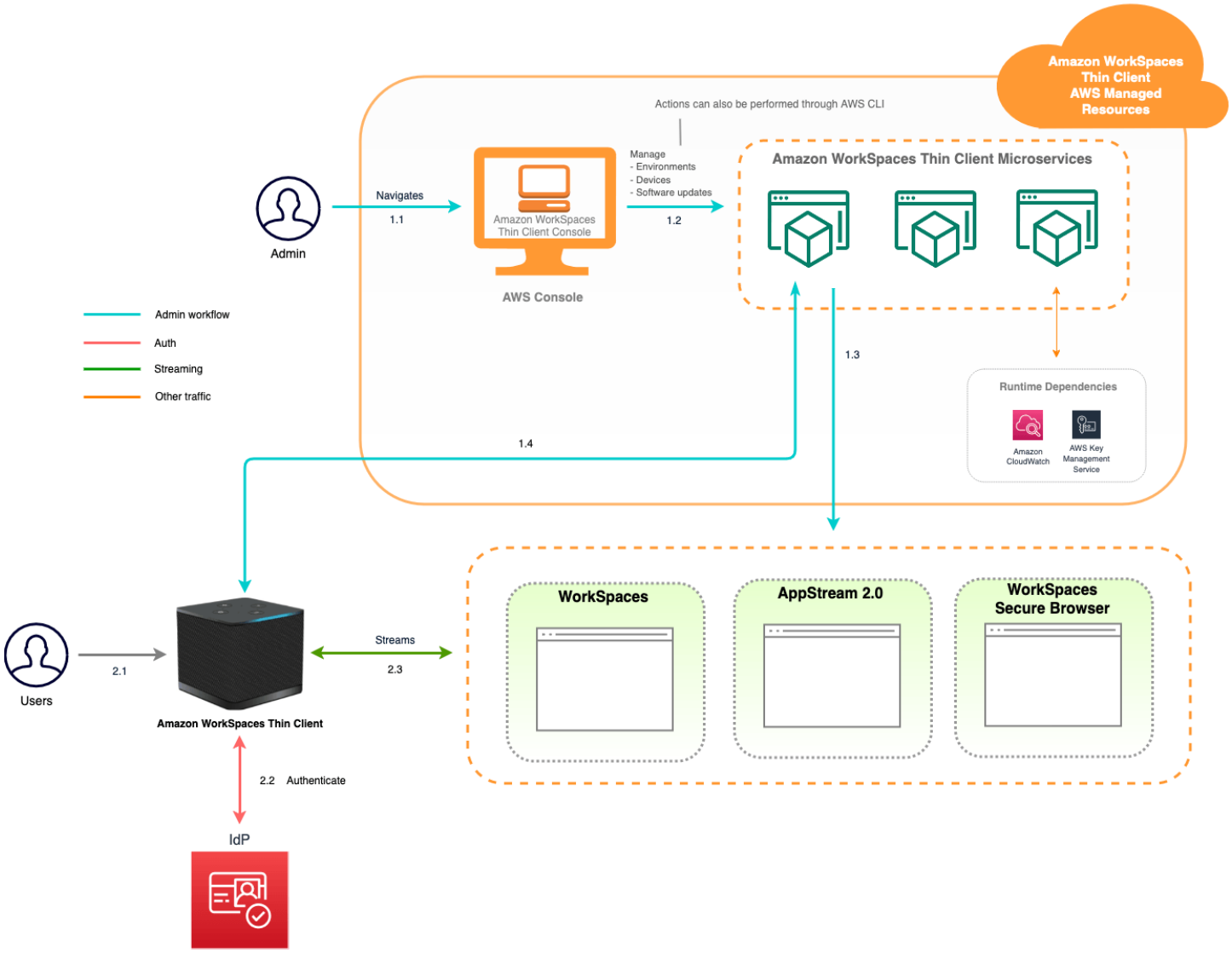
A seconda della VDI utilizzata, è possibile accedere e gestire le informazioni relative al WorkSpaces Thin Client tramite le directory per WorkSpaces, gli stack per la AppStream versione 2.0 e gli endpoint del portale Web per Secure Browser. WorkSpaces

Per ulteriori informazioni su Amazon WorkSpaces, consulta la sezione Introduzione alla configurazione WorkSpaces rapida. Le directory sono gestite tramite AWS Directory Service, che offre le seguenti opzioni: Simple AD, AD Connector o AWS Directory Service per Microsoft Active Directory, noto anche come AWS Managed Microsoft AD. Per ulteriori informazioni, consulta la Guida di amministrazione di AWS Directory Service.

Per ulteriori informazioni sulla AppStream versione 2.0, consulta Get Started with Amazon AppStream 2.0: Configurazione con applicazioni di esempio. AppStream 2.0 gestisce le AWS risorse necessarie per ospitare ed eseguire le applicazioni, si ridimensiona automaticamente e fornisce l'accesso agli utenti su richiesta. AppStream 2.0 fornisce agli utenti l'accesso alle applicazioni di cui hanno bisogno sul dispositivo di loro scelta, con un'esperienza utente reattiva e fluida, indistinguibile dalle applicazioni installate nativamente.

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

Il diagramma seguente mostra l'architettura di Thin Client. WorkSpaces


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
Admin workflow
Auth
Streaming
Other traffic
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
1.4
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
2.2 Authenticate
IdP

Configurazione della console di amministrazione Amazon WorkSpaces Thin Client

Argomenti

Registrazione ad AWS

Se non ne hai una Account AWS, completa i seguenti passaggi per crearne una.

Per iscriverti a un Account AWS

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

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

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Crea un utente IAM

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle best practice, consulta Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .	Configura l'accesso programmatico configurando l'uso AWS IAM Identity Center nella AWS CLI Guida per l'utente.AWS Command Line Interface
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Segui le istruzioni in Creazione del primo utente e gruppo di utenti IAM di amministrazione nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Inizia a usare la tua VDI per Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client è un dispositivo thin client conveniente progettato per funzionare con i servizi di AWS End User Computing per fornirti un accesso sicuro e immediato alle applicazioni e ai desktop virtuali.

Scegli un'infrastruttura desktop virtuale (VDI) e configurala per funzionare con Thin Client. WorkSpaces

> **Important**
>
> Affinché la console di amministrazione WorkSpaces Thin Client funzioni correttamente, il sistema deve prima soddisfare requisiti specifici. Questi requisiti sono elencati nella procedura di configurazione per ogni provider di desktop virtuale.

WorkSpaces Thin Client richiede configurazioni software specifiche, a seconda del provider di desktop virtuale.

Argomenti

- Configurazione WorkSpaces per Amazon WorkSpaces Thin Client
- Configurazione AppStream 2.0 per Amazon WorkSpaces Thin Client
- Configurazione di Amazon WorkSpaces Secure Browser per Amazon WorkSpaces Thin Client

Configurazione WorkSpaces per Amazon WorkSpaces Thin Client

Affinché WorkSpaces Thin Client possa essere utilizzato con Amazon WorkSpaces, il servizio deve essere configurato per accedere alle WorkSpaces directory. Amazon WorkSpaces è elencato in base ai nomi delle directory nella pagina dell'ambiente WorkSpaces Thin Client Create all'interno della AWS console.

> **Note**
>
> Le configurazioni devono essere effettuate prima di utilizzare la console per la prima volta. Non è consigliabile modificare le funzionalità dei prerequisiti dopo aver iniziato a utilizzare la console.

Prima di iniziare

Assicurati di disporre di un AWS account per creare o amministrare un. WorkSpace Gli utenti dei dispositivi, tuttavia, non hanno bisogno di un AWS account a cui connettersi e utilizzare i propri WorkSpaces.

Esamina e comprendi i seguenti concetti prima di procedere con la configurazione:

- Quando lanci un WorkSpace, seleziona un WorkSpace pacchetto. Per ulteriori informazioni, consulta Amazon WorkSpaces Bundles.
- Quando avvii un WorkSpace, seleziona il protocollo che desideri utilizzare con il tuo pacchetto. Per ulteriori informazioni, consulta Protocols for Amazon WorkSpaces.
- Quando avvii un WorkSpace, specifica le informazioni del profilo per ogni utente, inclusi nome utente e indirizzo e-mail. Gli utenti completano i propri profili creando una password. Le informazioni sugli utenti WorkSpaces e sugli utenti vengono archiviate in una directory. Per ulteriori informazioni, consulta Gestire le directory per WorkSpaces.
- Quando avvii un WorkSpace, abilita e configura l'accesso WorkSpaces Web. Per ulteriori informazioni, consulta Abilitare e configurare Amazon WorkSpaces Web Access

Fase 1: Verifica che il sistema soddisfi le funzionalità WorkSpaces richieste

Affinché la console di amministrazione WorkSpaces Thin Client funzioni correttamente con Amazon WorkSpaces, il sistema deve soddisfare i seguenti requisiti specifici. Questa tabella elenca tutte queste funzionalità supportate e i relativi requisiti.

Funzionalità	Requisito
Accesso Web	Abilitato
Sistema operativo supportato	• Windows 10

Funzionalità	Requisito
	• Windows 10 (BYOL) • Windows 11 • Windows 11 (BYOL)
Pacchetti supportati	• Microsoft Power con Windows 10 (basato su Server 2016, 2019 e 2022) • Microsoft Power con Windows 10 (basato su Server 2016, 2019 e 2022) con Office • Microsoft PowerPro con Windows 10 (basato su Server 2016, 2019 e 2022) • Microsoft PowerPro con Windows 10 (basato su Server 2016, 2019 e 2022) con Office • Microsoft Performance con Windows 10 (basato su Server 2016, 2019 e 2022) • Microsoft Performance con Windows 10 (basato su Server 2016, 2019 e 2022) con Office
Protocolli supportati	Solo WSP

Passaggio 2: utilizza la configurazione avanzata per avviare il WorkSpace

Per utilizzare la configurazione avanzata per avviare il WorkSpace

1. Apri la WorkSpaces console all'indirizzohttps://console.aws.amazon.com/workspaces/.
2. Scegli una dei seguenti tipi di directory e quindi seleziona Successivo:
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. Inserisci le informazioni sulla directory.
4. In un VPC, scegli due sottoreti appartenenti a due zone di disponibilità diverse. Per ulteriori informazioni, consulta Configurazione di un VPC con sottoreti pubbliche.

5. Controlla le informazioni sulla tua directory e scegli Crea cartella.

Configurazione AppStream 2.0 per Amazon WorkSpaces Thin Client

AppStream Le istanze 2.0 verranno elencate in base ai nomi dello stack e richiederanno la configurazione di un URL di accesso IdP nella pagina di creazione dell'ambiente. Poiché l'autenticazione SAML per AppStream 2.0 supporta solo l'autenticazione avviata, l'amministratore dovrà inserire manualmente l'URL di accesso corretto.

> **Note**
>
> Le configurazioni devono essere effettuate prima di utilizzare la console per la prima volta. Non è consigliabile modificare le funzionalità dei prerequisiti dopo aver iniziato a utilizzare la console.

