



Guida per l'amministratore

Amazon WorkSpaces Thin Client



Amazon WorkSpaces Thin Client: Guida per l'amministratore

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

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

Table of Contents

Cos'è la console di amministrazione di Amazon WorkSpaces Thin Client?	1
È il primo utilizzo?	1
Architecture	1
Configurazione della console di amministrazione Amazon WorkSpaces Thin Client	4
Registrazione ad AWS	4
Crea un utente IAM	4
Guida introduttiva alla console di amministrazione VDI per Amazon WorkSpaces Thin Client	6
Configurazione di WorkSpaces Personal per WorkSpaces Thin Client	6
Prima di iniziare	7
Fase 1: Verificare che il sistema soddisfi le funzionalità WorkSpaces personali richieste	7
Fase 2: Utilizza la configurazione avanzata per avviare il WorkSpace	8
Continuità aziendale	9
Configurazione dei WorkSpaces pool per WorkSpaces Thin Client	10
Prima di iniziare	10
Crea un WorkSpaces pool	11
Configurazione dell'accesso WorkSpaces Thin Client	13
Configurazione delle WorkSpaces applicazioni per Amazon WorkSpaces Thin Client	14
Fase 1: Verificare che il sistema soddisfi WorkSpaces le funzionalità richieste dall'applicazione	14
Fase 2: Configura gli stack WorkSpaces delle applicazioni	15
Configurazione di Amazon WorkSpaces Secure Browser per Amazon WorkSpaces Thin Client	16
Passaggio 1: verifica che il sistema soddisfi le funzionalità richieste da Amazon WorkSpaces Secure Browser	16
Passaggio 2: configurare i portali WorkSpaces Secure Browser	17
Avvio della console di amministrazione WorkSpaces Thin Client	18
Regioni coperte	18
Avvio della console di amministrazione WorkSpaces Thin Client	19
Utilizzo della console di amministrazione WorkSpaces Thin Client	20
Ambienti	21
Elenco di ambienti	21
Dettagli dell'ambiente	23
Creazione di un ambiente	26
Modifica di un ambiente	30

Eliminazione di un ambiente	31
dispositivi	31
Un elenco dispositivi	31
Dettagli del dispositivo	35
Modifica del nome di un dispositivo	41
Reimpostazione e annullamento della registrazione di un dispositivo	41
Archiviazione di un dispositivo	42
Eliminazione di un dispositivo	42
Esportazione dei dettagli del dispositivo	43
Aggiornamenti software	44
Aggiornamento del software dell'ambiente	45
Aggiornamento del software del dispositivo	46
WorkSpaces Versioni del software Thin Client	46
Utilizzo dei tag nelle risorse WorkSpaces Thin Client	61
Sicurezza	64
Protezione dei dati	64
Crittografia dei dati	66
Crittografia dei dati a riposo	67
Crittografia dei dati in transito	81
Gestione delle chiavi	81
Privacy del traffico di lavoro su Internet	81
Gestione dell'identità e degli accessi	82
Destinatari	82
Autenticazione con identità	82
Gestione dell'accesso tramite policy	84
Come funziona Amazon WorkSpaces Thin Client con IAM	86
Esempi di policy basate su identità	91
AWS politiche gestite	96
Risoluzione dei problemi	102
Resilienza	105
Analisi e gestione delle vulnerabilità	105
Monitoraggio	106
CloudTrail registri	106
CloudTrail eventi relativi ai dati	108
CloudTrail eventi di gestione	109
CloudTrail esempi di eventi	109

Monitora utilizzando le metriche CloudWatch	112
WorkSpaces Metriche Thin Client	113
AWS CloudFormation risorse	116
WorkSpaces Thin Client e CloudFormation modelli	116
Scopri di più su CloudFormation	116
AWS PrivateLink	117
Considerazioni	117
Creazione di un endpoint di interfaccia	117
Creazione di una policy dell'endpoint	118
Cronologia dei documenti	119
.....	cxxii

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?](#)
- [Architecture](#)

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](#)

Architecture

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

- [Amazon WorkSpaces](#)
- [WorkSpaces Applicazioni](#)
- [Browser WorkSpaces sicuro Amazon](#)

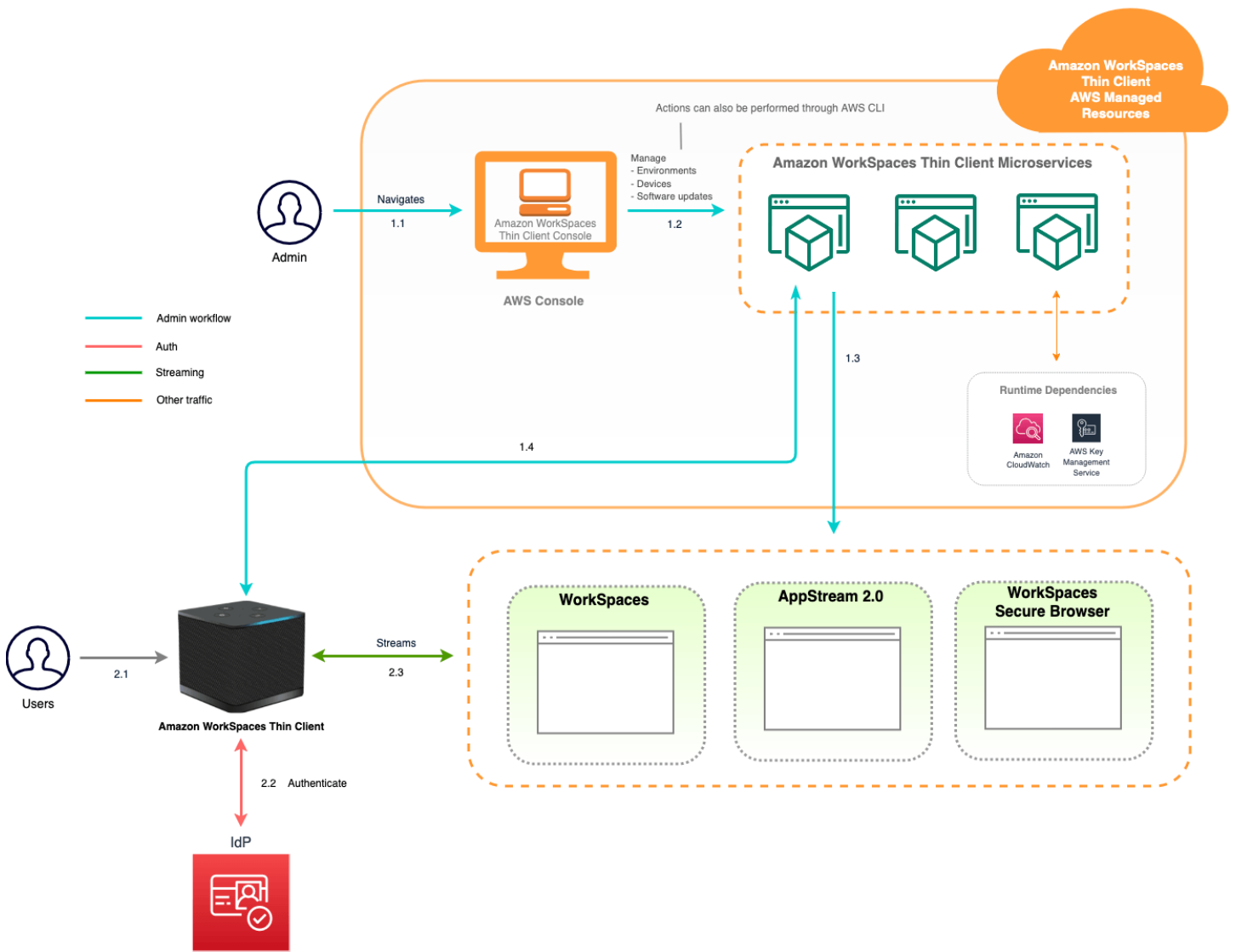
A seconda della VDI utilizzata, è possibile accedere e gestire le informazioni relative al WorkSpaces Thin Client tramite le directory WorkSpaces, gli stack per le WorkSpaces applicazioni e gli endpoint del portale Web per Secure Browser. WorkSpaces

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

Per ulteriori informazioni sulle WorkSpaces applicazioni, consulta [Get Started with Amazon WorkSpaces Applications: Configurazione con applicazioni di esempio](#). WorkSpaces Applications gestisce le AWS risorse necessarie per ospitare ed eseguire le applicazioni, si ridimensiona automaticamente e fornisce l'accesso agli utenti su richiesta. WorkSpaces Applications 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-serviceSaaS). 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



Configurazione della console di amministrazione Amazon WorkSpaces Thin Client

Argomenti

- [Registrazione ad AWS](#)
- [Crea un utente IAM](#)

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 <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un 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
<p>In IAM Identity Center</p> <p>(Consigliato)</p>	<p>Usa credenziali a breve termine per accedere a AWS.</p> <p>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.</p>	<p>Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .</p>	<p>Configura l'accesso programmatico configurando l'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface utente.</p>
<p>In IAM</p> <p>(Non consigliato)</p>	<p>Usa credenziali a lungo termine per accedere a AWS.</p>	<p>Segui le istruzioni in Creare un utente IAM per l'accesso di emergenza nella Guida per l'utente di IAM.</p>	<p>Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.</p>

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 di WorkSpaces Personal per WorkSpaces Thin Client](#)
- [Configurazione dei WorkSpaces pool per WorkSpaces Thin Client](#)
- [Configurazione delle WorkSpaces applicazioni per Amazon WorkSpaces Thin Client](#)
- [Configurazione di Amazon WorkSpaces Secure Browser per Amazon WorkSpaces Thin Client](#)

Configurazione di WorkSpaces Personal per WorkSpaces Thin Client

Affinché WorkSpaces Thin Client possa essere utilizzato con Amazon WorkSpaces Personal, il servizio deve essere configurato per accedere alle WorkSpaces directory. Le directory di Amazon WorkSpaces Personal sono elencate in base ai loro nomi di 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 [Protocolli per Amazon WorkSpaces Personal](#).
- 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 [Manage directories for WorkSpaces Personal](#).
- Quando avvii un Workspace, abilita e configura l'accesso web WorkSpaces Thin Client. Per ulteriori informazioni, vedere [Configurare WorkSpaces Thin Client](#)

Fase 1: Verificare che il sistema soddisfi le funzionalità WorkSpaces personali richieste

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

Funzionalità	Requisito
Accesso Web	Abilitato

Funzionalità	Requisito
Sistema operativo supportato	<ul style="list-style-type: none">• Windows 10• Windows 10 (BYOL)• Windows 11• Windows 11 (BYOL)
Pacchetti supportati	<ul style="list-style-type: none">• 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 DCV

Fase 2: Utilizza la configurazione avanzata per avviare il WorkSpace

Per utilizzare la configurazione avanzata per avviare il WorkSpace

1. Apri la WorkSpaces console all'indirizzo <https://console.aws.amazon.com/workspaces/v2/home/>.
2. Scegli uno dei seguenti tipi di directory, quindi scegli Successivo:
 - AWS Microsoft AD gestito
 - 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 directory.

