# Best practice per la distribuzione di Amazon 2.0 AppStream

# Best practice per la distribuzione di Amazon 2.0 AppStream :

# Table of Contents

# Best practice per la distribuzione di Amazon 2.0 AppStream

Data di pubblicazione: 19 gennaio 2022 (Revisioni del documento)

## Sintesi

Questo white paper delinea una serie di best practice per l'implementazione di Amazon 2.0. AppStream  Il paper tratta la progettazione di Amazon Virtual Private Cloud (VPC), la creazione e la gestione di immagini, la personalizzazione della flotta e le strategie di scalabilità automatica della flotta. Include metodi di connessione utente, autenticazione e integrazione con Microsoft Active Directory. Questo paper include anche raccomandazioni per la progettazione della sicurezza, del monitoraggio e dell'ottimizzazione dei costi AppStream 2.0.

Questo white paper è stato scritto per consentire un accesso rapido alle informazioni pertinenti. È destinato agli ingegneri di rete, agli specialisti della distribuzione delle applicazioni, ai tecnici degli elenchi o ai tecnici della sicurezza.

## Introduzione

Amazon AppStream 2.0 è un servizio di streaming di applicazioni completamente gestito che fornisce agli utenti l'accesso immediato alle loro applicazioni desktop da qualsiasi luogo. AppStream 2.0 gestisce le AWS risorse necessarie per ospitare ed eseguire le applicazioni. È scalabile automaticamente e fornisce l'accesso agli utenti su richiesta. AppStream 2.0 fornisce agli utenti finali l'accesso alle applicazioni di cui hanno bisogno sul dispositivo di loro scelta, con un'esperienza utente reattiva, indistinguibile dalle applicazioni installate nativamente.

Le sezioni seguenti forniscono dettagli su Amazon AppStream 2.0, spiegano come funziona il servizio, descrivono ciò di cui hai bisogno per avviare il servizio e indicano quali opzioni e funzionalità sono disponibili per l'uso. Quando si implementa la AppStream versione 2.0 per gli utenti finali, è importante implementare le migliori pratiche per fornire un'esperienza utente eccezionale. Inoltre, le aziende di tutte le dimensioni traggono vantaggio dall'ottimizzazione dei costi che riduce i costi operativi mensili.

# Concetti chiave

Per ottenere il massimo dalla AppStream versione 2.0, acquisisci familiarità con i seguenti concetti:

- Immagine: un'immagine è un modello di istanza preconfigurato. Un'immagine contiene applicazioni che è possibile trasmettere in streaming agli utenti e impostazioni predefinite di Windows e delle applicazioni per consentire agli utenti di iniziare rapidamente a utilizzare le proprie applicazioni. AWSfornisce immagini di base che è possibile utilizzare per creare immagini che includono applicazioni personalizzate. Dopo aver creato un'immagine, non è possibile modificarla. Per aggiungere altre applicazioni, aggiornare le applicazioni esistenti o modificare le impostazioni dell'immagine, è necessario creare una nuova immagine. Puoi copiare le tue immagini su altri Regioni AWSo condividerle con altri Account AWS nella stessa regione.
- Generatore di immagini: un generatore di immagini è una macchina virtuale che si utilizza per creare un'immagine. È possibile avviare e connettersi a un generatore di immagini utilizzando la AppStream console 2.0. Una volta connesso a un Image Builder, puoi installare, aggiungere e testare le applicazioni, quindi utilizzare l'Image Builder per creare un'immagine. Puoi avviare nuovi Image Builder utilizzando le immagini private di tua proprietà.
- Flotta: una flotta è composta da istanze (note anche come istanze di streaming) che eseguono l'immagine specificata. Puoi impostare il numero desiderato di istanze di streaming per il tuo parco istanze e configurare politiche per scalare automaticamente il parco istanze in base alla domanda. Tieni presente che ogni utente richiede un'istanza.
- Stack: uno stack è costituito da una flotta associata, da politiche di accesso degli utenti e da configurazioni di archiviazione. Puoi configurare uno stack per avviare lo streaming delle applicazioni per gli utenti.
- Istanza di streaming: un'istanza di streaming (nota anche come istanza fleet) è un'istanza Amazon Elastic Compute Cloud (Amazon EC2) resa disponibile a un singolo utente per lo streaming di applicazioni. Al termine della sessione dell'utente, l'istanza viene terminata da Amazon EC2.