Fase 1: Verificare che il sistema soddisfi le funzionalità richieste dalla AppStream versione 2.0

Affinché la console di amministrazione WorkSpaces Thin Client funzioni correttamente con la AppStream versione 2.0, il sistema deve soddisfare i seguenti requisiti specifici. Questa tabella elenca tutte queste funzionalità supportate e i relativi requisiti.

Funzionalità	Requisito
Provider di identità	Vai alla sezione Configurazione di SAML nella Guida per amministratori AppStream 2.0 per creare un provider di identità. Quando ti viene richiesto di creare una console env, inserisci l'URL di accesso IDP.
Sistema operativo	Windows
Tipo di piattaforma	Windows Server (2012 R2, 2016 o 2019)

Funzionalità	Requisito
Protocollo di streaming	Streaming TCP Se UDP non è disponibile, esiste un meccanismo di fallback automatico su TCP.
Copia e incolla locali	Disabilita Configurato a livello AppStream di stack 2.0
Condivisione di cartelle locali	Disabilita Configurato a livello di AppStream stack 2.0
Stampa locale	Disabilita Configurato a livello di AppStream stack 2.0

È supportato anche il requisito del blocco dello schermo tramite l'autenticazione SAML su AppStream 2.0. I meccanismi di autenticazione User Pool e Programmatic non sono supportati su WorkSpaces Thin Client.

Fase 2: Configura i tuoi stack AppStream 2.0

Per lo streaming delle applicazioni, la AppStream versione 2.0 richiede un ambiente che includa una flotta associata a uno stack e almeno un'immagine dell'applicazione. Segui questi passaggi per configurare una flotta e uno stack e consentire agli utenti di accedere allo stack. Se non l'hai ancora fatto, ti consigliamo di provare le procedure descritte nella Guida introduttiva alla AppStream versione 2.0: Configurazione con applicazioni di esempio.

Se desideri creare un'immagine da usare, consulta Tutorial: Creare un'immagine AppStream 2.0 personalizzata utilizzando la console AppStream 2.0.

Se prevedi di aggiungere un parco istanze a un dominio Active Directory, configura tale dominio prima di completare la procedura seguente. Per ulteriori informazioni, consulta Usare Active Directory con AppStream 2.0.

Attività

- Creazione di un parco istanze
- Creazione di uno stack
- Fornire accesso agli utenti
- Pulizia delle risorse

Configurazione di Amazon WorkSpaces Secure Browser per Amazon WorkSpaces Thin Client

Amazon WorkSpaces Secure Browser si basa sugli endpoint del portale Web nella pagina dell'ambiente WorkSpaces Thin Client Create all'interno della AWS console.

> **Note**
>
> Le configurazioni devono essere effettuate prima di utilizzare la console per la prima volta. Non è consigliabile modificare le funzionalità dei prerequisiti dopo aver iniziato a utilizzare la console.

Passaggio 1: verifica che il sistema soddisfi le funzionalità richieste da Amazon WorkSpaces Secure Browser

WorkSpaces Affinché la Thin Client Administrator Console funzioni correttamente con Amazon WorkSpaces Secure Browser, il sistema deve soddisfare i seguenti requisiti specifici. Questa tabella elenca tutte queste funzionalità supportate e i relativi requisiti.

Funzionalità	Requisito
Copia e incolla locali	Disabilita
Condivisione di cartelle locali	Disabilita

> **Note**
>
> L'estensione WorkSpaces Secure Browser per Single Sign-On non è attualmente supportata su WorkSpaces Thin Client.

Passaggio 2: configurare i portali WorkSpaces Secure Browser

WorkSpaces Thin Client funziona con il WorkSpaces Secure Browser VPC in una configurazione specifica:

1. Crea un VPC utilizzando il modello AWS CodeBuild Cloudformation.
2. Configura il tuo gestore dell'identità.
3. Crea un portale Amazon WorkSpaces Secure Browser.
4. Testa il tuo nuovo portale Amazon WorkSpaces Secure Browser.

Avvio della console di amministrazione WorkSpaces Thin Client

WorkSpaces Thin Client è un dispositivo thin client conveniente progettato per funzionare con i servizi di AWS End User Computing per fornire un accesso sicuro e immediato alle applicazioni e ai desktop virtuali.

Argomenti

Regioni coperte

WorkSpaces Thin Client è disponibile nelle seguenti regioni.

In queste regioni è disponibile solo la console di amministrazione WorkSpaces Thin Client. WorkSpaces I dispositivi Thin Client sono attualmente disponibili solo negli Stati Uniti, in Germania, Francia, Italia e Spagna.

Nome della regione	Regione	Endpoint	Collegamento alla console
US East (N. Virginia)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
US West (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Asia Pacific (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

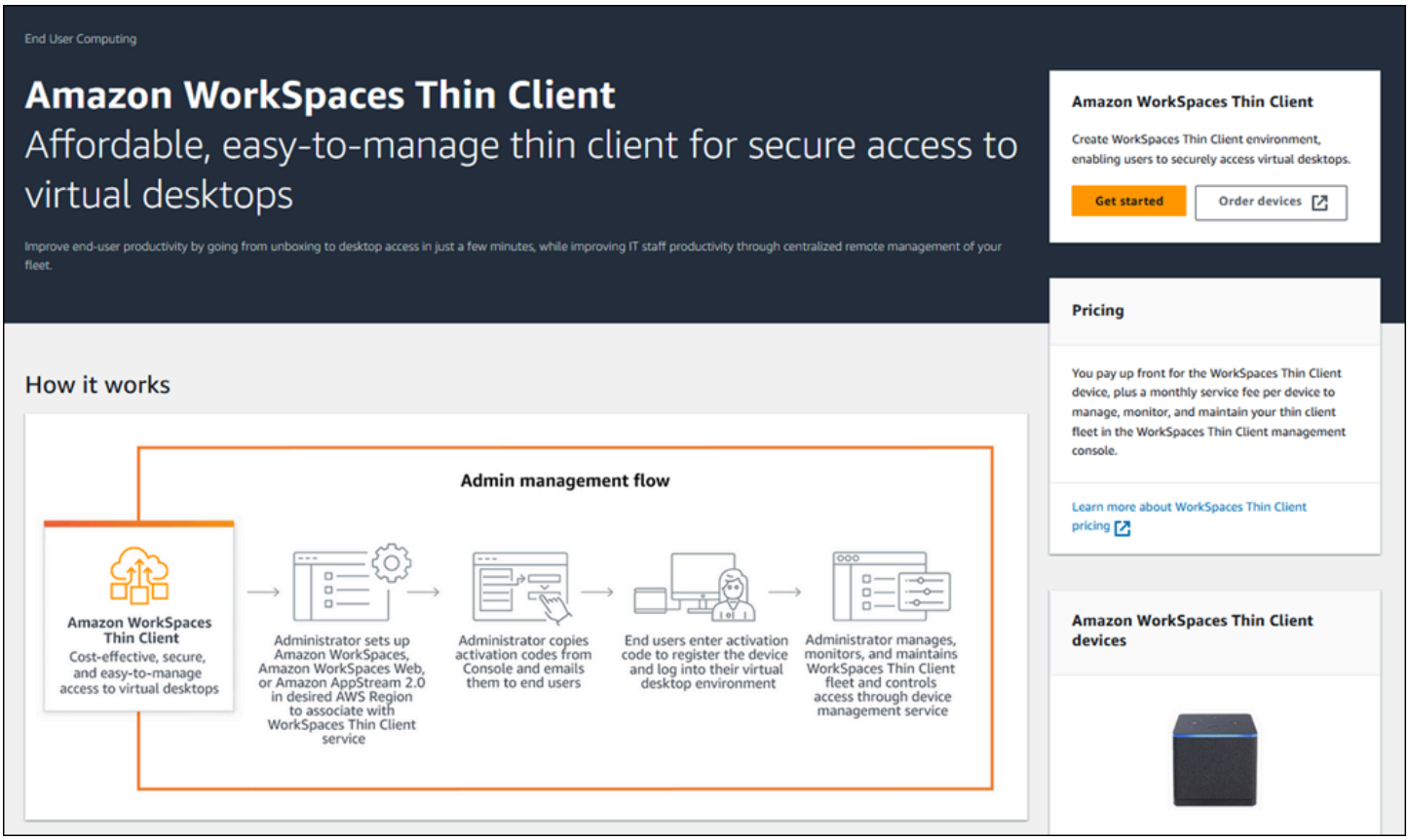
Nome della regione	Regione	Endpoint	Collegamento alla console
Europa (Irlanda)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Canada (Central)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europe (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europe (London)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

Avvio della console di amministrazione WorkSpaces Thin Client

Quando si dispone di un AWS account, è possibile avviare la console dell'amministratore e accedere alla console WorkSpaces Thin Client. Per avviare la console, procedi come segue:

1. Accedi al tuo AWS account.
2. Accedi alla console WorkSpaces Thin Client.
3. Seleziona Inizia e verrai indirizzato alla pagina Ambienti.

Utilizzo della console di amministrazione WorkSpaces Thin Client



Benvenuto nella console di amministrazione WorkSpaces Thin Client!

Da qui, puoi gestire la tua flotta di dispositivi e ambienti WorkSpaces Thin Client per il tuo team.

Per informazioni sul dispositivo WorkSpaces Thin Client, consulta la Guida per l'utente di WorkSpaces Thin Client.

Iniziamo.

Argomenti

Ambienti

Ogni dispositivo WorkSpaces Thin Client utilizza un ambiente desktop virtuale individuale per accedere alle proprie risorse online. Gli utenti accedono a questo ambiente utilizzando uno dei seguenti provider di desktop virtuali:

- Amazon WorkSpaces
- AppStream 2.0
- Browser WorkSpaces sicuro Amazon

Elenco di ambienti

Dettagli dell'elenco di ambienti

Nome: l'identificatore univoco associato a questo ambiente.

Servizio desktop virtuale: il provider di desktop virtuale utilizzato da questo ambiente.

ID del servizio di desktop virtuale: l'identificatore univoco che il fornitore di servizi di desktop virtuale assegna a questo ambiente.

Codice di attivazione: il codice utilizzato dagli utenti finali per accedere all'ambiente desktop virtuale.

Numero di dispositivi: il numero di dispositivi WorkSpaces Thin Client che accedono a questo ambiente.

Operazioni per l'elenco di ambienti

Cerca: cerca in tutti gli ambienti che gestisci.

Aggiorna: aggiorna l'elenco degli ambienti.

Visualizza dettagli: visualizza i dettagli dell'ambiente.

Azioni: apre un elenco a discesa in cui è possibile modificare o eliminare un ambiente.

Crea ambiente: avvia il processo di creazione di un ambiente

Crea ambiente: avvia il processo di creazione di un ambiente.

Argomenti

Dettagli dell'ambiente

Quando si seleziona un ambiente, la console WorkSpaces Thin Client mostra i dettagli di quell'ambiente da esaminare. La console visualizza anche i dettagli sul provider di desktop virtuale utilizzato da questo ambiente.

Argomenti

Riepilogo

Nome: l'identificatore univoco associato a questo ambiente.