Continuità aziendale

WorkSpaces Thin Client fornisce supporto per la continuità aziendale come parte di un [piano di continuità aziendale \(BCP\)](#). WorkSpaces La continuità aziendale di Thin Client è disponibile per l'uso solo con WorkSpaces Personal. Per ulteriori informazioni sulla continuità aziendale, consulta la sezione [Business continuity for WorkSpaces Personal](#) nella guida all' WorkSpaces amministrazione di Amazon.

Prerequisiti

Affinché la continuità aziendale funzioni su WorkSpaces Thin Client, devono essere soddisfatti i seguenti prerequisiti:

- Per il reindirizzamento WorkSpaces tra regioni: sono state configurate le policy di routing e di servizio DNS. Per configurarle, consulta [Configurare il servizio DNS e configurare le politiche di routing DNS](#).
- Per la resilienza WorkSpaces multiregionale: è stato creato uno standby. WorkSpaces Per crearlo, consulta [Creare uno standby](#). WorkSpace
- Un alias di connessione nella regione che utilizza WorkSpaces Thin Client. Per verificare la tua regione, [consulta Regioni coperte](#).

Configurazione della continuità aziendale per WorkSpaces Thin Client

Per abilitare WorkSpaces Personal DR su Amazon WorkSpaces Thin Client, dovrai configurare gli alias di connessione da mappare all'ambiente utilizzando l'SDK.

Esempio di spiegazione del documento per la configurazione del disaster recovery:

Example

Un comando di esempio che utilizza la AWS CLI per creare un nuovo ambiente utilizzando un alias di WorkSpaces connessione per il desktop di streaming:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
```

```
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

wsca-id Sostituiscilo con il tuo alias di connessione WorkSpaces personale. L'ID dell'alias di WorkSpaces connessione è disponibile nella Console di WorkSpaces gestione o nell'SDK.

Esperienza dell'utente finale

Una volta configurata la continuità aziendale, i dispositivi devono essere registrati e attivi negli ultimi 15 giorni. Dopodiché, se i servizi di gestione WorkSpaces Thin Client non fossero più disponibili, gli utenti possono rimanere connessi alle loro sessioni per un massimo di 24 ore. In questa condizione, il dispositivo non riceverà aggiornamenti software, non scambierà informazioni sulla postura e non potrà essere attivato. La voce corrispondente del dispositivo nella console WorkSpaces Thin Client non mostrerà le informazioni più recenti.

Se i servizi di gestione dei dispositivi WorkSpaces Thin Client rimangono non disponibili oltre 24 ore, verrà visualizzato il seguente messaggio di errore:

«Si è verificato un errore. Riprova. Se il problema persiste, contatta l'amministratore IT. (Codice di errore: 3006).»

Configurazione dei WorkSpaces pool per WorkSpaces Thin Client

WorkSpaces Affinché Thin Client possa essere utilizzato con Amazon WorkSpaces Pools, il tuo provider di identità SAML 2.0 (IdP) dovrà essere configurato per accedere WorkSpaces alla directory Pools. WorkSpaces Le directory Amazon Pools sono un pool non persistente WorkSpaces assegnato a un gruppo di utenti.

Note

Le configurazioni devono essere effettuate prima di utilizzare la console per la prima volta.

Prima di iniziare

Assicurati di avere 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 concetti elencati in [Prima di iniziare a usare Active Directory with WorkSpaces Pools](#) nella Amazon WorkSpaces Administration Guide prima di procedere con la configurazione.

Crea un WorkSpaces pool

Configura e crea un pool da cui vengono avviate e trasmesse in streaming le applicazioni utente.

Note

È necessario creare una directory prima di creare un WorkSpaces Pool. Per maggiori informazioni, consulta [Configurare SAML 2.0 e creare una directory di directory WorkSpaces Pools](#).

Per configurare e creare un pool

1. Apri la WorkSpaces console all'indirizzo <https://console.aws.amazon.com/workspaces/v2/home/>.
2. Nel riquadro di navigazione WorkSpaces, scegli Pools.
3. Scegli Crea WorkSpaces pool.
4. In Onboarding (opzionale), puoi scegliere le opzioni Consiglia a me in base al mio caso d'uso per ottenere consigli sul tipo di dispositivo che WorkSpaces desideri utilizzare. Puoi saltare questo passaggio se sai di voler usare Pools. WorkSpaces
5. In Configure WorkSpaces, inserisci i seguenti dettagli:
 - Per Nome, inserisci un identificatore univoco per il pool. I caratteri speciali non sono consentiti.
 - In Descrizione, inserisci una descrizione per il pool (massimo 256 caratteri).
 - Per Bundle, scegli tra i seguenti il tipo di pacchetto che desideri utilizzare per il tuo WorkSpaces
 - Usa un WorkSpaces pacchetto base: scegli uno dei pacchetti dal menu a discesa. Per ulteriori informazioni sul tipo di pacchetto selezionato, scegli Dettagli del pacchetto. Per confrontare i pacchetti offerti per i pool, scegli Confronta tutti i pacchetti.
 - Usa il tuo pacchetto personalizzato: scegli un pacchetto creato in precedenza. Per creare un pacchetto personalizzato, consulta [Creare un' WorkSpaces immagine e un pacchetto personalizzati](#) per Personal. WorkSpaces

Note

Il BYOL non è attualmente disponibile per i pool. WorkSpaces

- Per Durata massima della sessione in minuti, scegli la quantità massima di tempo in cui una sessione di streaming può rimanere attiva. Se gli utenti sono ancora connessi a un'istanza di streaming cinque minuti prima del raggiungimento di questo limite, viene richiesto loro di salvare tutti i documenti aperti prima di disconnettersi. Trascorso questo periodo, l'istanza viene terminata e sostituita da una nuova istanza. La durata massima della sessione che è possibile impostare nella console WorkSpaces Pools è di 5760 minuti (96 ore). La durata massima della sessione che è possibile impostare utilizzando l'API WorkSpaces Pools e la CLI è di 432000 secondi (120 ore).
- Per Disconnect timeout in minutes (Scollega timeout in pochi minuti), scegliere la quantità di tempo in cui una sessione di streaming rimane attiva dopo la disconnessione degli utenti. Se gli utenti provano a riconnettersi alla sessione di streaming dopo una disconnessione o un'interruzione di rete entro questo intervallo di tempo, vengono connessi alla sessione precedente. Altrimenti, sono connessi a una nuova sessione con una nuova istanza di streaming.
- Se un utente termina la sessione scegliendo Termina sessione o Esci dalla barra degli strumenti del pool, il timeout di disconnessione non si applica. All'utente viene invece richiesto di salvare tutti i documenti aperti e quindi viene immediatamente disconnesso dall'istanza di streaming. L'istanza utilizzata dall'utente viene quindi terminata.
- Per Idle disconnect timeout in minutes (Timeout disconnessione inattività in pochi minuti), scegliere la quantità di tempo in cui gli utenti possono rimanere inattivi prima di essere disconnessi dalla sessione di streaming e l'inizio dell'intervallo di tempo Disconnect timeout in minutes (Timeout disconnessione in minuti). Gli utenti vengono avvisati prima di essere disconnessi per inattività. Se tentano di riconnettersi alla sessione di streaming prima che sia trascorso l'intervallo di tempo specificato in Disconnect timeout in minutes (Timeout disconnessione in minuti), vengono collegati alla sessione precedente. In caso contrario, vengono collegati a una nuova sessione con una nuova istanza di streaming. L'impostazione di questo valore su 0 lo disabilita. Quando questo valore viene disabilitato, gli utenti non vengono disconnessi a causa di inattività.

Note

Gli utenti vengono considerati inattivi quando smettono di fornire input da tastiera o mouse durante la sessione di streaming. Per i pool aggiunti a un dominio, il conto alla rovescia per il timeout di disconnessione dell'inattività non inizia finché gli utenti non accedono con la password del dominio Active Directory o con una smart card. Download e upload dei file, file audio in entrata e in uscita e modifiche dei pixel non

vengono considerati attività degli utenti. Se gli utenti continueranno ad essere inattivi una volta trascorso Idle disconnect timeout in minutes (Timeout disconnessione inattività in pochi minuti), vengono disconnessi.

- Per i criteri di capacità pianificata (facoltativi), scegli Aggiungi nuova capacità di pianificazione. Indica la data e l'ora di inizio e fine in cui effettuare il provisioning del numero minimo e massimo di istanze per il pool in base al numero minimo di utenti simultanei previsti.
- Per le politiche di scalabilità manuale (facoltative), specifica le politiche di scalabilità per i pool da utilizzare per aumentare e diminuire la capacità del pool. Espandi le politiche di scalabilità manuale per aggiungere nuove politiche di scalabilità.

Note

La dimensione del pool è limitata dalla capacità minima e massima specificata.

- Scegli Aggiungi nuove politiche di scalabilità orizzontale e inserisci i valori per l'aggiunta di istanze specifiche se l'utilizzo della capacità specificato è inferiore o superiore al valore di soglia specificato.
 - Scegli Aggiungi nuova scala nelle politiche e inserisci i valori per rimuovere le istanze specificate se l'utilizzo della capacità specificato è inferiore o superiore al valore di soglia specificato.
 - Per i tag, specifica il valore della coppia di chiavi che desideri utilizzare. Una chiave può essere una categoria generale, ad esempio «progetto», «proprietario» o «ambiente», con valori associati specifici.
6. Nella pagina Seleziona directory, scegli la directory che hai creato. Per creare una directory, scegli Crea cartella. Per ulteriori informazioni, consulta [Gestire le directory per i WorkSpaces pool](#).
 7. Scegli Crea WorkSpace pool.

Configurazione dell'accesso WorkSpaces Thin Client

Per configurare l'accesso Web per i WorkSpaces pool in modo che utilizzino WorkSpaces Thin Client, sarà necessario utilizzare l'interfaccia a riga di AWS comando.