# Progettazione VPC

## Linee guida di progettazione

Implementa la AppStream versione 2.0 in un VPC dedicato. Quando si progetta il VPC AppStream 2.0, dimensioni adatte alla crescita prevista. Riserva la capacità degli indirizzi IP per nuovi casi d'uso e zone di disponibilità (AZ) aggiuntive che possono essere aggiunte in un secondo momento. Un punto fondamentale di progettazione della AppStream versione 2.0 è che solo un utente può utilizzare un'istanza AppStream 2.0. Quando si alloca lo spazio IP, si consideri un utente come un indirizzo IP per istanza AppStream 2.0. Con la AppStream versione 2.0, è possibile che un utente utilizzi più istanze AppStream 2.0. Pertanto, la pianificazione dello spazio IP deve tenere conto anche dei casi d'uso che richiedono istanze AppStream 2.0 aggiuntive.

Sebbene la dimensione massima di un VPC Classless Inter-Domain Routing (CIDR) sia /16, consiglia di non sovraallocare gli indirizzi IP privati. AWS È possibile estendere le dimensioni del VPC tramite CIDR aggiuntivi, ma esiste un limite; pertanto, è necessario allocare ciò che è necessario sin dall'inizio.

Se la distribuzione AppStream 2.0 viene aggiunta a un dominio Active Directory, le opzioni DHCP impostate per il VPC devono avere il dominio DNS configurato. Il server dei nomi di dominio deve specificare gli indirizzi IP DNS che sono autorevoli per il dominio Active Directory oppure il DNS deve inoltrare le richieste DNS alle istanze DNS autorevoli per il dominio Active Directory. Inoltre, il VPC deve avere `enableDnsHostnames` e `EnableDnsSupport` configurato.

## Zone di disponibilità

Una zona di disponibilità (AZ) è uno o più data center discreti con alimentazione, rete e connettività ridondanti in un. Regione AWS Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Amazon AppStream 2.0 richiede solo una sottorete per il lancio di una flotta. La migliore pratica consiste nel configurare un minimo di due zone di disponibilità, una sottorete per zona di disponibilità unica. Per ottimizzare la scalabilità automatica della flotta, utilizza più di due zone di disponibilità. La scalabilità orizzontale ha l'ulteriore vantaggio di aggiungere spazio IP nelle sottoreti per favorire la crescita, come illustrato nella seguente sezione sul dimensionamento delle sottoreti di questo documento. La Console di gestione AWS consente di specificare solo due sottoreti durante la

creazione di una flotta. Utilizza AWS Command Line Interface(AWSCLI) o per consentire più AWS CloudFormation di due ID di sottorete.

## Dimensionamento sottorete

Dedica le sottoreti alle flotte AppStream 2.0 per consentire flessibilità nelle politiche di routing e nella lista di controllo degli accessi alla rete. Gli stack avranno probabilmente requisiti di risorse separati. Ad esempio, gli stack AppStream 2.0 possono avere requisiti di isolamento che lasciano il posto a set di regole separati. Quando più flotte Amazon AppStream 2.0 utilizzano le stesse sottoreti, assicurati che la somma della capacità massima di tutte le flotte non superi il numero totale di indirizzi IP disponibili.

Se la capacità massima per tutte le flotte nella stessa sottorete può, o ha superato, il numero totale di indirizzi IP disponibili, migra le flotte verso sottoreti dedicate. In questo modo si evita che gli eventi di scalabilità automatica esauriscano lo spazio IP allocato. Se la capacità totale di una flotta supera lo spazio IP allocato delle sottoreti assegnate, utilizza l'API o la «flotta di aggiornamento» della AWS CLI per assegnare più sottoreti. Per ulteriori informazioni, consulta le quote di Amazon VPC e come aumentarle.