Servizio desktop virtuale: il provider di desktop virtuale utilizzato da questo ambiente.

ID del servizio di desktop virtuale: l'identificatore univoco che il provider di servizi di desktop virtuale assegna a questo ambiente.

Codice di attivazione: questo codice viene utilizzato dagli utenti finali per accedere all'ambiente desktop virtuale.

Conserva sempre il software up-to-date: questa impostazione consente gli aggiornamenti automatici del software.

Ora di inizio della finestra di manutenzione: l'ora settimanale in cui iniziano gli aggiornamenti automatici del software.

Ora di fine della finestra di manutenzione: l'ora settimanale in cui terminano gli aggiornamenti automatici del software.

Finestra di manutenzione (giorni della settimana): i giorni in cui si verificano gli aggiornamenti automatici del software.

Dispositivi associati: il numero di dispositivi WorkSpaces Thin Client che accedono a questo ambiente.

Ora di creazione: la data e l'ora di creazione dell'ambiente.

Dettagli dell'ambiente desktop virtuale

Dettagli della WorkSpaces directory Amazon

ID directory: la WorkSpaces directory Amazon associata a questo ambiente.

Nome della directory: l'identificatore univoco associato a questa WorkSpaces directory Amazon.

Nome dell'organizzazione: il nome dell'organizzazione che controlla la WorkSpaces directory Amazon.

Tipo di directory: il formato della WorkSpaces directory Amazon.

Registrato: indica se questa WorkSpaces directory Amazon è registrata.

Stato: indica se questa WorkSpaces directory Amazon è attiva.

Dettagli del portale Amazon WorkSpaces Secure Browser

Nome: l'identificatore univoco associato a questo portale Amazon WorkSpaces Secure Browser.

Ora di creazione: la data e l'ora in cui è stato creato questo stack AppStream 2.0.

Endpoint del portale Web: l'URL utilizzato per accedere all'ambiente desktop virtuale.

AppStream Dettagli 2.0

Nome dello stack: l'identificatore univoco associato a questo stack AppStream 2.0.

URL di accesso IdP: l'URL del provider di identità utilizzato per accedere e disconnettersi dallo stack AppStream 2.0.

Ora di creazione: la data e l'ora in cui è stato creato questo stack AppStream 2.0.

Creazione di un ambiente

Per iniziare, ogni dispositivo richiede un servizio AWS End User Computing. WorkSpaces Thin Client utilizza i seguenti servizi:

- Amazon WorkSpaces tramite una directory assegnata

- AppStream 2.0 tramite uno stack assegnato
- Amazon WorkSpaces Secure Browser tramite un indirizzo del portale Web

È necessario assegnare un servizio a un ambiente esistente o crearne uno nuovo.

> **Note**
>
> WorkSpaces Thin Client visualizza solo i desktop virtuali nella stessa regione.

Argomenti

Fase 1: Specifica dei dettagli dell'ambiente

1. Inserisci un nome per l'ambiente nel campo Dettagli ambiente.
2. Per configurare patch software automatiche, seleziona la casella Always keep software. up-to-date

   > **Note**
   >
   > Se gli aggiornamenti software automatici non sono abilitati, i dispositivi registrati in questo ambiente non riceveranno gli aggiornamenti software finché non invierai manualmente l'aggiornamento o quando il software raggiungerà la scadenza e il sistema ne forzerà l'aggiornamento.
   > Inoltre, la versione del Software Set del dispositivo è determinata dal sistema. Questa versione potrebbe non essere la più recente.

3. Seleziona quando desideri pianificare la finestra di manutenzione per il tuo ambiente.

   - Applica la finestra di manutenzione a livello di sistema: aggiorna automaticamente il software dell'ambiente a un determinato orario ogni settimana.
   - Applica una finestra di manutenzione personalizzata: imposta un giorno e un'ora in cui desideri che il software di ambiente venga aggiornato ogni settimana.

4. Seleziona un servizio di desktop virtuale.

   - Amazon WorkSpaces
   - Browser WorkSpaces sicuro Amazon
   - AppStream 2.0

Fase 2: Selezione del provider di desktop virtuale

È necessario disporre di un servizio che fornisca agli utenti l'accesso al desktop virtuale e alle risorse compatibili.

> **Important**
>
> WorkSpaces Affinché la Thin Client Administrator Console funzioni correttamente, il sistema deve soddisfare requisiti specifici. Questi requisiti sono elencati in Prerequisiti e configurazioni.
> Assicurati che il sistema soddisfi questi requisiti prima di configurare la console.

Usare Amazon WorkSpaces

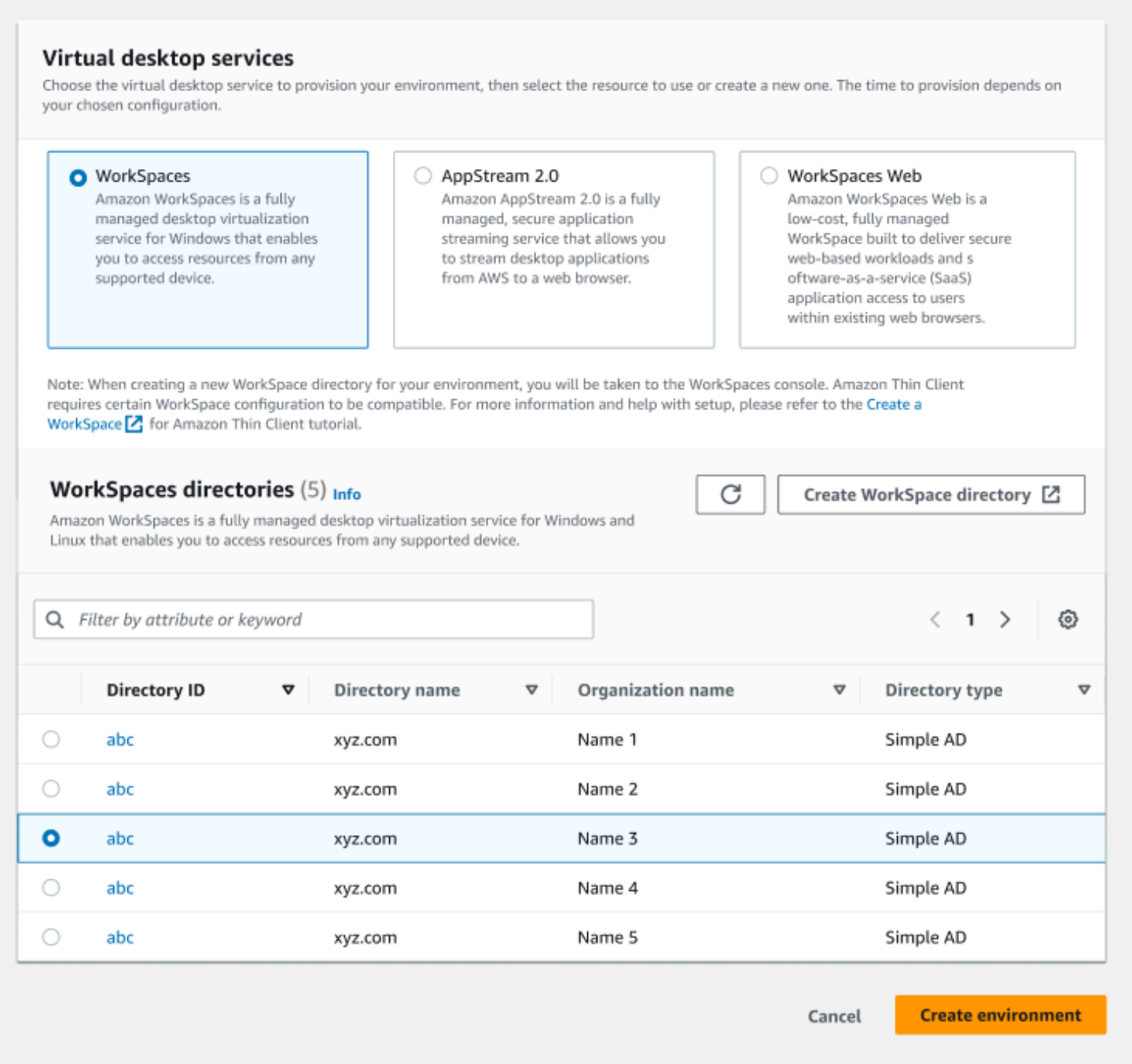
Amazon WorkSpaces è un servizio di virtualizzazione desktop completamente gestito per Windows che consente di accedere alle risorse da qualsiasi dispositivo supportato.

1. Per utilizzare Amazon WorkSpaces, esegui una delle seguenti operazioni:

   - Scegli la directory da utilizzare per il tuo ambiente. Puoi sfogliare l'elenco a discesa oppure cercare nelle directory utilizzando il campo di ricerca.

     > **Note**
     >
     > Se non vedi le tue directory esistenti nell'elenco, verifica nella Console di WorkSpaces gestione che soddisfino i requisiti del WorkSpaces Thin Client.

   - Crea una directory selezionando il pulsante Crea WorkSpaces cartella. Per ulteriori informazioni sulla creazione di WorkSpaces directory, consulta Gestire le directory per. WorkSpaces
2. Seleziona il pulsante Crea ambiente.



Quando crei il tuo ambiente, puoi comunque modificare i dettagli in un secondo momento. Per ulteriori informazioni, consulta Modifica di un ambiente.