1. Installa o aggiorna il [AWS Command Line Interface](#)

2. Configura [AWS CLI le tue impostazioni](#).
3. Apri il AWS CLI.
4. Esegui quanto segue sostituendo `WORKSPACES_DIRECTORY_ID` e `REGION` con le informazioni appropriate:

```
aws workspaces modify-workspace-access-properties --resource-id WORKSPACES_DIRECTORY_ID --workspace-access-properties '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

Configurazione delle WorkSpaces applicazioni per Amazon WorkSpaces Thin Client

WorkSpaces Le istanze delle applicazioni verranno elencate in base ai nomi degli stack e richiederanno la configurazione di un URL di accesso IdP nella pagina di creazione dell'ambiente. Poiché l'autenticazione SAML for WorkSpaces Applications 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 WorkSpaces le funzionalità richieste dall'applicazione

Affinché la console di amministrazione WorkSpaces Thin Client funzioni correttamente con WorkSpaces le applicazioni, 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 l'amministratore WorkSpaces delle applicazioni per creare un provider di identità.

Funzionalità	Requisito
	Quando ti viene richiesto di creare la console env, inserisci l'URL di accesso IDP.
Sistema operativo	Windows
Tipo di piattaforma	Windows Server (2012 R2, 2016 o 2019)
Appunti	Disabilita Configurato a livello di stack di WorkSpaces applicazioni
Trasferimento di file	Disabilita Configurato a livello di stack di WorkSpaces applicazioni
Stampa su dispositivo locale	Disabilita Configurato a livello di WorkSpaces stack di applicazioni

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

Fase 2: Configura gli stack WorkSpaces delle applicazioni

Per lo streaming delle WorkSpaces applicazioni, Applications 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 riportate in Guida [introduttiva alle WorkSpaces applicazioni: 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
Appunti	Disabilita
Trasferimento di file	Disabilita

Funzionalità	Requisito
Stampa su dispositivo locale	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 e fornire un accesso sicuro e immediato alle applicazioni e ai desktop virtuali.

Argomenti

- [Regioni coperte](#)
- [Avvio della console di amministrazione WorkSpaces Thin Client](#)

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, 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

End User Computing

Amazon WorkSpaces Thin Client

Affordable, easy-to-manage thin client for secure access to virtual desktops

Improve end-user productivity by going from unboxing to desktop access in just a few minutes, while improving IT staff productivity through centralized remote management of your fleet.

Amazon WorkSpaces Thin Client
Create WorkSpaces Thin Client environment, enabling users to securely access virtual desktops.

[Get started](#) [Order devices](#)

How it works

Admin management flow

Amazon WorkSpaces Thin Client
Cost-effective, secure, and easy-to-manage access to virtual desktops

Administrator sets up Amazon WorkSpaces, Amazon WorkSpaces Web, or Amazon AppStream 2.0 in desired AWS Region to associate with WorkSpaces Thin Client service

Administrator copies activation codes from Console and emails them to end users

End users enter activation code to register the device and log into their virtual desktop environment

Administrator manages, monitors, and maintains WorkSpaces Thin Client fleet and controls access through device management service

Pricing

You pay up front for the WorkSpaces Thin Client device, plus a monthly service fee per device to manage, monitor, and maintain your thin client fleet in the WorkSpaces Thin Client management console.

[Learn more about WorkSpaces Thin Client pricing](#)

Amazon WorkSpaces Thin Client devices

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](#)
- [dispositivi](#)
- [Aggiornamenti software](#)

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](#)
- [WorkSpaces Applicazioni](#)
- [Browser WorkSpaces sicuro Amazon](#)

Elenco di ambienti

Esistono diversi parametri del tuo ambiente da esaminare e alcune azioni che puoi intraprendere.

The screenshot shows the 'Environments' page in the Amazon WorkSpaces Thin Client console. It includes a 'Getting started' section with three numbered steps: 1. Enter your environment details, 2. Select your virtual desktop provider, and 3. Send the activation codes to your device users. Below this is a table of environments with columns for Name, Virtual desktop service, Virtual desktop service ID, Activation code, Device count, and Time created. The table lists four environments: Environment 01, Environment 02, Environment 03, and Environment 04.

Name	Virtual desktop service	Virtual desktop service ID	Activation code	Device count	Time created
Environment 01	WorkSpaces	d-00000000	ghe1tpa5	1	October 16, 2023, 20:38 (UTC-07:00)
Environment 02	WorkSpaces	d-00000000	ghi5rax1	1	October 13, 2023, 11:38 (UTC-07:00)
Environment 03	WorkSpaces	d-00000000	ghi13e0p	0	October 03, 2023, 21:22 (UTC-07:00)
Environment 04	WorkSpaces	d-00000000	ghn0f2br	0	October 03, 2023, 21:22 (UTC-07:00)

Dettagli dell'elenco di ambienti

I parametri relativi all'ambiente sono elencati per la revisione. La tabella seguente elenca ogni elemento del riepilogo e il relativo funzionamento.

Elemento	Description
Nome	L'identificatore univoco associato a questo ambiente.

Elemento	Description
Servizio di 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	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.
Ora di creazione	La data e l'ora di creazione dell'ambiente.

Operazioni per l'elenco di ambienti

Da qui è possibile eseguire diverse azioni. Seleziona una di queste per eseguire l'azione corrispondente.

Elemento	Description
Cerca	Cerca in tutti gli ambienti che gestisci.
Aggiorna	Aggiorna l'elenco degli ambienti.
Visualizzazione dei dettagli	Visualizza i dettagli dell'ambiente .
Azioni	Apri un elenco a discesa in cui è possibile modificare o eliminare un ambiente.
Crea ambiente	Avvia il processo di creazione di un ambiente .

Argomenti

- [Dettagli dell'ambiente](#)
- [Creazione di un ambiente](#)

- [Modifica di un ambiente](#)
- [Eliminazione di un ambiente](#)

Dettagli dell'ambiente

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

Argomenti

- [Riepilogo](#)
- [Dettagli dell'ambiente desktop virtuale](#)

Riepilogo

La sezione Riepilogo fornisce una panoramica di alto livello delle funzionalità chiave dell'ambiente WorkSpaces Thin Client. La tabella seguente elenca ogni elemento del riepilogo e come funziona.

Summary		
Name DRK Environment - Mon, Aug 7, 2023, 16:03:41	Always keep software up-to-date Yes	Activation code
Virtual desktop service WorkSpaces Web	Maintenance window start time 00:00 (Device local time)	Associated devices 1
Virtual desktop service ID	Maintenance window end time 03:00 (Device local time)	Time created August 07, 2023, 16:04 (UTC-04:00)
	Maintenance window days of the week Sunday	Time last modified August 07, 2023, 16:04 (UTC-04:00)

Elemento	Description
Nome	L'identificatore univoco associato a questo ambiente.
Servizio di desktop virtuale	Il provider di desktop virtuale utilizzato da questo ambiente.
Nome del servizio di desktop virtuale	L'identificatore univoco che il provider di servizi di desktop virtuale assegna a questo ambiente.

Elemento	Description
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.
Intervallo di manutenzione (giorni della settimana)	I giorni in cui vengono effettuati 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

WorkSpaces Gli ambienti Thin Client vengono eseguiti su un'interfaccia desktop virtuale. Ogni interfaccia ha un diverso set di parametri che controllano l'ambiente dedicato.

Dettagli della WorkSpaces directory Amazon

WorkSpaces Gli ambienti Thin Client eseguiti su Amazon WorkSpaces utilizzano le directory per creare ed eseguire i propri desktop virtuali. La tabella seguente elenca ogni elemento nei dettagli e come funziona.

WorkSpaces directory details		
Directory ID abc	Organization name Name	Registered ✔ True
Directory name xyz	Directory type Simple AD	Status ✔ Active

Elemento	Description
ID della directory	La WorkSpaces directory Amazon associata a questo ambiente.
Nome della directory	L'identificatore univoco associato a questa WorkSpaces directory Amazon.
Nome organizzazione	Il nome dell'organizzazione che controlla la WorkSpaces directory Amazon.
Tipo di directory	Il formato della WorkSpaces directory Amazon.
Registered	Se questa WorkSpaces directory Amazon è registrata.
Status	Se questa WorkSpaces directory Amazon è attiva.

Dettagli del portale Amazon WorkSpaces Secure Browser

WorkSpaces Gli ambienti Thin Client eseguiti su Amazon WorkSpaces Secure Browser utilizzano portali Web per creare ed eseguire i propri desktop virtuali. La tabella seguente elenca ogni elemento nei dettagli e come funziona.

WorkSpaces Web portal details		
Name	Time created	Web portal endpoint
Custom Web Portal - Mon, Mar 06, 2023, 12:00:51 🔗	March 06, 2023, 13:50 (UTC-05:00)	

Elemento	Description
Nome	L'identificatore univoco associato a questo portale WorkSpaces Secure Browser.
Ora di creazione	La data e l'ora di creazione di questo portale WorkSpaces Secure Browser.

Elemento	Description
Endpoint del portale web	L'URL utilizzato per accedere all'ambiente desktop virtuale.

WorkSpaces Dettagli delle applicazioni

WorkSpaces Gli ambienti Thin Client vengono eseguiti sugli stack di informazioni WorkSpaces delle applicazioni per creare ed eseguire i rispettivi desktop virtuali. La tabella seguente elenca ogni elemento nei dettagli e come funziona.

AppStream 2.0 details		
Stack name xyz	IdP login url https://abc.com	Time created Thu Jun 08 2023 10:26:29 GMT-0700 (Pacific Daylight Time)


Elemento	Description
Stack name (Nome stack)	L'identificatore univoco associato a questo stack di WorkSpaces applicazioni.
URL di accesso IdP	L'URL del provider di identità utilizzato per accedere e disconnettersi dallo stack delle WorkSpaces applicazioni.
Ora di creazione	La data e l'ora di creazione dello stack di WorkSpaces applicazioni.

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
- WorkSpaces Applicazioni 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](#)
- [Fase 2: Selezione del provider di desktop virtuale](#)
- [Fase 3: Invio del codice di attivazione agli utenti del dispositivo](#)

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](#)
- [WorkSpaces Applicazioni](#)

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.
 - Crea una cartella 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 WorkSpaces delle applicazioni

WorkSpaces Applications 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.

⚠ Important

Per creare un ambiente WorkSpaces Applicazioni, 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 WorkSpaces le applicazioni, 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.
 - Crea una pila selezionando il pulsante **Crea pila**. Per ulteriori informazioni sulla creazione di stack di WorkSpaces applicazioni, 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.

- 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 di 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

Per ogni dispositivo della rete sono disponibili numerosi parametri da esaminare e alcune azioni che è possibile intraprendere.

Devices [Info](#) Order devices

This is a list of all end user devices that you manage, including information about the user logins for each device.

Devices (1) **Actions** ▼



1

	Device ID	Device name	Activity status
<input type="checkbox"/>	G0723H08	-	✔ Active

Dettagli dell'elenco di dispositivi

I parametri del tuo dispositivo sono elencati per la tua revisione. La tabella seguente elenca ogni elemento del riepilogo e il relativo funzionamento.

Elemento	Description
Numero di serie del dispositivo	Il numero di identificazione assegnato a un singolo dispositivo.
Nome dispositivo	(opzionale) Il nome univoco assegnato a un dispositivo.
Usato per ultimo da	Il numero identificativo dell'utente che accede al dispositivo. Disponibile solo quando si utilizza WorkSpaces Personal.
Stato dell'attività	Lo stato attuale di un dispositivo. Esistono due stati di stato: <ul style="list-style-type: none"> Attivo: connesso a una rete almeno una volta negli ultimi sette giorni. Inattivo: non connesso a una rete negli ultimi sette giorni.
Stato della registrazione	Conferma che un dispositivo è stato configurato, è associato a questo account AWS e fa

Elemento	Description
	<p>parte di un ambiente specifico. Può trovarsi in uno dei seguenti stati:</p> <ul style="list-style-type: none"> • Registrato: questo è lo stato predefinito. • Annullamento della registrazione: il dispositivo è in fase di ripristino e annullamento della registrazione. <div data-bbox="862 569 1507 835" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>È possibile eliminare un dispositivo se si trova in uno stato di annullamento della registrazione.</p> </div> <ul style="list-style-type: none"> • Annullata la registrazione: la registrazione del dispositivo è stata annullata con successo. <div data-bbox="862 974 1507 1241" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Puoi eliminare un dispositivo solo se si trova nello stato Annullamento o Annullamento della registrazione.</p> </div> <ul style="list-style-type: none"> • Archiviato: il dispositivo è archiviato.