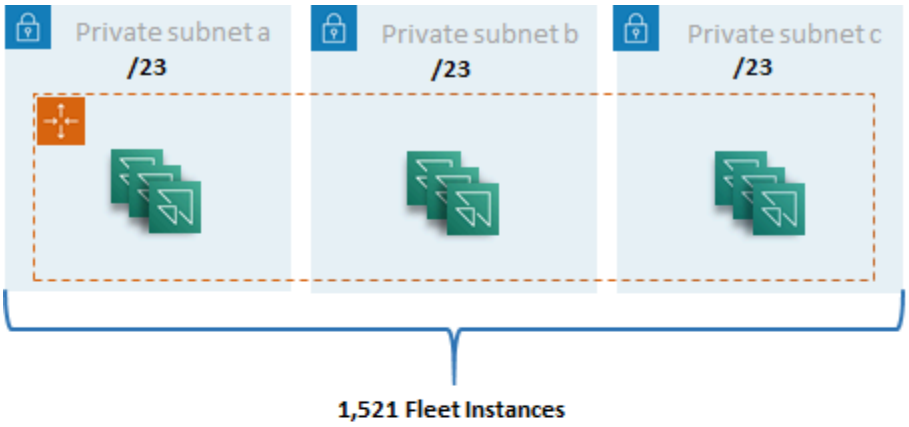
È consigliabile ridimensionare il numero di sottoreti, dimensionarle di conseguenza e riservare la capacità di crescita del VPC. Inoltre, assicurati che il numero massimo di unità AppStream 2.0 non superi lo spazio IP totale allocato dalle sottoreti. Per ogni sottorete in ingressoAWS, nel calcolo della quantità totale di spazio IP vengono riservati cinque indirizzi IP. L'utilizzo di più di due sottoreti e la scalabilità orizzontale offrono diversi vantaggi, ad esempio:

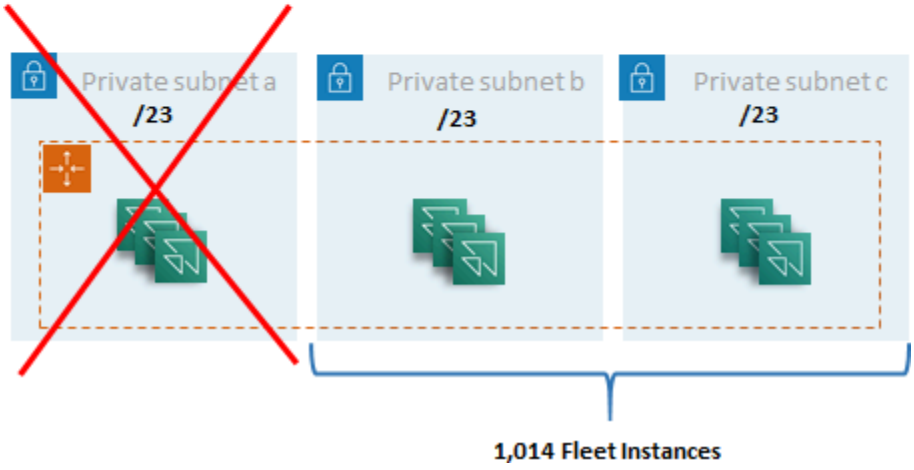
- Maggiore resilienza in caso di guasto nella zona di disponibilità
- Maggiore produttività grazie alla scalabilità automatica delle istanze del parco istanze
- Utilizzo più efficiente degli indirizzi IP privati, evitando la masterizzazione degli IP

Nel dimensionare le sottoreti per Amazon AppStream 2.0, considera il numero totale di sottoreti e il picco di concorrenza previsto durante i picchi di utilizzo. Questo può essere monitorato utilizzando (`InUseCapacity`) plus la capacità riservata () per una flotta. `AvailableCapacity` In Amazon AppStream 2.0, la somma delle istanze consumate e delle available-to-be-consumed AppStream 2,0 istanze del parco istanze è `ActualCapacity` etichettata. Per dimensionare correttamente lo spazio IP totale, prevedi quello necessario `ActualCapacity` e dividilo per il numero di sottoreti, meno una sottorete per la resilienza, assegnate alla flotta.