Utilizzo della AppStream versione 2.0

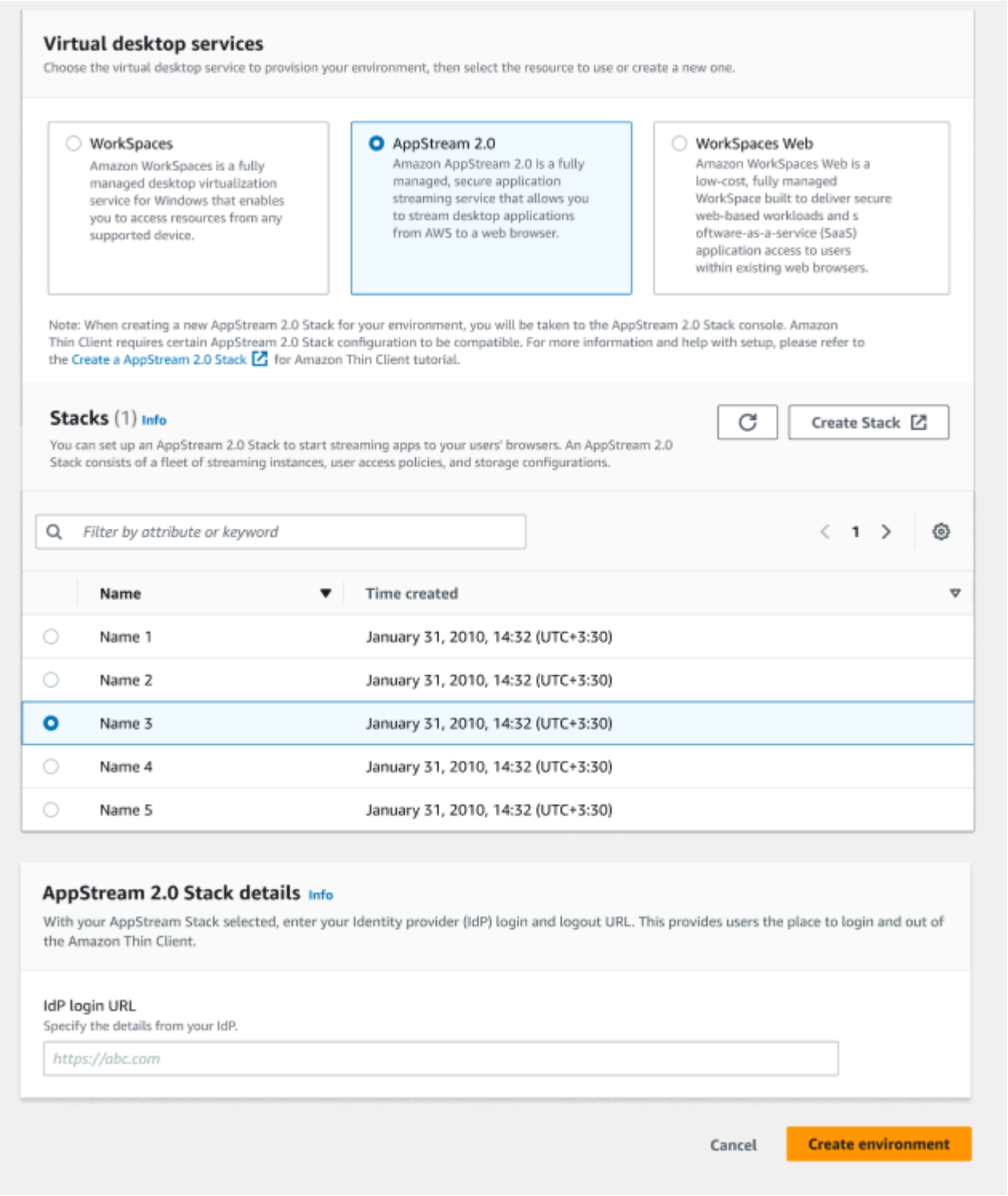
AppStream 2.0 è un servizio di streaming di applicazioni completamente gestito e sicuro che è possibile utilizzare per lo streaming di applicazioni desktop AWS da un browser Web.

> **Warning**
>
> Per creare un ambiente AppStream 2.0, è necessario aver `cli_follow_urlparam` impostato su`false`. Per raggiungere questo obiettivo, effettuare le seguenti operazioni:
>
> - Per un profilo predefinito, esegui `aws configure set cli_follow_urlparam false`.
> - Per un profilo con nome `ProfileName`, esegui `aws configure set cli_follow_urlparam false --profile ProfileName`.

1. Per configurare la AppStream versione 2.0, effettuate una delle seguenti operazioni:
   - Seleziona lo stack da utilizzare per il tuo ambiente. Puoi sfogliare l'elenco a discesa oppure cercare tra gli stack utilizzando il campo di ricerca.

     > **Note**
     >
     > Se non vedi gli stack esistenti nell'elenco, verifica nella console di gestione AppStream 2.0 che soddisfi i requisiti del WorkSpaces Thin Client.

   - Crea uno stack selezionando il pulsante Crea pila. Per ulteriori informazioni sulla creazione di pile AppStream 2.0, consulta Create a stack.
2. Inserisci l'URL di accesso e disconnessione del tuo gestore delle identità nel campo URL di accesso IdP. Ciò fornisce agli utenti un luogo in cui accedere e disconnettersi da WorkSpaces Thin Client.
3. Seleziona il pulsante Crea ambiente.



Dopo aver creato l'ambiente, puoi comunque modificare i dettagli in un secondo momento. Per ulteriori informazioni, consulta Modifica di un ambiente.

Utilizzo di Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser è una WorkSpaces console a basso costo e completamente gestita, progettata per fornire carichi di lavoro basati sul Web e accesso alle applicazioni SaaS (Software as a Service) agli utenti all'interno dei browser Web esistenti.

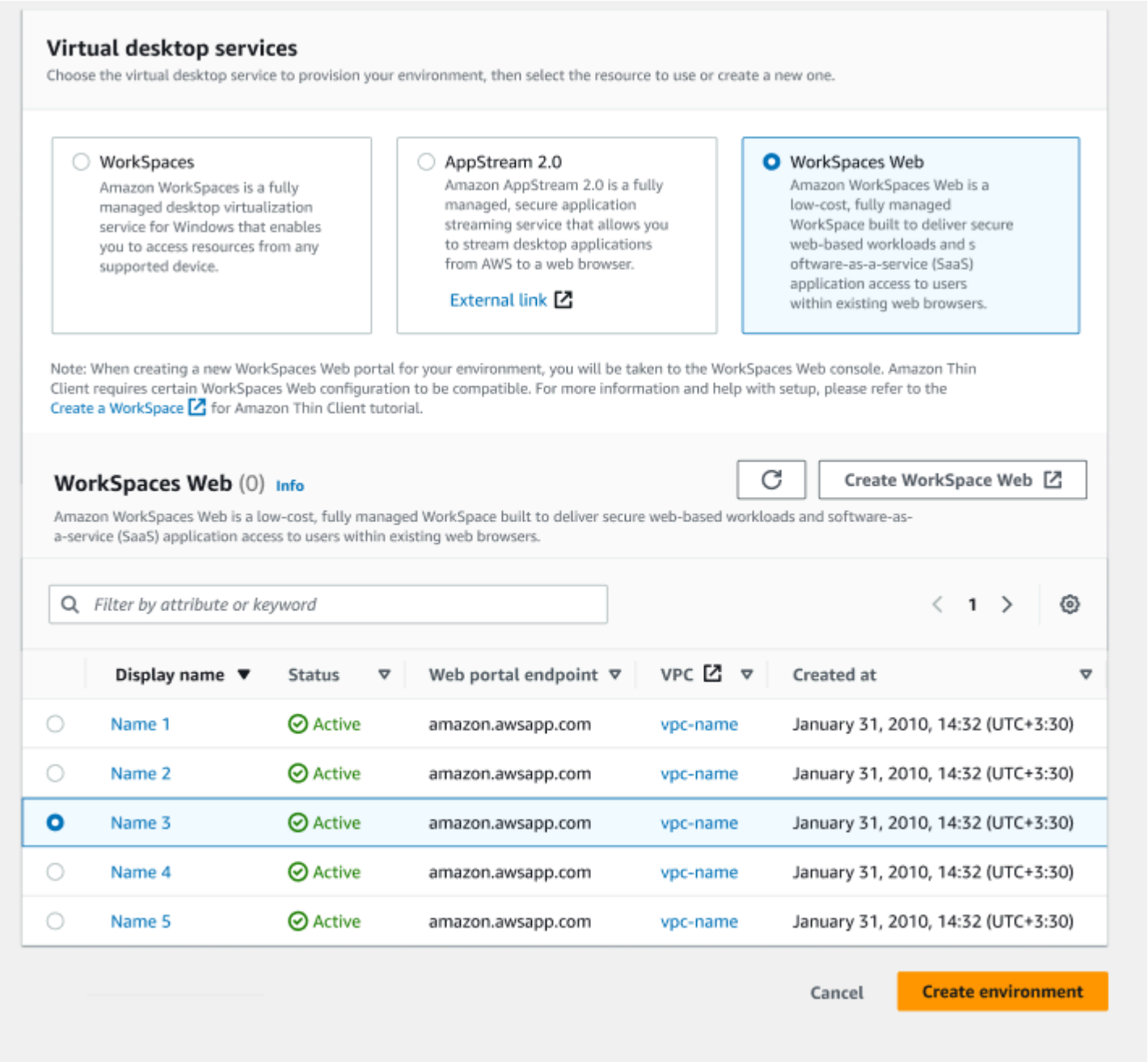
1. Per configurare Amazon WorkSpaces Secure Browser, esegui una delle seguenti operazioni:

   - Seleziona il portale web che desideri utilizzare per il tuo ambiente. Puoi sfogliare l'elenco a discesa oppure cercare nei portali web utilizzando il campo di ricerca.

     > **Note**
     >
     > Se non vedi i portali web esistenti nell'elenco, verifica nella WorkSpaces Secure Browser Management Console che soddisfino i requisiti del WorkSpaces Thin Client.

   - Crea un portale web selezionando il pulsante Crea browser WorkSpaces sicuro. Per ulteriori informazioni sulla creazione di portali Web WorkSpaces Secure Browser, consulta Configurazione di Amazon WorkSpaces Secure Browser.

2. Seleziona il pulsante Crea ambiente.



Dopo aver creato l'ambiente, puoi comunque modificare i dettagli in un secondo momento. Per ulteriori informazioni, consulta Modifica di un ambiente.

Fase 3: Invio del codice di attivazione agli utenti del dispositivo

Dopo aver impostato l'ambiente e il servizio desktop virtuale, riceverai un codice di attivazione univoco per la configurazione sulla console di AWS gestione.

Fornisci questo codice di attivazione a qualsiasi utente del dispositivo WorkSpaces Thin Client, che potrà utilizzarlo per accedere al proprio desktop virtuale.

Consulta la WorkSpaces Thin Client User Guide per ulteriori informazioni su come aiutare l'utente del dispositivo a configurare Amazon WorkSpaces Thin Client.

Modifica di un ambiente

La console di amministrazione WorkSpaces Thin Client gestisce ambienti desktop virtuali per singoli utenti. Da questa console è possibile modificare o eliminare ambienti desktop virtuali.

1. Seleziona l'ambiente che desideri modificare.

   > **Note**
   >
   > È possibile sfogliare l'elenco a discesa oppure cercare negli ambienti utilizzando il campo di ricerca.

2. Seleziona il pulsante Azioni.
3. Seleziona Modifica dall'elenco a discesa. Verrai indirizzato alla finestra Modifica ambiente.
4. Modifica uno dei seguenti:

   - Cambia il nome del tuo ambiente nel campo Nome ambiente.
   - Modifica la casella di controllo relativa ai dettagli degli aggiornamenti software per gli aggiornamenti automatici delle patch software.
   - Seleziona quando desideri pianificare la finestra di manutenzione per il tuo ambiente.

5. Seleziona il pulsante Modifica ambiente.

Eliminazione di un ambiente

> **Note**
>
> Non è possibile eliminare un ambiente se contiene dispositivi registrati. Innanzitutto, è necessario annullare la registrazione ed eliminare tutti i dispositivi in un ambiente.

1. Seleziona l'ambiente che desideri eliminare. Puoi sfogliare l'elenco a discesa oppure cercare negli ambienti utilizzando il campo di ricerca.

2. Seleziona il pulsante Azioni.
3. Seleziona Elimina dall'elenco a discesa. Viene visualizzata la finestra di conferma dell'eliminazione dell'ambiente.
4. Digita "delete" nel campo di conferma.
5. Seleziona il pulsante Elimina.