ID ambiente	L'identificatore dell'ambiente a cui è collegato questo dispositivo.
Conformità del software	<p>Lo stato di conformità del software del dispositivo. Esistono due stati di stato:</p> <ul style="list-style-type: none"> • Conforme • Non conforme

Operazioni per l'elenco di dispositivi

Da qui è possibile eseguire diverse azioni. Seleziona una di queste per eseguire l'azione corrispondente.

Elemento	Description
Cerca	Cerca tutti i dispositivi che gestisci.
Aggiorna	Aggiorna l'elenco dei dispositivi.
Visualizzazione dei dettagli	Visualizza i dettagli del dispositivo.
Azioni	Apri un elenco a discesa in cui è possibile effettuare le seguenti operazioni: <ul style="list-style-type: none">• Modifica il nome del dispositivo• Annullare la registrazione• Archive (Archivia)• Elimina• Esporta i dettagli del dispositivo
Ordina dispositivi	Avvia il processo di ordinazione dei dispositivi.

Argomenti

- [Dettagli del dispositivo](#)
- [Modifica del nome di un dispositivo](#)
- [Reimpostazione e annullamento della registrazione di un dispositivo](#)
- [Archiviazione di un dispositivo](#)
- [Eliminazione di un dispositivo](#)
- [Esportazione dei dettagli del dispositivo](#)

Dettagli del dispositivo

Quando si seleziona un dispositivo, la console WorkSpaces Thin Client mostra i dettagli relativi a quel dispositivo affinché l'utente possa esaminarli. La console visualizza anche i dettagli sul tipo di rete del dispositivo e sulle periferiche collegate.

Argomenti


- [Riepilogo](#)
- [Impostazioni del dispositivo](#)
- [Attività dell'utente](#)

Riepilogo

La sezione Riepilogo fornisce una panoramica di alto livello delle funzionalità principali del dispositivo WorkSpaces Thin Client. La tabella seguente elenca ogni elemento del riepilogo e come funziona.

Summary

Device serial number

ARN 


Device name

-

Device type

-

Activity status

 Inactive

Environment ID

Enrollment status

Registered

Enrolled since


September 27, 2023, 20:33 (UTC-07:00)

Last logged in

October 07, 2023, 03:09 (UTC-07:00)

Last posture checked at

March 19, 2024, 17:53 (UTC-07:00)

 Not checked in for past 7 days

Current software version

-


Scheduled for software update

2.8.1

Software compliance

-

Elemento	Description
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 dispositivo	Il nome che dai a un dispositivo. Se non hai creato un nome, puoi assegnargli un nome o riceverà un nome predefinito.

Elemento	Description
Tipo dispositivo	Il tipo di dispositivo dell'utente finale collegato all'account.
Stato dell'attività	Lo stato attuale di questo dispositivo. I due stati di stato sono: <ul style="list-style-type: none">• Attivo• Inattivo
ID ambiente	Il numero di identificazione dell'ambiente utilizzato dal dispositivo.
Stato della registrazione	<p>Conferma che un dispositivo è stato configurato, è associato a questo account AWS e fa parte di un ambiente specifico. Può trovarsi in uno dei quattro stati seguenti:</p> <ul style="list-style-type: none">• Registrato: questo è lo stato predefinito.• Annullamento della registrazione: il dispositivo è in fase di ripristino e annullamento della registrazione.• Annullata registrazione: la registrazione del dispositivo è stata annullata con successo. <div data-bbox="862 1304 1508 1570" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Puoi eliminare il dispositivo solo se si trova nello stato Annullato o Archiviato.</p></div> <ul style="list-style-type: none">• Archiviato: questo dispositivo è stato contrassegnato dall'amministratore come non attualmente in servizio.
Iscritto dal	La data di attivazione del dispositivo.

Elemento	Description
Ultimo accesso	La data e l'ora dell'ultimo accesso.
Ultima postura verificata presso	La data e l'ora dell'ultimo check-in del dispositivo.
Versione attuale del software	La versione del software attualmente utilizzata da questo dispositivo.
Aggiornamento del software pianificato	La versione programmata del software sul dispositivo.
Conformità del software	<p>Conferma della validità del set di software. Esistono due stati di stato:</p> <ul style="list-style-type: none"> • Conforme • Non conforme
Usato per ultimo da	Il numero identificativo dell'utente che accede al dispositivo. Disponibile solo quando si utilizza WorkSpaces Personal.

Log degli utenti

User activity details (5) [Info](#) Export details ↻

< 1 > ⚙️

Device accessed on
August 28, 2023, 21:46 (UTC-04:00)
August 28, 2023, 18:18 (UTC-04:00)
August 24, 2023, 10:56 (UTC-04:00)
August 24, 2023, 10:56 (UTC-04:00)
August 24, 2023, 09:33 (UTC-04:00)

Elemento	Description
Ultimo accesso al dispositivo	La data e l'ora dell'ultimo utilizzo del dispositivo.

Impostazioni del dispositivo

I parametri del tuo dispositivo sono elencati per la tua revisione. La tabella seguente elenca ogni elemento e il suo funzionamento.

Note


Le informazioni sulle impostazioni del dispositivo vengono aggiornate solo quando il dispositivo è online. Se il dispositivo è offline, alcune informazioni potrebbero non essere aggiornate.

Intestazione e rete

WorkSpaces I dettagli del dispositivo Thin Client forniscono una panoramica delle connessioni di rete del dispositivo. La tabella seguente elenca ogni elemento e il suo funzionamento.

Device settings [Info](#)

Last synced on: October 21, 2024, 14:28 (UTC-07:00)

▼ Network	
Connection type ETHERNET	Local IP address
Status  Connected	Gateway address

Elemento	Description
Ultima sincronizzazione	La data e l'ora delle impostazioni più recenti del dispositivo vengono sincronizzate con la console.
Tipo di connessione	Il tipo di connessione di rete utilizzata dal dispositivo. Il tipo di connessione può essere Ethernet o Wifi.

Elemento	Description
Status	Lo stato della rete. Se il dispositivo è attualmente connesso o connesso negli ultimi 20 minuti, lo stato verrà visualizzato come «connesso». Se la rete è stata disconnessa per più di 20 minuti, lo stato cambierà per mostrare il tempo trascorso dall'ultima connessione del dispositivo a Internet, ad esempio «ultima connessione 20 minuti fa».
Indirizzo IP locale	L'indirizzo IP locale della rete connessa.
Indirizzo del gateway	L'indirizzo del gateway della rete connessa.

Bluetooth e periferiche

WorkSpaces I dettagli del dispositivo Thin Client forniscono un elenco di tutte le periferiche connesse a un dispositivo. La tabella seguente elenca ogni elemento e il suo funzionamento.

▼ **Bluetooth and peripheral devices**

Bluetooth
✔ Enabled

Connected peripheral devices (5)

Name	Type
Logitech USB Receiver Mouse	Mouse (USB)
Logitech USB Receiver	Keyboard (USB)
Plantronics Blackwire 5220 Series	Speaker (USB)
Plantronics Blackwire 5220 Series	Microphone (USB)
UVC Camera (046d:0825)	Webcam (USB)

Elemento	Description
Bluetooth	Lo stato Bluetooth del dispositivo. I due stati di stato sono: <ul style="list-style-type: none"> • Abilitato • Disabilitato

Elemento	Description
Dispositivi periferici collegati	L'elenco dei nomi delle periferiche collegate, ad esempio il mouse Logitech, e il tipo di periferiche collegate, ad esempio Mouse (USB).

Alimentazione e sospensione

Ogni dispositivo WorkSpaces Thin Client dispone di una modalità di risparmio energetico. La tabella seguente elenca lo stato di questa modalità.

▼ **Power and sleep**

Turn off display after
Never

Elemento	Description
Disattiva lo schermo dopo	Il periodo di inattività dopo il quale il dispositivo spegne lo schermo.

Attività dell'utente

Questa scheda mostra il registro delle informazioni di configurazione e utilizzo di un dispositivo specifico. La tabella seguente elenca ogni elemento di questo registro.

User activity details (1) [Info](#) Export details

Filter by device accessed date and time

Device accessed on	User ID	Virtual desktop service	Virtual desktop service ID	IP address	Session ID
March 06, 2025, 16:43 (UTC+01:00)	sld-demo	WorkSpaces	d-123456abcde	2a02:a46a:9b7c...	gw2-8a88e81

Elemento	Description
Dispositivo accessibile su	La data e l'ora di attivazione del dispositivo.
ID utente	Il numero identificativo dell'utente che accede al dispositivo.

Elemento	Description
Servizio di desktop virtuale	Il servizio di desktop virtuale utilizzato dal dispositivo.
ID del servizio di desktop virtuale	Il numero ID del servizio di desktop virtuale associato all'utente.
IP address (Indirizzo IP)	Il numero di identificazione dell'IP che accede al dispositivo.
Tipo di evento	Dettagli su come viene utilizzato il dispositivo.

Note

Ad eccezione di WorkSpaces Personal, mostra VDIs solo un evento avviato dal login.

Puoi utilizzare la barra di ricerca sopra la tabella per trovare informazioni specifiche nella tabella. Puoi anche filtrare i risultati della tabella per data e ora.

Puoi esportare la tabella in un file csv selezionando il pulsante Esporta dettagli.

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. È possibile 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.

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.

Il tuo Amazon WorkSpaces Thin Client: dati generati dall'uso del dispositivo

Il tuo Amazon WorkSpaces Thin Client genera e raccoglie dati sulle tue interazioni con esso.

Tipi di dati: Amazon WorkSpaces Thin Client genera dati sulle prestazioni del dispositivo, sui modelli di utilizzo e sulle interazioni con altri AWS servizi. Ciò include dati tecnici (come stato e impostazioni), dati di utilizzo (come i timestamp di accesso) e dati di diagnostica (come il registro di sistema, se pertinente).

Volume e raccolta dei dati: la quantità di dati generati varia in base all'utilizzo del dispositivo e dei servizi da parte dell'utente. I dati vengono raccolti continuamente durante il funzionamento del dispositivo.

Archiviazione dei dati: i dati del dispositivo vengono archiviati in modo sicuro sul dispositivo stesso o sui AWS server. Sono archiviati in formati strutturati e leggibili da una macchina.

Accesso ai dati: [puoi accedere ai dati del tuo dispositivo tramite il tuo AWS account seguendo le istruzioni elencate qui](#). Ulteriori informazioni, tra cui istruzioni sul download dei dati e informazioni sulla qualità del servizio, sono disponibili su queste [pagine](#).

Gestione dei dati: puoi esaminare i dati del tuo dispositivo tramite il tuo AWS account. Per saperne di più sulle pratiche relative ai dati del tuo dispositivo, consulta i nostri [Termini di servizio](#) e l'[Informativa sulla privacy](#).

Eliminazione dei dati: puoi eliminare i dati del dispositivo tramite il tuo AWS account. Per informazioni sulle opzioni di conservazione ed eliminazione dei dati, visita [Eliminazione di un dispositivo](#).

Condivisione dei dati con altri: AWS non condivide i dati del dispositivo con terze parti. Solo le terze parti autorizzate possono accedere ai dati previa approvazione dell'utente tramite i nostri processi di

[gestione delle identità e degli accessi](#). AWS condivide i dati personali con terze parti in casi limitati inclusi nell'[AWS Informativa sulla privacy](#).

Hai bisogno di aiuto? Visita l'[assistenza clienti](#) per contattare il nostro team di assistenza. Ciò non pregiudica il diritto dell'utente di presentare un reclamo ai sensi della legge applicabile.

Titolare dei dati: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Lussemburgo

Aggiornamenti software

WorkSpaces Thin Client richiede aggiornamenti software periodici per introdurre nuove funzionalità e applicare patch di sicurezza. Questi aggiornamenti sono rappresentati da un set di software con versioni.

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

Esistono due tipi di set software:

- Set di software che introducono nuove funzionalità, correggono i difetti e apportano miglioramenti generali. Vengono rilasciati mensilmente.
- Set software che contengono patch di sicurezza e correzioni per problemi critici. Questi vengono rilasciati quando necessario.

In qualità di amministratore, se non hai abilitato gli aggiornamenti software automatici nel tuo ambiente, i dispositivi registrati in quell'ambiente non riceveranno gli aggiornamenti software finché non invierai manualmente l'aggiornamento.

Quando vengono rilasciati nuovi set software, i set software precedenti scadono. A partire dalla data di rilascio di un set software con nuove funzionalità, hai 40 giorni prima della scadenza dei set software precedenti.

Per garantire che il livello di sicurezza del dispositivo rimanga intatto, il servizio aggiorna automaticamente i dispositivi se rileva software scaduto. Questo tipo di aggiornamento può interrompere le sessioni attive perché non rispetta la finestra di manutenzione o consente agli utenti

finali di ritardare l'aggiornamento. Per evitare ciò, consigliamo di aggiornare i set software almeno una volta ogni 30 giorni.

Note

Se viene rilasciato un set software con patch di sicurezza o un aggiornamento critico, tutti i set software precedenti scadranno dopo 3 giorni. Per garantire la sicurezza del dispositivo e ridurre al minimo le interruzioni delle operazioni quotidiane, consigliamo di aggiornare immediatamente questi set software.