Dispositivi

Ogni utente finale WorkSpaces Thin Client dispone di un dispositivo dedicato che lo collega ai propri ambienti desktop virtuali e alle risorse online. Questi dispositivi sono gestiti tramite la console di amministrazione WorkSpaces Thin Client sul AWS sito.

Da questa console puoi ordinare i dispositivi per il tuo team.

Un elenco dispositivi

Dettagli dell'elenco di dispositivi

ID dispositivo: il numero di identificazione assegnato a un singolo dispositivo.

Nome dispositivo: (opzionale) Il nome univoco assegnato a un dispositivo.

Stato dell'attività: lo stato attuale di un dispositivo. Esistono due stati di stato:

- Attivo: connesso a una rete almeno una volta negli ultimi sette giorni.
- Inattivo: non connesso a una rete almeno una volta negli ultimi sette giorni.

Stato di registrazione: conferma che un dispositivo è stato configurato, è associato a questo AWS account e fa parte di un ambiente specifico. Può trovarsi in uno dei seguenti stati:

- Registrato: questo è lo stato predefinito.
- Annullamento della registrazione: il dispositivo è in fase di ripristino e annullamento della registrazione.

> **Note**
>
> È possibile eliminare un dispositivo se si trova in uno stato di annullamento della registrazione.

- Registrazione annullata: la registrazione del dispositivo è stata annullata correttamente.

> **Note**
>
> Puoi eliminare un dispositivo solo se si trova nello stato Annullamento della registrazione o Annullamento della registrazione.

- Archiviato: il dispositivo è stato archiviato.

ID ambiente: l'identificatore dell'ambiente a cui è collegato questo dispositivo.

Conformità del software: lo stato di conformità del software del dispositivo. Esistono due stati di stato:

- Conforme
- Non conforme

Operazioni per l'elenco di dispositivi

Cerca: cerca tra tutti i dispositivi che gestisci.

Aggiorna: aggiorna l'elenco dei dispositivi.

Visualizza dettagli: visualizza i dettagli del dispositivo.

Azioni: apre un elenco a discesa in cui è possibile effettuare le seguenti operazioni:

- Modificare il nome del dispositivo
- Annulla registrazione
- Archive (Archivia)
- Eliminazione
- Esportare i dettagli del dispositivo

Ordina dispositivi: avvia il processo di ordinamento dei dispositivi.

Argomenti

Dettagli del dispositivo

Riepilogo

Numero di serie del dispositivo: il numero di identificazione assegnato a un singolo dispositivo.

ARN: l'identificatore univoco del dispositivo in formato Amazon Resource Name (ARN).

Nome del dispositivo: il nome che dai a un dispositivo. Se non hai creato un nome, puoi assegnargli un nome o riceverà un nome predefinito.

Tipo di dispositivo: il tipo di dispositivo dell'utente finale collegato all'account.

Stato attività: lo stato corrente di questo dispositivo. I due stati di stato sono:

- Attivo
- Inattivo

ID ambiente: il numero di identificazione dell'ambiente utilizzato dal dispositivo.

Stato di registrazione: conferma che un dispositivo è stato configurato, è associato a questo AWS account e fa parte di un ambiente specifico. Può trovarsi in uno dei quattro stati seguenti:

- Registrato: questo è lo stato predefinito.
- Annullamento della registrazione: il dispositivo è in fase di ripristino e annullamento della registrazione.

- Registrazione annullata: la registrazione del dispositivo è stata annullata correttamente.

> **Note**
>
> Puoi eliminare il dispositivo solo se si trova nello stato Annullato o Archiviato.

- Archiviato: questo dispositivo è stato contrassegnato dall'amministratore come non attualmente in servizio.

Iscritto da: la data di attivazione del dispositivo.

Ultimo accesso: la data e l'ora dell'accesso più recente.

Ultima postura controllata a: data e ora dell'ultimo check-in del dispositivo.

Versione attuale del software: la versione del software correntemente utilizzata da questo dispositivo.

Aggiornamento programmato del software: la versione programmata del software sul dispositivo.

Conformità del software: conferma della validità del set software. Esistono due stati di stato:

- Conforme
- Non conforme

Log degli utenti

Ultimo accesso al dispositivo: la data e l'ora dell'ultimo utilizzo del dispositivo.

Modifica del nome di un dispositivo

1. Seleziona il dispositivo da modificare. Puoi sfogliare l'elenco a discesa oppure cercare il dispositivo utilizzando il campo di ricerca.
2. Seleziona il pulsante Azioni.
3. Seleziona Modifica nome dispositivo dall'elenco a discesa. Viene visualizzata la finestra Modifica nome dispositivo.
4. Inserisci il nuovo nome per il dispositivo nel campo di conferma Nome del dispositivo.
5. Selezionare il pulsante Salva.

Reimpostazione e annullamento della registrazione di un dispositivo

1. Seleziona il dispositivo di cui desideri annullare la registrazione. Puoi sfogliare l'elenco a discesa oppure cercare il dispositivo utilizzando il campo di ricerca.
2. Seleziona il pulsante Azioni.
3. Seleziona Annulla registrazione dall'elenco a discesa. Viene visualizzata la finestra Annulla registrazione.
4. Inserisci "deregister" nel campo di conferma.
5. Seleziona il pulsante Annulla registrazione.

> **Note**
>
> L'annullamento della registrazione comporta la disconnessione forzata dell'utente e richiede il riavvio del dispositivo WorkSpaces Thin Client nel bel mezzo di una sessione.

Archiviazione di un dispositivo

1. Seleziona il dispositivo da archiviare. Puoi sfogliare l'elenco a discesa oppure cercare il dispositivo utilizzando il campo di ricerca.
2. Seleziona il pulsante Azioni.
3. Seleziona Archivio dall'elenco a discesa. Viene visualizzata la finestra Archivio.
4. Inserisci "reset and archive" nel campo di conferma.
5. Seleziona il pulsante Ripristina e archivia.

> **Note**
>
> L'archiviazione di un dispositivo comporta la disconnessione forzata dell'utente e richiede il riavvio del dispositivo WorkSpaces Thin Client nel bel mezzo di una sessione.

Eliminazione di un dispositivo

1. Seleziona il dispositivo che desideri eliminare. Puoi sfogliare l'elenco a discesa oppure cercare il dispositivo utilizzando il campo di ricerca.
2. Seleziona il pulsante Azioni.
3. Seleziona Elimina dall'elenco a discesa. Viene visualizzata la finestra Elimina.
4. Digita "delete" nel campo di conferma.
5. Seleziona il pulsante Elimina.

> **Note**
>
> Quando il dispositivo è stato eliminato con successo, l'utente deve restituire il dispositivo WorkSpaces Thin Client ad Amazon.

Esportazione dei dettagli del dispositivo

1. Seleziona il dispositivo da cui desideri esportare i dettagli. Puoi sfogliare l'elenco a discesa oppure cercare il dispositivo utilizzando il campo di ricerca.
2. Seleziona il pulsante Azioni.
3. Seleziona Esporta i dettagli del dispositivo dall'elenco a discesa. I dettagli del dispositivo selezionato vengono scaricati in formato foglio di calcolo.

Aggiornamenti software

WorkSpaces Thin Client a volte richiede aggiornamenti software che introducono nuove funzionalità e applicano patch di sicurezza. Questi aggiornamenti sono rappresentati da un set di software con versioni.

Un set software può contenere aggiornamenti alle applicazioni software o al sistema operativo per il dispositivo WorkSpaces Thin Client. Da questa console, è possibile scegliere di aggiornare immediatamente il software oppure pianificare un aggiornamento automatico durante la finestra di manutenzione degli ambienti.

Fate riferimento ai set software dell'ambiente WorkSpaces Thin Client per l'elenco dei set software rilasciati.

Argomenti

Aggiornamento del software dell'ambiente

WorkSpaces Thin Client è un servizio di elaborazione per utenti AWS finali che fornisce agli utenti l'accesso ai desktop virtuali. Questi desktop virtuali vengono aggiornati periodicamente con nuovi set di software. Per aggiornare il software ambientale, procedi come segue:

1. Seleziona il set di software dall'elenco in Aggiornamenti software disponibili. Per un elenco dei set software, fare riferimento ai set di software per l'ambiente WorkSpaces Thin Client.
2. Seleziona il pulsante Installa.
3. Seleziona Ambienti nella parte superiore della pagina.
4. Seleziona l'ambiente da aggiornare dall'elenco nella sezione Ambienti.
5. Seleziona quando aggiornare l'ambiente in Pianifica l'aggiornamento scegliendo una delle seguenti opzioni:

   - Aggiorna subito il software: avvia l'aggiornamento del software dell'ambiente su tutti i dispositivi registrati.

     > **Note**
     >
     > L'aggiornamento del software ora può interrompere qualsiasi sessione utente attiva.

   - Aggiorna il software durante ogni finestra di manutenzione dell'ambiente: aggiorna il software dell'ambiente durante la finestra di manutenzione programmata per l'ambiente.
6. Seleziona la casella per autorizzare l'aggiornamento. Questa casella deve essere selezionata per consentire l'aggiornamento del software.
7. Seleziona il pulsante Installa.

Aggiornamento del software del dispositivo

WorkSpaces Thin Client è un servizio di elaborazione per utenti AWS finali che fornisce un dispositivo thin client che collega gli utenti a desktop virtuali dedicati. Questi dispositivi vengono aggiornati periodicamente con nuovi software. Per aggiornare il software del dispositivo, procedi come segue:

1. Seleziona il set di software dall'elenco in Aggiornamenti software disponibili.
2. Seleziona il pulsante Installa.
3. Nella parte superiore della pagina, seleziona Elimina.
4. Seleziona il dispositivo o i dispositivi da aggiornare dall'elenco nella sezione Dispositivi. Per un elenco dei set software, fare riferimento ai set di software in ambiente WorkSpaces Thin Client.
5. Seleziona quando aggiornare l'ambiente dalle opzioni Pianifica l'aggiornamento scegliendo una delle seguenti opzioni:
   - Aggiorna subito il software: aggiorna immediatamente il software del dispositivo.

     > **Note**
     >
     > L'aggiornamento del software ora può interrompere qualsiasi sessione utente attiva.

   - Aggiorna il software durante ogni finestra di manutenzione del dispositivo: aggiorna il software dell'ambiente durante la finestra di manutenzione programmata del dispositivo.
6. Seleziona la casella per autorizzare l'aggiornamento. Questa casella deve essere selezionata per consentire l'aggiornamento del software.
7. Seleziona il pulsante Installa.

WorkSpaces Versioni del software Thin Client

WorkSpaces Thin Client è un servizio di AWS End User Computing che fornisce agli utenti l'accesso ai desktop virtuali su un dispositivo. Questi dispositivi vengono aggiornati periodicamente con nuovi set di software. La tabella seguente descrive tutti i set di software rilasciati. Gli amministratori possono utilizzare la console di AWS gestione per visualizzare i set di software disponibili.

Set di software	Data di rilascio	Modifiche
2.5.0	06-13-2024	• Risolto il problema per cui il dispositivo mostrava brevemente la schermata di configurazione della tastiera e del mouse al risveglio dalla modalità di sospensione prima di avviare la sessione. • Il pulsante Home sulla barra degli strumenti del dispositivo è stato rinominat o Accedi. • Miglioramenti alle prestazio ni delle chiamate audio/vid eo durante la sessione.
2.4.3	29-05-2024	• Correzione immediata del problema critico di sicurezza CVE-2024-5274 di Chromium.
2.4.2	17-05-2024	• Correzione immediata del problema critico di sicurezza CVE-2024-4947 di Chromium.
2.4.1	15/05/2024	• Correzioni zero-day per i problemi critici di sicurezza CVE-2024-4671 e CVE-2024-4761 di Chromium. • È stato risolto il problema che consentiva di fare clic con il pulsante destro del

Set di software	Data di rilascio	Modifiche
		mouse sui collegamenti AWS e Privacy nella pagina di WorkSpaces accesso per aprire il browser in modalità autonoma.
2.4.0	05-09-2024	• È stato risolto un problema che bloccava «accounts .google.com» e impediva l'utilizzo di Google Workspace come IDP per la sessione 2.0. AppStream • La barra degli strumenti delle impostazioni del dispositivo si comprime automaticamente con un clic in qualsiasi area dello schermo.

Set di software	Data di rilascio	Modifiche
2.3.0	04-05-2024	• Le impostazioni del dispositivo vengono visualizzate in una barra degli strumenti compressa che consente un migliore utilizzo dello schermo visibile. • Gli utenti finali possono ora configurare la durata di attesa prima che il dispositivo dorma in caso di inattività. • È stato risolto il problema per cui l'URL «about:blank» veniva visualizzato sul secondo display. • È stato risolto il problema che causava la visualizzazione di una schermata bianca alla chiusura della visualizzazione estesa. • I livelli di volume impostati dagli utenti finali ora persistono anche dopo i riavvii del dispositivo.
2.2.1	16/02/2024	• È stato risolto un problema che si verificava durante il processo di accesso che impediva agli utenti di accedere all'autenticazione configurata con SAML 2.0. WorkSpaces

Set di software	Data di rilascio	Modifiche
2.2.0	02-08-2024	• Aggiunto il supporto per tastiere ISO con localizza zioni in inglese (Regno Unito), francese, tedesco, italiano e spagnolo.
2.1.2	26/01-2024	• Correzione immediata del problema critico di sicurezza CVE-2024-0519 di Chromium. • Miglioramento della latenza dell'utente finale associata alla funzionalità Lock. • Gli endpoint interni rivolti ai dispositivi vengono trasferiti al dominio 'thinclient* '.
2.1.1	21-12/2023	• Correzione immediata del problema critico di sicurezza CVE-2023-7024 di Chromium.
2.1.0	20-12/2023	• Aggiunge un pulsante Home alle impostazioni del dispositivo e abilita il supporto per i tasti Meta. Ciò consente agli utenti finali di richiamar e la schermata di blocco premendo Meta+L.
2.0.1	12-06-2023	• Correzione immediata del problema critico di sicurezza CVE-2024-6345 di Chromium.

Set di software	Data di rilascio	Modifiche
2.0.0	15-11-2023	• Rilascio iniziale

Utilizzo dei tag nelle risorse WorkSpaces Thin Client

È possibile organizzare e gestire le risorse per il WorkSpaces Thin Client assegnando i propri metadati a ciascuna risorsa sotto forma di tag. Per ogni tag, specifica una chiave e un valore. Una chiave può essere una categoria generale, ad esempio "progetto", "proprietario" o "ambiente", con valori specifici associati. Puoi usare i tag come un modo semplice ma efficace per gestire le risorse AWS e organizzare i dati, inclusi i dati di fatturazione.

Quando si aggiungono tag a una risorsa esistente, tali tag non vengono visualizzati nel report di allocazione dei costi fino al primo giorno del mese successivo. Ad esempio, se aggiungi tag a un dispositivo WorkSpaces Thin Client esistente il 15 luglio, i tag non verranno visualizzati nel rapporto di allocazione dei costi fino al 1° agosto. Per ulteriori informazioni, consulta Using Cost Allocation Tags nella AWS Billing User Guide.

> **Note**
>
> Per visualizzare i tag delle risorse WorkSpaces Thin Client nel Cost Explorer, è necessario attivare i tag applicati alle risorse WorkSpaces Thin Client seguendo le istruzioni riportate in Attivazione dei tag di allocazione dei costi definiti dall'utente nella Guida per l'AWS Billing utente.
>
> I tag vengono visualizzati 24 ore dopo l'attivazione, ma possono essere necessari 4-5 giorni prima che i valori associati a tali tag vengano visualizzati in Cost Explorer. Inoltre, per visualizzare e fornire i dati sui costi in Cost Explorer, le risorse WorkSpaces Thin Client che sono state etichettate devono essere soggette a addebiti durante quel periodo. Cost Explorer mostra solo i dati sui costi dal momento in cui i tag sono stati attivati. Al momento non sono disponibili dati storici.

Risorse che puoi taggare:

- È possibile aggiungere tag alle seguenti risorse al momento della creazione: ambienti WorkSpaces Thin Client.
- È possibile aggiungere tag alle risorse esistenti dei seguenti tipi: ambienti WorkSpaces Thin Client, dispositivi e set software.

Limitazioni applicate ai tag

- Numero massimo di tag per risorsa: 50
- Lunghezza massima della chiave: 128 caratteri Unicode
- Lunghezza massima del valore: 256 caratteri Unicode
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali.
- Non utilizzate il `aws:` prefisso nei nomi o nei valori dei tag perché è riservato all'uso. AWS Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso.

Per aggiornare i tag per un ambiente esistente utilizzando la console

1. Aprire la console WorkSpaces Thin Client.
2. Seleziona l'ambiente per aprirne la pagina dei dettagli
3. Scegli Modifica.
4. Nella sezione Tag, esegui una o più delle seguenti operazioni:.
   - Per aggiungere un tag, scegli Aggiungi nuovo tag, quindi modifica i valori per Chiave e Valore.
   - Per aggiornare un tag, modifica il valore di Value.
   - Per eliminare un tag, scegli Rimuovi accanto al tag.
5. Quando hai finito di aggiornare i tag, scegli Salva.

Per aggiornare i tag di un dispositivo esistente utilizzando la console

1. Aprire la console WorkSpaces Thin Client.
2. Seleziona il dispositivo per aprire la pagina dei dettagli.
3. Scegliere Tags (Tag).
4. Scegliere Gestisci tag.
5. Effettuare una o più delle seguenti operazioni:
   - Per aggiungere un tag, scegli Aggiungi nuovo tag, quindi modifica i valori per Chiave e Valore.
   - Per aggiornare un tag, modifica il valore di Value.
   - Per eliminare un tag, scegli Rimuovi accanto al tag.

6. Quando hai finito di aggiornare i tag, scegli Salva.

Per aggiornare i tag per un aggiornamento software utilizzando la console

1. Aprire la console WorkSpaces Thin Client.
2. Seleziona l'aggiornamento del software per aprirne la pagina dei dettagli.
3. Nella sezione Tag, scegli Gestisci tag.
4. Effettuare una o più delle seguenti operazioni:
   - Per aggiungere un tag, scegli Aggiungi nuovo tag, quindi modifica i valori per Chiave e Valore.
   - Per aggiornare un tag, modifica il valore di Valore.
   - Per eliminare un tag, scegli Rimuovi accanto al tag.
5. Quando hai finito di aggiornare i tag, scegli Salva.

Sicurezza in Amazon WorkSpaces Thin Client

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile 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 informazioni sui programmi di conformità che si applicano ad Amazon WorkSpaces Thin Client, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza WorkSpaces Thin Client. I seguenti argomenti mostrano come configurare WorkSpaces Thin Client per soddisfare gli obiettivi di sicurezza e conformità. Puoi anche imparare a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse WorkSpaces Thin Client.

Argomenti

Protezione dei dati in Amazon WorkSpaces Thin Client

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon WorkSpaces Thin Client. 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. Questi contenuti includono la configurazione della protezione e le attività di gestione per i servizi Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza 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 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con WorkSpaces Thin Client o altri utenti 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 fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Amazon WorkSpaces Thin Client raccoglie e fornisce informazioni sull'uso da parte degli utenti dei dispositivi WorkSpaces Thin Client e sulla loro interazione con i servizi desktop virtuali. Ad esempio, memoria disponibile, diagnostica di rete, informazioni di rete, connettività del dispositivo, credenziali SAML, informazioni di identificazione del dispositivo e segnalazioni di arresti anomali. Queste informazioni vengono utilizzate per fornire il servizio e possono essere utilizzate per migliorare

l'esperienza dell'utente con il servizio. Inoltre, esclusivamente per fornire all'utente il servizio, le informazioni possono essere trasferite al di fuori della AWS regione in cui gli utenti utilizzano il servizio. Trattiamo queste informazioni in conformità con l'AWS Informativa sulla privacy.

Argomenti

Crittografia dei dati

WorkSpaces Thin Client raccoglie dati di personalizzazione dell'ambiente e del dispositivo, come impostazioni utente, identificatori dei dispositivi, informazioni sui provider di identità e identificatori desktop in streaming. WorkSpaces Thin Client raccoglie anche i timestamp delle sessioni. I dati raccolti vengono archiviati in Amazon DynamoDB e Amazon S3. WorkSpaces Thin Client utilizza AWS Key Management Service (KMS) 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 WorkSpaces Thin Client.
- Proteggi i dati end-to-end fornendo una chiave gestita dal cliente, in modo che WorkSpaces Thin Client possa crittografare i dati inattivi con le chiavi fornite.
- Fai attenzione alla condivisione dei codici di attivazione dell'ambiente e delle credenziali utente:
  - Gli amministratori devono accedere alla console WorkSpaces Thin Client e gli utenti devono fornire i codici di attivazione per la configurazione di WorkSpaces Thin Client. Utilizza le credenziali per accedere al desktop di streaming.
  - Chiunque abbia accesso fisico può configurare un WorkSpaces Thin Client, ma non può avviare una sessione a meno che non disponga di un codice di attivazione valido e di credenziali utente per accedere.
- Gli utenti possono terminare esplicitamente le sessioni scegliendo di bloccare lo schermo, riavviare o spegnere il dispositivo utilizzando la barra degli strumenti del dispositivo. In questo modo si annulla la sessione del dispositivo e si cancellano le credenziali della sessione.

WorkSpaces Thin Client protegge contenuti e metadati per impostazione predefinita crittografando tutti i dati sensibili con KMS. AWS Se si verifica un errore durante l'applicazione delle impostazioni esistenti, un utente non potrà accedere a nuove sessioni e i dispositivi non potranno applicare gli aggiornamenti software.

Crittografia dei dati a riposo per Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client fornisce la crittografia di default per proteggere i dati sensibili dei clienti archiviati utilizzando chiavi AWS di crittografia proprietarie.