Fate riferimento ai [set di software in ambiente WorkSpaces Thin Client](#) per l'elenco dei set software rilasciati.

Aggiornamento del software dell'ambiente

WorkSpaces Thin Client è un servizio di AWS End User Computing 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
2.20.3	03-19-2026	<ul style="list-style-type: none">• Risolve i problemi critici di sicurezza CVE-2026-3909 e CVE-2026-3910 di Chromium.
2.20.2	02-23-2026	<ul style="list-style-type: none">• Risolve il problema di sicurezza critico CVE-2026-2441 di Chromium.
2.20.1	11-18-2025	<ul style="list-style-type: none">• Risolve i problemi critici di sicurezza CVE-2025-13223 e CVE-2025-13224 di Chromium.
2.20.0	11-5-2025	<ul style="list-style-type: none">• Migliora l'autenticazione del dispositivo.
2.19.0	9-30-2025	<ul style="list-style-type: none">• Le azioni della barra degli strumenti come Restart, Shut down e Sleep ora richiedono agli utenti finali di effettuare nuovamente e l'autenticazione con WorkSpaces• È stato risolto un problema per cui gli utenti finali non erano in grado di utilizzare e i tasti Ctrl+Spazio per selezionare la colonna in Excel.• È stata modificata la parte interna delle pagine URLs Lock and Licensing.

Set di software	Data di rilascio	Modifiche
2.18.0	8-28-2025	<ul style="list-style-type: none">• Aggiunto il pulsante Esci dalla sessione alla barra degli strumenti del dispositivo.• È stato risolto un problema per cui la notifica dello stato dell'attività veniva mostrata erroneamente sul dispositivo.• È stato aggiunto il supporto per l'autenticazione FIDO2 in sessione.• Correzioni e miglioramenti generali.
2.17.0	7-30-2025	<ul style="list-style-type: none">• L'hub USB collegabile UD-3900Z è ora supportato per l'uso con Thin Client WorkSpaces• È stato aggiunto il supporto per AltGr i tasti con tastiere spagnole.• È stato risolto il problema che causava la duplicazione delle voci per l'attività della sessione utente per il dispositivo.• È stato aggiunto il supporto per il tasto Invio sul tastierino o numerico.• Correzioni e miglioramenti generali.

Set di software	Data di rilascio	Modifiche
2.16.2	7-22-2025	<ul style="list-style-type: none">• Risolve il problema di sicurezza critico CVE-2025-6558 di Chromium.
2.16.1	7-3-2025	<ul style="list-style-type: none">• Risolve il problema di sicurezza critico CVE-2025-6554 di Chromium.
2.16.0	27-6-2025	<ul style="list-style-type: none">• Aggiunte notifiche per la latenza di rete.• È stata aggiunta la possibilità di ripristino quando il secondo monitor si spegne durante una sessione.• È stato risolto il problema con i monitor che mostravano o una schermata bianca o non si estendevano automaticamente dopo che il dispositivo tornava dalla modalità di sospensione.
2.15.0	19/06/2025	<ul style="list-style-type: none">• Aggiunto il supporto per tastiere in spagnolo in America Latina e inglese internazionale.• Gli utenti finali visualizzano notifiche quando il dispositivo non rileva l'attività della tastiera o del mouse per un periodo di tempo prolungato.

Set di software	Data di rilascio	Modifiche
2.14.1	6-09-2025	<ul style="list-style-type: none">• Risolvi i problemi critici di sicurezza CVE-2025-5419 di Chromium.
2.13.0	31-3-2025	<ul style="list-style-type: none">• Gli utenti finali vedranno il sondaggio sul feedback sulla soddisfazione del prodotto come una notifica.• Aggiunge il supporto della funzionalità non definitiva per il flusso di FIDO2 autenticazione. Vedi i dettagli FIDO2 prima della sessione.• Il dispositivo non entrerà in modalità di sospensione se si audio/video sta giocando durante la sessione.• Gli utenti finali visualizzano le notifiche quando il monitor è connesso e disconnesso.• Il dispositivo raccoglie informazioni diagnostiche dal sistema operativo per migliorare il servizio.• Risolve un problema per cui veniva mostrata una data errata nelle Impostazioni per la data di installazione del software.
2.14.0	29-4-2025	<ul style="list-style-type: none">• Miglioramenti dell'usabilità e correzioni di bug.

Set di software	Data di rilascio	Modifiche
2.13.0	31-3-2025	<ul style="list-style-type: none">• Gli utenti finali vedranno il sondaggio sul feedback sulla soddisfazione del prodotto come una notifica.• Aggiunge il supporto della funzionalità non definitiva per il flusso di FIDO2 autenticazione. Vedi i dettagli FIDO2 prima della sessione.• Il dispositivo non entrerà in modalità di sospensione se si audio/video sta giocando durante la sessione.• Gli utenti finali visualizzano le notifiche quando il monitor è connesso e disconnesso.• Il dispositivo raccoglie informazioni diagnostiche dal sistema operativo per migliorare il servizio.• Risolve un problema per cui veniva mostrata una data errata nelle Impostazioni per la data di installazione del software.
2.12.0	1-30-2025	<ul style="list-style-type: none">• Risolve un problema a causa del quale l'utente finale veniva disconnesso dalla sessione premendo il pulsante Indietro del mouse.

Set di software	Data di rilascio	Modifiche
2.11.2	1-24-2025	<ul style="list-style-type: none">• Risolve un problema a causa del quale l'audio crepitava durante le chiamate con i movimenti del mouse tra i monitor.
2.11.1	12-27-2024	<ul style="list-style-type: none">• Risolve il problema dell'estensione automatica del doppio monitor.• Piccoli miglioramenti all'etichetta. VoiceView
2.11.0	19/12/2024	<ul style="list-style-type: none">• WorkSpaces Thin Client ora supporta e Magnifier. VoiceView
2.10.0	22/11/2024	<ul style="list-style-type: none">• Gli utenti finali possono utilizzare una scorciatoia da tastiera per comprimere la barra degli strumenti del dispositivo.

Set di software	Data di rilascio	Modifiche
2.9.0	28-10-2024	<ul style="list-style-type: none">• Gli amministratori possono ora visualizzare le impostazioni dei dispositivi degli utenti finali all'interno della AWS console nella pagina dei dettagli del dispositivo di un dispositivo specifico.• WorkSpaces Thin Client ora supporta monitor con risoluzione 2K per schermo singolo.• Gli utenti finali possono visualizzare le notifiche relative alla diagnostica di rete sui propri dispositivi WorkSpaces Thin Client.• L'utente finale può ora scegliere di posizionare la barra degli strumenti del dispositivo a sinistra o a destra in base alle proprie preferenze.• È stato risolto un problema a causa del quale il dispositivo non installava gli aggiornamenti software durante la sospensione o il periodo di inattività.

Set di software	Data di rilascio	Modifiche
2.8.1	09-26-2024	<ul style="list-style-type: none">È stato risolto un problema critico a causa del quale il secondo monitor non poteva essere acceso dopo la riattivazione del dispositivo dalla modalità di sospensione.
2.8.0	09-06-2024	<ul style="list-style-type: none">Thin Client supporta monitor con risoluzione 4K.Gli utenti possono connettersi alla sessione VDI anche se i servizi di gestione dei dispositivi WorkSpaces Thin Client sono temporaneamente non disponibili.È stato risolto il problema per cui la sezione dei dettagli delle attività degli utenti nella AWS console mostrava voci duplicate.Gli utenti finali possono utilizzare l' PrintScre en opzione durante lo streaming WorkSpaces su WorkSpaces Thin Client.
2.7.1	27/08/2024	<ul style="list-style-type: none">Correzioni zero-day per i problemi critici di sicurezza CVE-2024-7971 e CVE-2024-7965 di Chromium.

Set di software	Data di rilascio	Modifiche
2.7.0	29/07/2024	<ul style="list-style-type: none">• Miglioramenti alle prestazioni del secondo monitor.• È stato risolto un problema per cui la lingua della barra degli strumenti non era influenzata dalla modifica della lingua del dispositivo.• Il dispositivo ora raccoglie informazioni diagnostiche per migliorare il servizio.
2.6.0	07-09-2024	<ul style="list-style-type: none">• Gli utenti possono posticipare gli aggiornamenti software in arrivo in modo da poter completare il lavoro senza interruzioni.• Le impostazioni del dispositivo consentono agli utenti di dimenticare le reti salvate. WiFi• Miglioramenti delle prestazioni delle audio/video chiamate durante la sessione.• Alcune impostazioni utente per le sessioni VDI persistono anche dopo il riavvio del dispositivo.

Set di software	Data di rilascio	Modifiche
2.5.0	06-13-2024	<ul style="list-style-type: none">• 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 rinominato Accedi.• Miglioramenti delle prestazioni delle audio/video chiamate durante la sessione.
2.4.3	29-05-2024	<ul style="list-style-type: none">• Correzione immediata del problema critico di sicurezza CVE-2024-5274 di Chromium.
2.4.2	17-05-2024	<ul style="list-style-type: none">• Correzione immediata del problema critico di sicurezza CVE-2024-4947 di Chromium.

Set di software	Data di rilascio	Modifiche
2.4.1	15/05/2024	<ul style="list-style-type: none">• 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 mouse sui collegamenti AWS e Privacy nella pagina di WorkSpaces accesso per aprire il browser in modalità autonoma.
2.4.0	05-09-2024	<ul style="list-style-type: none">• È stato risolto un problema che bloccava «accounts.google.com» e impediva l'utilizzo di Google Workspace come sessione IDP for Applications. WorkSpaces• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Aggiunto il supporto per tastiere ISO con localizzazioni in inglese (Regno Unito), francese, tedesco, italiano e spagnolo.
2.1.2	26/01-2024	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Correzione immediata del problema critico di sicurezza CVE-2023-7024 di Chromium.
2.1.0	20-12/2023	<ul style="list-style-type: none">• Aggiunge un pulsante Home alle impostazioni del dispositivo e abilita il supporto per i tasti Meta. Ciò consente agli utenti finali di richiamare e la schermata di blocco premendo Meta+L.
2.0.1	12-06-2023	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.
- È possibile configurare i tag per un dispositivo in un ambiente in modo che vengano applicati automaticamente quando si registra un dispositivo.

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 gestire 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 gestire i tag per 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 gestire i tag per un nuovo dispositivo 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 di creazione del dispositivo, effettuate 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.

Quando un dispositivo viene creato, viene registrato nell'ambiente e vengono applicati i tag di creazione del dispositivo. Ciò avviene solo durante la registrazione di un nuovo dispositivo. Inoltre, il tag di `aws:thinclient:environment-id` sistema viene applicato con l'ID di ambiente utilizzato come valore.

Per gestire 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. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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](#)
- [Gestione delle identità e degli accessi per Amazon WorkSpaces Thin Client](#)
- [Resilienza in Amazon WorkSpaces Thin Client](#)
- [Analisi e gestione delle vulnerabilità in Amazon WorkSpaces Thin Client](#)

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. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

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. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

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

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](#)
- [Crittografia dei dati a riposo per Amazon WorkSpaces Thin Client](#)
- [Crittografia dei dati in transito](#)
- [Gestione delle chiavi](#)
- [Privacy del traffico di lavoro su Internet](#)

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 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 ambiente WorkSpaces Nome dell'ambiente Thin Client	Abilitato	Abilitato
Nome dispositivo WorkSpaces Nome del dispositivo Thin Client	Abilitato	Abilitato
Attività dell'utente WorkSpaces Attività degli utenti Thin Client	Abilitato	Abilitato
Impostazioni del dispositivo WorkSpaces Impostazioni del dispositivo Thin Client	Abilitato	Abilitato
Tag per la creazione del dispositivo WorkSpaces Tag di creazione dei dispositivi Thin Client Environment	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 AWS KMS

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

Amazon WorkSpaces Thin Client richiede la policy chiave per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia [GenerateDataKey](#) richieste a AWS KMS per crittografare i dati.
- Invia [Decrypt](#) richieste a AWS KMS per decrittografare i dati crittografati.

Puoi 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 si tenta di [ottenere dettagli ambientali](#) a cui 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.

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"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "thinclient.region.amazonaws.com",
          "kms:CallerAccount": "111122223333"
        }
      }
    },
    {
      "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt data",
      "Effect": "Allow",
      "Principal": {"Service": "thinclient.amazonaws.com"},