- AWS chiavi di proprietà: Amazon WorkSpaces Thin Client utilizza queste chiavi per impostazione predefinita per crittografare automaticamente i dati di identificazione personale. Non è possibile visualizzare, gestire o utilizzare chiavi AWS di proprietà o controllarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta Chiavi di proprietà di AWS nella Guida per gli sviluppatori di AWS Key Management Service.

La crittografia predefinita dei dati a riposo aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia.

Sebbene non sia possibile disabilitare questo livello di crittografia o selezionare un tipo di crittografia alternativo, puoi aggiungere un secondo livello di crittografia alle chiavi di crittografia esistenti di proprietà di AWS scegliendo una chiave gestita dal cliente quando crei il tuo ambiente Thin Client:

- Chiavi gestite dal cliente: Amazon WorkSpaces Thin Client supporta l'uso di una chiave simmetrica gestita dal cliente che puoi creare, possedere e gestire per aggiungere un secondo livello di crittografia alla crittografia di AWS proprietà esistente. Poiché hai il pieno controllo di questo livello di crittografia, puoi eseguire attività come le seguenti:
  - Stabilire e mantenere le policy delle chiavi
  - Stabilire e mantenere le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi
  - Pianificare l'eliminazione delle chiavi

Per ulteriori informazioni, consulta Chiave gestita dal cliente nella Guida per gli sviluppatori di AWS Key Management Service.

La tabella seguente riassume il modo in cui Amazon WorkSpaces Thin Client crittografa i dati di identificazione personale.

Tipo di dati	Crittografia con chiavi di proprietà di AWS	Crittografia con chiavi gestite dal cliente (opzionale)
Nome dell'ambiente WorkSpaces Nome dell'ambiente Thin Client	Abilitato	Abilitato
Nome dispositivo WorkSpaces Nome del dispositivo Thin Client	Abilitato	Abilitato

> **Note**
>
> Amazon WorkSpaces Thin Client abilita automaticamente la crittografia a riposo utilizzando chiavi AWS proprietarie per proteggere gratuitamente i dati di identificazione personale. Tuttavia, si applicano le tariffe AWS KMS per l'utilizzo di una chiave gestita dal cliente. Per informazioni sui prezzi, consulta Prezzi di AWS Key Management Service.

In che modo Amazon WorkSpaces Thin Client utilizza le sovvenzioni in KMS AWS

Amazon WorkSpaces Thin Client richiede una concessione per utilizzare la chiave gestita dal cliente.

Quando crei un ambiente WorkSpaces Thin Client crittografato con una chiave gestita dal cliente, Amazon WorkSpaces Thin Client crea una concessione per tuo conto inviando una CreateGrant richiesta a AWS KMS. Le sovvenzioni in AWS KMS vengono utilizzate per consentire ad Amazon WorkSpaces Thin Client l'accesso a una chiave KMS in un account cliente.

Quando un nuovo dispositivo Thin Client viene registrato in un ambiente crittografato WorkSpaces Thin Client con una chiave gestita dal cliente e il nome di tale dispositivo viene modificato, Amazon

WorkSpaces Thin Client crea una concessione per tuo conto inviando una CreateGrant richiesta a AWS KMS. Le sovvenzioni in AWS KMS vengono utilizzate per consentire ad Amazon WorkSpaces Thin Client l'accesso a una chiave KMS in un account cliente.

Amazon WorkSpaces Thin Client richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia richieste Decrypt a AWS KMS per decrittografare i dati crittografati

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, Amazon WorkSpaces Thin Client non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influisce sulle operazioni che dipendono da tali dati. Ad esempio, se tenti di ottenere dettagli sull'ambiente a cui Amazon WorkSpaces Thin Client non può accedere, l'operazione restituisce un `AccessDeniedException` errore. Inoltre, il dispositivo WorkSpaces Thin Client non sarà in grado di utilizzare un ambiente WorkSpaces Thin Client.

Creazione di una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando la Console di gestione AWS o le operazioni dell'API AWS KMS.

Per creare una chiave simmetrica gestita dal cliente

Segui la procedura riportata in Creazione di una chiave simmetrica gestita dal cliente nella Guida per gli sviluppatori di AWS Key Management Service.

Policy della chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestione dell'accesso alle chiavi gestite dal cliente nella Guida per gli sviluppatori di AWS Key Management Service.

Per utilizzare la chiave gestita dal cliente con le tue risorse Amazon WorkSpaces Thin Client, nella policy chiave devono essere consentite le seguenti operazioni API:

- `kms:DescribeKey`— Fornisce i dettagli chiave gestiti dal cliente in modo che Amazon WorkSpaces Thin Client possa convalidare la chiave.

- `kms:GenerateDataKey`: consente di utilizzare la chiave gestita dal cliente per crittografare i dati.
- `kms:Decrypt`: consente di utilizzare la chiave gestita dal cliente per decrittografare i dati.
- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una chiave KMS specificata, che consente l'accesso alle operazioni di concessione richieste da Amazon WorkSpaces Thin Client. Per ulteriori informazioni, consulta Utilizzo delle concessioni nella Guida per gli sviluppatori di AWS Key Management Service.

  Ciò consente ad Amazon WorkSpaces Thin Client di effettuare le seguenti operazioni:

  - Chiamare `Decrypt` per decrittografare i dati crittografati.

Di seguito sono riportati alcuni esempi di policy che puoi aggiungere per Amazon WorkSpaces Thin Client:

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
```

```
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni sulla specifica delle autorizzazioni in una policy, consulta la Guida per gli sviluppatori di AWS Key Management Service.

Per ulteriori informazioni sulla risoluzione dei problemi di accesso alle chiavi, consulta la Guida per gli sviluppatori di AWS Key Management Service.

Specificazione di una chiave gestita dal cliente per WorkSpaces Thin Client

È possibile specificare una chiave gestita dal cliente come crittografia di secondo livello per le seguenti risorse:

- WorkSpaces Ambiente Thin Client

Quando crei un ambiente, puoi specificare la chiave dati fornendo un`kmsKeyArn`, che Amazon WorkSpaces Thin Client utilizza per crittografare i dati personali identificabili.

- `kmsKeyArn`— Un identificatore chiave per una chiave AWS KMS gestita dal cliente. Fornire un ARN della chiave.

Quando un nuovo dispositivo WorkSpaces Thin Client viene aggiunto all'ambiente WorkSpaces Thin Client crittografato con una chiave gestita dal cliente, il dispositivo WorkSpaces Thin Client eredita l'impostazione della chiave gestita dal cliente dall'ambiente WorkSpaces Thin Client.

Un contesto di crittografia è un insieme opzionale di coppie chiave-valore che contiene informazioni contestuali aggiuntive sui dati.

AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, includi lo stesso contesto di crittografia nella richiesta.

Contesto di crittografia Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client utilizza lo stesso contesto di crittografia in tutte le operazioni crittografiche AWS KMS, in cui la chiave è `aws:thinclient:arn` e il valore è Amazon Resource Name (ARN).

Di seguito è riportato il contesto di crittografia Environment:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

Di seguito è riportato il contesto di crittografia del dispositivo:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

Utilizzo del contesto di crittografia per il monitoraggio

Quando si utilizza una chiave simmetrica gestita dal cliente per crittografare i dati dell'ambiente WorkSpaces Thin Client e del dispositivo, è inoltre possibile utilizzare il contesto di crittografia nei record e nei registri di controllo per identificare come viene utilizzata la chiave gestita dal cliente. Il contesto di crittografia appare anche nei log generati da AWS CloudTrail o Amazon CloudWatch Logs.

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come condizioni per controllare l'accesso alla chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

Amazon WorkSpaces Thin Client utilizza un vincolo di contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nel tuo account o nella tua regione. Il vincolo

della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

Di seguito sono riportati alcuni esempi di istruzioni delle policy delle chiavi per concedere l'accesso a una chiave gestita dal cliente per un contesto di crittografia specifico. La condizione di questa istruzione della policy richiede che la chiamata `kms:Decrypt` abbia un vincolo di contesto di crittografia che specifica il contesto di crittografia.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Monitoraggio delle chiavi di crittografia per Amazon WorkSpaces Thin Client

Quando utilizzi una chiave gestita dal cliente AWS KMS con le tue risorse Amazon WorkSpaces Thin Client, puoi utilizzare AWS CloudTrail Amazon CloudWatch Logs per tenere traccia delle richieste che Amazon WorkSpaces Thin Client invia a AWS KMS.

I seguenti esempi sono AWS CloudTrail eventi per`DescribeKey`,, `CreateGrant` `GenerateDataKeyDecrypt`, `Decrypt` (utilizzo`Grant`) per monitorare le operazioni KMS chiamate da Amazon WorkSpaces Thin Client per accedere ai dati crittografati dalla chiave gestita dal cliente:

Nei seguenti esempi, puoi vedere `encryptionContext` per quanto riguarda l'ambiente WorkSpaces Thin Client. CloudTrail Eventi simili vengono registrati per il dispositivo WorkSpaces Thin Client.

DescribeKey

Amazon WorkSpaces Thin Client utilizza l'`DescribeKey`operazione per verificare la chiave gestita dal cliente AWS KMS.

L'evento di esempio seguente registra l'operazione `DescribeKey`:

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateGrant

Amazon WorkSpaces Thin Client utilizza l'`CreateGrant`operazione per creare un KMS Grant, che consente di decrittografare i dati quando il dispositivo vi accede.

L'evento di esempio seguente registra l'operazione `CreateGrant`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
```

```
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces Thin Client utilizza l'`GenerateDataKey`operazione per crittografare i dati.

L'evento di esempio seguente registra l'operazione `GenerateDataKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces Thin Client utilizza l'`Decrypt`operazione per decrittografare i dati.

L'evento di esempio seguente registra l'operazione `Decrypt`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
```

```
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

Quando WorkSpaces Thin Client Device accede alle informazioni sull'ambiente o sul dispositivo, viene utilizzata l'`Decrypt`operazione, che è consentita tramite una chiave KMS. `Grant`

L'evento di esempio seguente registra l'`Decrypt`operazione, autorizzata tramite un: `Grant`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
```

```
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati inattivi:

- Per ulteriori informazioni, consulta Concetti di base su AWS Key Management Service nella Guida per gli sviluppatori di AWS Key Management Service.

- Per ulteriori informazioni sulle best practice di sicurezza per AWS Key Management Service, consulta la AWS Key Management Service Developer Guide.

Crittografia in transito

WorkSpaces Thin Client crittografa i dati in transito tramite HTTPS e TLS 1.2. È possibile inviare una richiesta a WorkSpaces Thin Client utilizzando la console o chiamate API dirette. I dati della richiesta trasferiti vengono crittografati inviandoli tramite una connessione HTTPS o TLS. I dati della richiesta possono essere trasferiti dalla AWS console, dall'interfaccia a riga di AWS comando o dall' AWS SDK a WorkSpaces Thin Client. Ciò include anche eventuali aggiornamenti software sul dispositivo.

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

Gestione delle chiavi

Puoi fornire la tua chiave AWS KMS gestita dal cliente per crittografare le informazioni dei tuoi clienti. Se non fornisci una chiave, WorkSpaces Thin Client utilizza una chiave AWS proprietaria. Puoi impostare la tua chiave utilizzando l' AWS SDK.