```

```

    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:SourceArn":
          "arn:aws:thinclient:region:111122223333:*",
        "kms:EncryptionContext:aws:thinclient:arn":
          "arn:aws:thinclient:region: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*"
    ],
    "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 `unkmsKeyArn`, 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.

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`, `GenerateDataKeyDecrypt`, 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 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": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-04-08T13:43:33Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:44:22Z",
  "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"
  }

```

GenerateDataKey

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

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

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-04-08T12:21:03Z",

```

```

        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:03:56Z",
  "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",
  "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
  "vpcEndpointId": "vpce-1234abcd567SAMPLE",
  "vpcEndpointAccountId": "thinclient.amazonaws.com",
  "eventCategory": "Management"
}

```

GenerateDataKey (by service)

Quando Amazon WorkSpaces Thin Client utilizza le informazioni GenerateDataKey salvate sul dispositivo, l'GenerateDataKeyoperazione viene utilizzata per crittografare i dati.

L'GenerateDataKeyoperazione è consentita nella dichiarazione politica chiave di KMS con Sid «Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt data».

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

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "thinclient.amazonaws.com"
  },
  "eventTime": "2024-04-08T13:03:56Z",
  "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",  
  "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",  
  "vpcEndpointId": "vpce-1234abcd567SAMPLE",  
  "vpcEndpointAccountId": "thinclient.amazonaws.com",  
  "eventCategory": "Management"  
}
```

Decrypt

Amazon WorkSpaces Thin Client utilizza l'Decryptoperazione per decrittografare i dati.

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

```
{  
  "eventVersion": "1.09",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",  
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",  
    "accountId": "111122223333",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",  
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",  
        "accountId": "111122223333",  
        "userName": "Admin"  
      },  
      "attributes": {  
        "creationDate": "2024-04-08T13:43:33Z",  
        "mfaAuthenticated": "false"  
      }  
    },  
    "invokedBy": "thinclient.amazonaws.com"  
  },  
  "eventTime": "2024-04-08T13:44:25Z",  
  "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
  }

```

Decrypt (by service)

Quando WorkSpaces Thin Client Device accede alle informazioni sull'ambiente o sul dispositivo, l'Decryptoperazione viene utilizzata per decrittografare i dati. L'Decryptoperazione è consentita nella dichiarazione politica chiave di KMS con Sid «Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt data».

L'evento di esempio seguente registra l'Decryptoperazione, autorizzata tramite un: Grant

```
{
```

```
"eventVersion": "1.09",
"userIdentity": {
  "type": "AWSService",
  "invokedBy": "thinclient.amazonaws.com"
},
"eventTime": "2024-04-08T13:44:25Z",
"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",
"sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
"vpcEndpointId": "vpce-1234abcd567SAMPLE",
"vpcEndpointAccountId": "thinclient.amazonaws.com",
"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, consulta [Best practice di sicurezza per AWS Key Management Service](#) nella [Guida per gli sviluppatori di AWS Key Management Service](#).

Crittografia dei dati 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 che vengono 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 WorkSpaces Applications](#) 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](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come funziona Amazon WorkSpaces Thin Client con IAM](#)
- [Esempi di policy basate sull'identità per Amazon Thin Client WorkSpaces](#)
- [AWS politiche gestite per Amazon WorkSpaces Thin Client](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Thin Client](#)

Destinatari

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

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon WorkSpaces Thin Client](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come funziona Amazon WorkSpaces Thin Client con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (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 autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

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

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

Account AWS utente root

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

Identità federata

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

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

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

Utenti e gruppi IAM

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

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

Ruoli IAM

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

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

Gestione dell'accesso tramite policy

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

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

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

Policy basate sull'identità

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

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

Policy basate sulle risorse

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

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

Altri tipi di policy

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

- **Limiti delle autorizzazioni:** imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Politiche di controllo del servizio (SCPs):** specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- **Politiche di controllo delle risorse (RCPs):** imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- **Policy di sessione:** policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

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

Come funziona Amazon WorkSpaces 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 sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	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 sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che

utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

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

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

Azioni politiche per WorkSpaces Thin Client

Supporta le operazioni di policy: si

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

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni WorkSpaces 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:

```
thinclient
```

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

```
"Action": [  
  "thinclient:action1",  
  "thinclient: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 relative alle policy: sì

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse WorkSpaces Thin Client e relativi ARNs, 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco 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](#)

ACLs in Thin Client WorkSpaces

Supporti ACLs: No

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

ABAC con Thin Client WorkSpaces

Supporta ABAC (tag nelle policy): sì

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

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

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

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con WorkSpaces Thin Client

Supporta le credenziali temporanee: sì

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

Autorizzazioni principali multiservizio per Thin Client WorkSpaces

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

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per Thin Client WorkSpaces

Supporta i ruoli di servizio: no

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

⚠ Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di WorkSpaces 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'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

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

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

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

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

Per dettagli sulle azioni e sui tipi di risorse definiti da WorkSpaces Thin Client, incluso il formato di ARNs per ogni 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 azioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

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

vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

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

Utilizzo della console 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, è opportuno concedere l'accesso solo alle azioni 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.