Privacy del traffico di lavoro su Internet

Gli amministratori possono visualizzare gli eventi delle sessioni di WorkSpaces Thin Client, inclusi gli orari di inizio e le informazioni sugli aggiornamenti software in sospeso. Questi registri sono crittografati e consegnati in modo sicuro ai clienti nella console Thin Client. WorkSpaces Le informazioni sugli utenti e ulteriori dettagli sulle singole sessioni desktop di streaming vengono registrate dai servizi desktop. Per ulteriori informazioni, consulta Monitoring your WorkSpaces, Monitoring and Reporting for AppStream 2.0 o User access logging for WorkSpaces Web.

Gestione delle identità e degli accessi per Amazon WorkSpaces Thin Client

AWS Identity and Access Management (IAM) è uno strumento 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 Thin Client. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui si utilizza AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in WorkSpaces Thin Client.

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

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

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

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

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

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

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

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

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

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

Ruoli IAM

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

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati 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 ai servizi, ma non modificarle.

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

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

Gestione dell'accesso con policy

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

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

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

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

Policy basate su identità

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

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

Policy basate su risorse

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

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

Liste di controllo degli accessi (ACL)

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

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

Altri tipi di policy

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

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

Più tipi di policy

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

Come funziona Amazon WorkSpaces Thin Client con IAM

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

Funzionalità IAM che puoi utilizzare con Amazon WorkSpaces Thin Client

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

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

Politiche basate sull'identità per Thin Client WorkSpaces

Supporta le policy basate su identità	Sì

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

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

Esempi di policy basate sull'identità per Thin Client WorkSpaces

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

Politiche basate sulle risorse all'interno di Thin Client WorkSpaces

Supporta le policy basate su risorse	No

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

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

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

Azioni politiche per WorkSpaces Thin Client

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

Per visualizzare un elenco di azioni WorkSpaces Thin Client, consulta Actions Defined by Amazon WorkSpaces Thin Client nel Service Authorization Reference.

Le azioni politiche in WorkSpaces Thin Client utilizzano il seguente prefisso prima dell'azione:

```
workspaces-thin-client
```

Per specificare più azioni in una singola istruzione, separale con virgole, come mostrato nell'esempio seguente:

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

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

Risorse relative alle policy per Thin Client WorkSpaces

Supporta le risorse di policy	Sì

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

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

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

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

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

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

Chiavi delle condizioni delle policy per Thin Client 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. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

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

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. 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 delle chiavi di condizione di WorkSpaces Thin Client, consulta Condition Keys for Amazon WorkSpaces Thin Client nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Actions Defined by Amazon WorkSpaces Thin Client.

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

ACL in Thin Client WorkSpaces

Supporta le ACL	No

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

ABAC con WorkSpaces Thin Client

Supporta ABAC (tag nelle policy)	Sì

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

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

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

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

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

Utilizzo di credenziali temporanee con WorkSpaces Thin Client

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente

e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Thin Client WorkSpaces

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per WorkSpaces Thin Client

Supporta i ruoli di servizio	No

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

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

Ruoli collegati ai servizi per WorkSpaces Thin Client

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati 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 ai servizi, ma non modificarle.

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

Esempi di policy basate sull'identità per Amazon Thin Client WorkSpaces

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

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

Per dettagli sulle azioni e sui tipi di risorse definiti da WorkSpaces Thin Client, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Actions, Resources and Condition Keys for Amazon WorkSpaces Thin Client nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Thin WorkSpaces Client
- Concedi l'accesso in sola lettura a Thin Client WorkSpaces
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concedi l'accesso completo a Thin Client WorkSpaces

Best practice per le policy

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

- 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 ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- 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, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console Thin WorkSpaces Client

Per accedere alla console Amazon WorkSpaces Thin Client, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse WorkSpaces Thin Client 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, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Concedi l'accesso in sola lettura a Thin Client WorkSpaces

Questo esempio mostra come è possibile creare una policy che consenta agli utenti IAM di visualizzare una configurazione WorkSpaces Thin Client, ma non di apportare modifiche. Questa policy include le autorizzazioni per completare questa azione sulla console o sul programma utilizzando l'AWS CLI o l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
```

```
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o in modo programmatico. 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": "*"
        }
    ]
}
```

Concedi l'accesso completo a Thin Client WorkSpaces

Questo esempio mostra come è possibile creare una policy che garantisca l'accesso completo agli utenti IAM di WorkSpaces Thin Client. Questa policy include le autorizzazioni per completare tutte le azioni WorkSpaces Thin Client sulla console o sul programma utilizzando l'AWS CLI o l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
```

```
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

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

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

Argomenti

Non sono autorizzato a eseguire un'azione in WorkSpaces Thin Client

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue politiche per consentirgli di accedere alla *my-thin-client-device* risorsa utilizzando l'`workspaces-thin-client:`*ListDevices*azione.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non è possibile visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

> **Important**
>
> Non fornire le chiavi di accesso a terze parti, neppure per aiutare a trovare l'ID utente canonico. In questo modo, potresti concedere a qualcuno l'accesso permanente al tuo Account AWS.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consulta Gestione delle chiavi di accesso nella Guida per l'utente di IAM.

Sono un amministratore e voglio consentire ad altri di accedere a WorkSpaces Thin Client

Per consentire ad altri di accedere a WorkSpaces Thin Client, è necessario creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che necessita di accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. È quindi necessario allegare una policy all'entità che conceda loro le autorizzazioni corrette in WorkSpaces Thin Client.

Per iniziare immediatamente, consulta Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

Per ulteriori informazioni, consulta Concedi l'accesso completo a Thin Client WorkSpaces .

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse WorkSpaces Thin Client

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se WorkSpaces Thin Client supporta queste funzionalità, consultaCome funziona Amazon WorkSpaces Thin Client con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Resilienza in Amazon WorkSpaces Thin Client

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, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

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

Oltre all'infrastruttura AWS globale, WorkSpaces Thin Client offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Analisi e gestione delle vulnerabilità in Amazon WorkSpaces Thin Client

La configurazione e i controlli IT sono una responsabilità condivisa tra te AWS e te. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Amazon WorkSpaces Thin Client si integra in modo incrociato con WorkSpaces Amazon, Amazon AppStream 2.0 e WorkSpaces Web. Consulta i seguenti link per ulteriori informazioni sulla gestione degli aggiornamenti per ciascuno di questi servizi:

- Gestione degli aggiornamenti in Amazon AppStream 2.0
- Gestione degli aggiornamenti in Amazon WorkSpaces
- Analisi della configurazione e delle vulnerabilità in Amazon Web WorkSpaces

Monitoraggio di Amazon WorkSpaces Thin Client

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

- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log al bucket Amazon S3 da te specificato. Puoi identificare gli utenti e gli account che hanno effettuato la chiamata AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Registrazione delle chiamate API Amazon WorkSpaces Thin Client utilizzando AWS CloudTrail

Amazon WorkSpaces Thin Client è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in WorkSpaces Thin Client. CloudTrail acquisisce tutte le chiamate API per WorkSpaces Thin Client come eventi. Le chiamate acquisite includono chiamate dalla console WorkSpaces Thin Client e chiamate di codice alle operazioni dell'API WorkSpaces Thin Client. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per WorkSpaces Thin Client. 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, è possibile determinare la richiesta che è stata effettuata a WorkSpaces Thin Client, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

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

WorkSpaces Informazioni su Thin Client in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in WorkSpaces Thin Client, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, inclusi gli eventi per WorkSpaces Thin Client, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo 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 WorkSpaces Thin Client vengono registrate CloudTrail e documentate nell'Amazon WorkSpaces Thin Client API Reference. Ad esempio, le chiamate alle `GetSoftwareSet` azioni `CreateEnvironmentListDevices`, e 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 credenziali utente root o AWS Identity and Access Management (IAM).
- 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.

Comprendere le voci dei file di registro di WorkSpaces Thin Client

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 così via. 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'`GetDevice`azione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
```

```
}
```

Creazione di risorse Amazon WorkSpaces Thin Client con AWS CloudFormation

Amazon WorkSpaces Thin Client è integrato con AWS CloudFormation, un servizio che ti aiuta a modellare e configurare AWS le tue risorse. In questo modo, puoi dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come gli ambienti) e fornisce AWS CloudFormation e configura tali risorse per te.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse WorkSpaces Thin Client in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse ripetutamente in più Account AWS regioni.

WorkSpaces Thin Client e AWS CloudFormation modelli

Per fornire e configurare le risorse per WorkSpaces Thin Client e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in formato JSON o YAML. Questi modelli descrivono le risorse che desideri inserire negli stack. AWS CloudFormation Se non conosci i formati JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

WorkSpaces Thin Client supporta la creazione di ambienti in. AWS CloudFormationPer ulteriori informazioni, inclusi esempi di modelli JSON e YAML per ambienti, consulta il riferimento al tipo di risorsa Amazon WorkSpaces Thin Client nella Guida per l'AWS CloudFormation utente.

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- Documentazione di riferimento delle API AWS CloudFormation
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Accedi ad Amazon WorkSpaces Thin Client utilizzando un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e Amazon WorkSpaces Thin Client. Puoi accedere a WorkSpaces Thin Client come VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non richiedono indirizzi IP pubblici per WorkSpaces accedere a Thin Client.

Questa connessione privata viene stabilita creando un endpoint di interfaccia alimentato da. AWS PrivateLink In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato a Thin Client. WorkSpaces

Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida di AWS PrivateLink .

Considerazioni per Thin Client WorkSpaces

Prima di configurare un endpoint di interfaccia per WorkSpaces Thin Client, consulta le considerazioni nella Guida.AWS PrivateLink

WorkSpaces Thin Client supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per WorkSpaces Thin Client

Puoi creare un endpoint di interfaccia per WorkSpaces Thin Client utilizzando la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per WorkSpaces Thin Client utilizzando il seguente nome di servizio:

```
com.amazonaws.region.thinclient.api
```

Se si abilita il DNS privato per l'endpoint dell'interfaccia, è possibile effettuare richieste API a WorkSpaces Thin Client utilizzando il nome DNS regionale predefinito. Ad esempio, `api.thinclient.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint offre l'accesso completo a WorkSpaces Thin Client tramite l'endpoint dell'interfaccia. Per controllare l'accesso concesso a WorkSpaces Thin Client dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di 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 in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC per WorkSpaces le azioni Thin Client

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

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

Cronologia dei documenti per la WorkSpaces Thin Client Administrator Guide

La tabella seguente descrive la cronologia della documentazione per le versioni della WorkSpaces Thin Client Administrator Guide.

Modifica	Descrizione	Data
• Configurazione WorkSpaces per Amazon WorkSpaces Thin Client • Configurazione AppStream 2.0 per Amazon WorkSpaces Thin Client	• Aggiornato l'elenco dei sistemi operativi. • È stata aggiornata la procedura Identity Provider.	12 febbraio 2024
Rilascio iniziale	Rilascio iniziale	26 novembre 2023

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.