JSON

```
{
  "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 collegate 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:ListGroupsWithUser",
        "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.

JSON

```

{
    "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/*"]
  }
]
}
```

AWS politiche gestite per Amazon WorkSpaces Thin Client

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AmazonWorkSpacesThinClientReadOnlyAccess

È possibile allegare la policy `AmazonWorkSpacesThinClientReadOnlyAccess` alle identità IAM. Questa politica concede le autorizzazioni di accesso complete al servizio WorkSpaces Thin Client e alle sue dipendenze. Per ulteriori informazioni su questa politica gestita, consulta [AmazonWorkSpacesThinClientReadOnlyAccess](#) la guida AWS Managed Policy Reference.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `thinclient(WorkSpaces Thin Client)`: consente l'accesso in sola lettura a tutte le azioni di WorkSpaces Thin Client.
- `workspaces(WorkSpaces)` — Consente le autorizzazioni per descrivere le WorkSpaces directory e gli alias di connessione. Viene utilizzato per verificare che le WorkSpaces risorse siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.
- `workspaces-web(WorkSpaces Secure Browser)` — Consente le autorizzazioni per descrivere i WorkSpaces Secure Browser portali e le impostazioni utente. Viene utilizzato per verificare che le WorkSpaces Secure Browser risorse siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.
- `appstream(WorkSpaces Applicazioni)`: consente le autorizzazioni per descrivere gli stack WorkSpaces delle applicazioni. Viene utilizzato per verificare che le risorse delle WorkSpaces applicazioni siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
```

```

    "thinclient:GetDeviceDetails",
    "thinclient:GetEnvironment",
    "thinclient:GetSoftwareSet",
    "thinclient:ListDevices",
    "thinclient:ListDeviceSessions",
    "thinclient:ListEnvironments",
    "thinclient:ListSoftwareSets",
    "thinclient:ListTagsForResource"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowWorkSpacesAccess",
  "Effect": "Allow",
  "Action": [
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeWorkspaceDirectories"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowWorkSpacesSecureBrowserAccess",
  "Effect": "Allow",
  "Action": [
    "workspaces-web:GetPortal",
    "workspaces-web:GetUserSettings",
    "workspaces-web:ListPortals"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowAppStreamAccess",
  "Effect": "Allow",
  "Action": [
    "appstream:DescribeStacks"
  ],
  "Resource": "*"
}
]
}

```

AWS politica gestita: AmazonWorkSpacesThinClientFullAccess

È possibile allegare la policy `AmazonWorkSpacesThinClientFullAccess` alle identità IAM. Questa politica concede le autorizzazioni di accesso complete al servizio WorkSpaces Thin Client e alle sue dipendenze. Per ulteriori informazioni su questa politica gestita, consulta la Managed Policy [AmazonWorkSpacesThinClientFullAccess](#) Reference AWS Guide.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `thinclient(WorkSpaces Thin Client)`: consente l'accesso completo a tutte le azioni di WorkSpaces Thin Client.
- `workspaces(WorkSpaces)` — Consente le autorizzazioni per descrivere le WorkSpaces directory e gli alias di connessione. Viene utilizzato per verificare che le WorkSpaces risorse siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.
- `workspaces-web(WorkSpaces Secure Browser)` — Consente le autorizzazioni per descrivere i WorkSpaces Secure Browser portali e le impostazioni utente. Viene utilizzato per verificare che le WorkSpaces Secure Browser risorse siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.
- `appstream(WorkSpaces Applicazioni)`: consente le autorizzazioni per descrivere gli stack WorkSpaces delle applicazioni. Viene utilizzato per verificare che le risorse delle WorkSpaces applicazioni siano compatibili con WorkSpaces Thin Client. Viene anche utilizzato per mostrare queste risorse nella AWS console WorkSpaces Thin Client.
- `iam`— Consente a WorkSpaces Thin Client di creare un ruolo collegato al servizio nell'account. Questo ruolo consente a WorkSpaces Thin Client di pubblicare le metriche per tuo CloudWatch conto.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
```

```
"Action": [
  "thinclient:*"
],
"Resource": "*"
},
{
  "Sid": "AllowWorkSpacesAccess",
  "Effect": "Allow",
  "Action": [
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeWorkspaceDirectories"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowWorkSpacesSecureBrowserAccess",
  "Effect": "Allow",
  "Action": [
    "workspaces-web:GetPortal",
    "workspaces-web:GetUserSettings",
    "workspaces-web:ListPortals"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowAppStreamAccess",
  "Effect": "Allow",
  "Action": [
    "appstream:DescribeStacks"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowCreateServiceLinkedRole",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "monitoring.thinclient.amazonaws.com"
    }
  }
}
```

```

    }
  ]
}
```

WorkSpaces Thin Client aggiorna le policy AWS gestite

Modifica	Descrizione	Data
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy— Politica rimossa	WorkSpaces Thin Client ha rimosso la AmazonWorkSpacesThinClientMonitoringServiceRolePolicy sezione.	12 novembre 2025
AmazonWorkSpacesThinClientFullAccess — Politica aggiornata AmazonWorkSpacesThinClientMonitoringServiceRolePolicy: nuova policy	WorkSpaces Thin Client ha aggiornato la policy per includere i ruoli collegati al servizio.	26 agosto 2025
AmazonWorkSpacesThinClientReadOnlyAccess — Politica aggiornata	WorkSpaces Thin Client ha aggiornato la policy per includere autorizzazioni di lettura limitate per i dettagli del dispositivo e gli alias di WorkSpaces connessione.	9 gennaio 2025
AmazonWorkSpacesThinClientFullAccess — Politica aggiornata	WorkSpaces Thin Client ha aggiornato la politica per includere autorizzazioni di lettura limitate per gli alias di WorkSpaces connessione.	9 gennaio 2025
AmazonWorkSpacesThinClientReadOnlyAccess — Politica aggiornata	WorkSpaces Thin Client ha aggiornato la policy per includere autorizzazioni di lettura limitate per WorkSpace	9 agosto 2024

Modifica	Descrizione	Data
	s Applicazioni, WorkSpaces Web e WorkSpaces.	
AmazonWorkSpacesThinClientFullAccess : nuova policy	Fornisce accesso completo ad Amazon WorkSpaces Thin Client e accesso limitato ai servizi correlati richiesti.	9 agosto 2024
AmazonWorkSpacesThinClientReadOnlyAccess : nuova policy	Fornisce accesso in sola lettura ad Amazon WorkSpace s Thin Client e alle sue dipendenze.	19 luglio 2024
WorkSpaces Thin Client ha iniziato a tracciare le modifiche	WorkSpaces Thin Client ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	19 luglio 2024

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](#)
- [Desidero visualizzare le mie chiavi di accesso](#)
- [Sono un amministratore e voglio consentire ad altri di accedere a WorkSpaces Thin Client](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Thin Client WorkSpaces](#)

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

Se ti Console di gestione AWS 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 `thinclient:ListDevices` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
thinclient: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'`thinclient: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 concedere l'autorizzazione alle persone o alle applicazioni che devono accedervi. Se si utilizza AWS IAM Identity Center per gestire persone e applicazioni, si assegnano set di autorizzazioni a utenti o gruppi per definire il loro livello di accesso. I set di autorizzazioni creano e assegnano automaticamente le policy IAM ai ruoli IAM associati alla persona o all'applicazione. Per ulteriori informazioni, consulta [Set di autorizzazioni](#) nella Guida per l'AWS IAM Identity Center utente.

Se non utilizzi IAM Identity Center, devi creare entità IAM (utenti o ruoli) per le persone o le applicazioni che necessitano di accesso. È quindi necessario allegare una policy all'entità che conceda loro le autorizzazioni corrette in WorkSpaces Thin Client. Dopo aver concesso le autorizzazioni, fornisci le credenziali all'utente o allo sviluppatore dell'applicazione. Utilizzeranno tali credenziali per accedere. AWS Per ulteriori informazioni sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta [IAM Identities](#) and [Policies and permissions in IAM nella IAM User Guide](#).

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 Thin Client WorkSpaces

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

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se WorkSpaces Thin Client supporta queste funzionalità, consulta. [Come 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 IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

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 WorkSpaces Applications e WorkSpaces Web. Consulta i seguenti link per ulteriori informazioni sulla gestione degli aggiornamenti per ciascuno di questi servizi:

- [Gestione degli aggiornamenti nelle WorkSpaces applicazioni Amazon](#)
- [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 CloudTrail acquisisce 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](#).

Argomenti

- [Registrazione delle chiamate API Amazon WorkSpaces Thin Client utilizzando AWS CloudTrail](#)
- [Monitora il tuo WorkSpaces Thin Client utilizzando le CloudWatch metriche](#)

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 un Servizio AWS. 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. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a WorkSpaces Thin Client, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Tutte le azioni di Amazon WorkSpaces Thin Client vengono registrate CloudTrail e documentate nell'[Amazon WorkSpaces Thin Client API Reference](#). Ad esempio, le chiamate a DeleteDevice e CreateEnvironment le GetSoftwareSet azioni generano voci nei file di CloudTrail registro.

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

- Se la richiesta è stata effettuata con le credenziali utente root o utente.

- Se la richiesta è stata effettuata per conto di un utente del Centro identità 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 Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per

ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail](#)

WorkSpaces Eventi relativi ai dati Thin Client in CloudTrail

[Gli eventi relativi ai dati](#) forniscono informazioni sulle operazioni eseguite sulle risorse su o all'interno di una risorsa (ad esempio, la registrazione di un dispositivo da parte di un utente finale). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione [AWS CloudTrail Prezzi](#).

È possibile registrare gli eventi relativi ai dati per i tipi di risorse WorkSpaces Thin Client utilizzando la CloudTrail AWS CLI console o le operazioni CloudTrail API. Per ulteriori informazioni su come registrare gli eventi relativi ai dati, consulta [Registrazione di eventi relativi ai dati con Console di gestione AWS](#) e [Registrazione di eventi di dati con AWS Command Line Interface](#) nella Guida per l'utente AWS CloudTrail .

La tabella seguente elenca i tipi di risorse WorkSpaces Thin Client per i quali è possibile registrare gli eventi relativi ai dati. La colonna Data event type (console) mostra il valore da scegliere dall'elenco Data event type (console) sulla CloudTrail console. La colonna del valore resources.type mostra il resources . type valore da specificare durante la configurazione dei selettori di eventi avanzati utilizzando o. AWS CLI CloudTrail APIs La CloudTrail colonna Dati APIs registrati mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore resources.type	Dati registrati APIs su CloudTrail
ThinClientDevice	AWS::WorkSpacesThinClient::Device	<ul style="list-style-type: none"> RegisterDevice UpdateDeviceDetails

È possibile configurare selettori di eventi avanzati per filtrare i campi `eventName`, `readOnly` e `resources`. ARN per registrare solo gli eventi importanti per l'utente. Per ulteriori informazioni su questi campi, consulta [AdvancedFieldSelector](#) in Riferimento API AWS CloudTrail .

WorkSpaces Eventi di gestione Thin Client in CloudTrail

[Gli eventi](#) di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon WorkSpaces Thin Client registra tutte le operazioni del piano di controllo di WorkSpaces Thin Client come eventi di gestione. Per un elenco delle operazioni del piano di controllo di Amazon WorkSpaces Thin Client a cui WorkSpaces Thin Client accede CloudTrail, consulta [Amazon WorkSpaces Thin Client API Reference](#).

WorkSpaces Esempi di eventi Thin Client

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra un CloudTrail evento che dimostra l'`RegisterDevice` operazione.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "111111111111",
    "userName": "DSN: G1X11X1111111111XX"
  },
  "eventTime": "2024-06-19T17:13:44Z",
  "eventSource": "thinclient.amazonaws.com",
  "eventName": "RegisterDevice",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "dsn": "G1X11X1111111111XX",
    "activationCode": "xxx1xxx1",
    "model": "AFTGAZL"
  }
}
```

```

    },
    "responseElements": null,
    "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
    "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "eventCategory": "Data"
  }
}

```

L'esempio seguente mostra un CloudTrail evento che dimostra l'UpdateDeviceDetails operazione.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "111111111111",
    "userName": "DSN: G1X11X11111111XX"
  },
  "eventTime": "2024-10-21T17:46:27Z",
  "eventSource": "thinclient.amazonaws.com",
  "eventName": "UpdateDeviceDetails",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
  "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
  "readOnly": false,
  "resources": [
    {
      "type": "AWS::ThinClient::Device",
      "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
    }
  ]
}

```

```
],
"eventType": "AwsServiceEvent",
"managementEvent": false,
"recipientAccountId": "111111111111",
"serviceEventDetails": {
  "settings": {
    "network": {
      "ethernet": {
        "addresses": [
          {
            "gateway": "gateway",
            "localIp": "localIp",
            "type": "IPV4"
          }
        ],
        "connectionStatus": "NOT_CONNECTED"
      },
      "networkInterfaceInUse": "ETHERNET",
      "wifi": {
        "addresses": [
          {
            "gateway": "gateway",
            "localIp": "localIp",
            "type": "IPV4"
          }
        ],
        "connectionStatus": "NOT_CONNECTED"
      }
    },
    "peripherals": {
      "bluetooth": {
        "enabledStatus": "ENABLED"
      },
      "keyboards": [
        {
          "name": "name",
          "type": "USB"
        }
      ],
      "mice": [
        {
          "name": "name",
          "type": "BLUETOOTH"
        }
      ]
    }
  }
}
```

```
    ],
    "sound": {
      "microphones": [
        {
          "name": "name",
          "selectionStatus": "SELECTED",
          "type": "BUILT_IN"
        }
      ],
      "speakers": [
        {
          "name": "name",
          "selectionStatus": "SELECTED",
          "type": "BUILT_IN"
        }
      ]
    },
    "webcams": [
      {
        "name": "name",
        "selectionStatus": "SELECTED",
        "type": "USB"
      }
    ],
    "powerAndSleep": {
      "sleepAfter": "FIFTEEN_MINUTES"
    },
    "updatedAt": "2024-10-21T17:46:27.624Z"
  },
  "eventCategory": "Data"
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

Monitora il tuo WorkSpaces Thin Client utilizzando le CloudWatch metriche

WorkSpaces I dispositivi Thin Client e Amazon CloudWatch sono integrati, quindi puoi raccogliere e analizzare i parametri prestazionali emessi dai tuoi dispositivi WorkSpaces Thin Client. Puoi

monitorare queste metriche utilizzando la CloudWatch console, l'interfaccia a riga di CloudWatch comando o utilizzando l'API a livello di codice. CloudWatch consente inoltre di impostare allarmi quando si raggiunge una soglia specificata per una metrica.

Per ulteriori informazioni sull'uso CloudWatch e sugli allarmi, consulta la [Amazon CloudWatch User Guide](#).

Prerequisiti

Non ci sono prerequisiti. Una volta registrato in un ambiente, un dispositivo WorkSpaces Thin Client inizierà a emettere i parametri del dispositivo.

Indice

- [WorkSpaces Metriche Thin Client](#)

WorkSpaces Metriche Thin Client

Lo spazio dei nomi `AWS/WorkSpacesThinClient` include le metriche descritte di seguito.

Metrica	Descrizione	Dimensioni	Statistiche	Units
DeviceSession	Il numero di ThinClient dispositivi che sono connessi a una sessione del dispositivo o che non sono in sessione.	Tipo di desktop	Media, minimo, massimo, somma, conteggio dei campioni	Conteggio
Connected Devices	Il numero di ThinClient dispositivi attualmente online.	N/A	Media, minimo, massimo, somma, numero di campioni	Conteggio
SoftwareSetVersion	Il numero di ThinClient	softwareSetVersion	Media, minimo, massimo,	Conteggio

Metrica	Descrizione	Dimensioni	Statistiche	Units
	dispositivi che eseguono una determinata versione del Software Set.		somma, numero di campioni	
NetworkConnectionEthernet	Il numero di ThinClient dispositivi attualmente connessi tramite Ethernet.	N/A	Media, minimo, massimo, somma, numero di campioni	Conteggio
NetworkConnectionWifi	Il numero di ThinClient dispositivi attualmente connessi tramite WiFi.	N/A	Media, minimo, massimo, somma, numero di campioni	Conteggio

Dalla dimensione alle metriche di WorkSpaces Thin Client

Dimensione	Descrizione
Tipo di desktop	Filtra i dati metrici in base al tipo di desktop attualmente in sessione sul dispositivo. Il dispositivo è in sessione se un utente è connesso a un desktop e se il dispositivo non è in modalità di sospensione. Se il dispositivo è in sessione, il valore della dimensione sarà il tipo di desktop utilizzato, ad esempio WorkSpaces, WorkSpacesSecureBrowser o. AppStream Se il dispositivo non è in sessione, il valore della dimensione sarà. NotInSession

Dimensione	Descrizione
softwareSetVersion	Filtra i dati metrici in base alla versione del Software Set installata sul dispositivo. La forma della dimensione in X.Y.Z, ad esempio 1.4.2.

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 CloudFormation e configura tali risorse per te.

Quando lo utilizzi 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 CloudFormation modelli

Per fornire e configurare le risorse per WorkSpaces Thin Client e i servizi correlati, è necessario conoscere [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. CloudFormation Se non conosci i formati JSON o YAML, puoi usare CloudFormation Designer per iniziare a usare i modelli. CloudFormation Per ulteriori informazioni, consulta [Che cos'è CloudFormation Designer?](#) nella Guida per l'utente di AWS CloudFormation .

WorkSpaces Thin Client supporta la creazione di ambienti in. CloudFormation Per 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 CloudFormation

Per ulteriori informazioni CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guida per l'utente](#)
- [Documentazione di riferimento dell'API 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. 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
AWS politica gestita: AmazonWorkSpacesThinClientMonitoringServiceRolePolicy	AmazonWorkSpacesThinClientMonitoringServiceRolePolicy Sezione rimossa di Amazon WorkSpaces Thin Client.	12 novembre 2025
AWS politica gestita: AmazonWorkSpacesThinClientMonitoringServiceRolePolicy AWS politica gestita: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client ha aggiunto una policy AmazonWorkSpacesThinClientMonitoringServiceRolePolicy gestita. Amazon WorkSpaces Thin Client ha aggiunto la versione 3 delle policy AmazonWorkSpacesThinClientFullAccess gestite.	26 agosto 2025
AWS politica gestita: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client ha aggiunto la versione 2 della policy AmazonWorkSpacesThinClientFullAccess gestita.	9 gennaio 2025
AWS politica gestita: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client ha aggiunto la versione 3 delle policy AmazonWorkSpacesThinClientReadOnlyAccess gestite.	9 gennaio 2025

Modifica	Descrizione	Data
	inClientReadOnlyAccess gestite.	
Registrazione delle chiamate API Amazon WorkSpaces Thin Client utilizzando AWS CloudTrail Impostazioni del dispositivo Crittografia dei dati a riposo per Amazon WorkSpaces Thin Client	<p>Aggiunta una nuova sezione per gli eventi relativi ai dati.</p> <p>Aggiunta una nuova sezione per le impostazioni del dispositivo.</p> <p>Sono state aggiornate le informazioni KMS nella sezione relativa alla crittografia dei dati inattivi.</p>	28 ottobre 2024
Continuità aziendale	È stata aggiunta una nuova sezione per la continuità aziendale e il disaster recovery.	6 settembre 2024
AWS politica gestita: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client ha aggiunto una policy AmazonWorkSpacesThinClientFullAccess gestita.	9 agosto 2024
AWS politica gestita: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client ha aggiunto la versione 2 delle policy AmazonWorkSpacesThinClientReadOnlyAccess gestite.	9 agosto 2024
Configurazione di WorkSpaces Personal per WorkSpaces Thin Client	Aggiornato il per il nuovo WorkSpaces Personal.	7 agosto 2024

Modifica	Descrizione	Data
Configurazione dei WorkSpaces pool per WorkSpaces Thin Client	Aggiunta una nuova sezione per i nuovi WorkSpaces pool.	7 agosto 2024
AWS politica gestita: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client ha aggiunto una policy AmazonWorkSpacesThinClientReadOnlyAccess gestita.	19 luglio 2024
AWS politiche gestite per Amazon WorkSpaces Thin Client	Amazon WorkSpaces Thin Client ha iniziato a tracciare le modifiche.	19 luglio 2024
Configurazione WorkSpaces per Amazon WorkSpaces Thin Client	Aggiornato l'elenco dei sistemi operativi.	12 febbraio 2024
Configurazione delle WorkSpaces applicazioni per Amazon WorkSpaces Thin Client	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.