Ad esempio, se il numero massimo previsto di istanze del parco istanze nei momenti di picco è 1000 e il requisito aziendale è la resilienza in caso di guasto di una zona di disponibilità, 3 sottoreti x/23 soddisfano i requisiti tecnici e aziendali.

- /23 = 512 host — 5 riservate = 507 istanze del parco istanze per sottorete
- 3 sottoreti — 1 sottorete = 2 sottoreti
- 2 sottoreti x 507 istanze di flotta per sottorete = 1.014 istanze di flotta al massimo




Esempio di dimensionamento di una sottorete

Anche se 2 sottoreti x/22 soddisferebbero anche la resilienza, considera quanto segue:

- Invece di 1.536 indirizzi IP riservati, utilizzando due AZ si ottengono 2.048 indirizzi IP riservati, sprecando indirizzi IP che potrebbero essere utilizzati per altre funzioni.
- Se una AZ diventa inaccessibile, la capacità di scalare orizzontalmente le istanze del parco istanze è limitata dalla velocità effettiva di una AZ. Ciò può prolungare la durata di. `PendingCapacity`

## Routing della sottorete

È consigliabile creare sottoreti private per istanze AppStream 2.0, instradandole verso la rete Internet pubblica tramite un VPC centralizzato per il traffico in uscita. Il traffico in entrata per lo streaming della sessione AppStream 2.0 viene gestito tramite il servizio Amazon AppStream 2.0 tramite Streaming Gateways: a tale scopo non è necessario configurare sottoreti pubbliche.

## Connettività intraregionale

Per le istanze della flotta AppStream 2.0 unite a un dominio Active Directory, configura i controller di dominio Active Directory in un VPC di Shared Services in ciascuno di essi. Regione AWS Le fonti per Active Directory possono essere controller di dominio basati su Amazon EC2 o AWSMicrosoft Managed AD. Il routing tra i servizi condivisi e i VPC AppStream 2.0 può avvenire tramite una connessione peering VPC o un gateway di transito. Sebbene i gateway di transito risolvano la complessità del routing su larga scala, esistono diversi motivi per cui il peering VPC è preferibile nella maggior parte delle impostazioni:

- Il peering VPC è una connessione diretta tra i due VPC (nessun hop aggiuntivo).
- Non è prevista alcuna tariffa oraria, ma solo la velocità di trasferimento dati standard tra le zone di disponibilità.
- Non ci sono limiti alla larghezza di banda.
- Support per l'accesso ai gruppi di sicurezza tra VPC.

Ciò è particolarmente vero se le istanze AppStream 2.0 si connettono all'infrastruttura applicativa e/o ai file server con set di dati di grandi dimensioni in un VPC di servizio condiviso. Ottimizzando il percorso verso queste risorse a cui si accede comunemente, la connessione peering VPC è preferita, anche nei progetti in cui tutti gli altri VPC e il routing Internet vengono eseguiti tramite gateway di transito.

## Traffico Internet in uscita

Sebbene il routing diretto verso i servizi condivisi sia per lo più ottimizzato tramite una connessione peering, il traffico in uscita per la AppStream versione 2.0 può essere progettato creando un unico punto di uscita Internet da più VPC utilizzando Transit Gateway. AWS In una progettazione multi-VPC, è prassi standard disporre di un VPC dedicato che controlli tutto il traffico Internet in uscita. Con questa configurazione, i Transit Gateway offrono maggiore flessibilità e controllo del routing sulle tabelle di routing standard collegate alle sottoreti. Questo design supporta anche il routing transitivo

senza complessità aggiuntiva ed elimina la necessità di gateway NAT (Network Address Translation) ridondanti o istanze NAT in ogni VPC.

Una volta centralizzato tutto il traffico Internet in uscita in un unico VPC, i gateway NAT o le istanze NAT sono una scelta di progettazione comune. Per determinare qual è la soluzione migliore per la tua organizzazione, consulta la guida amministrativa per confrontare i gateway NAT e le istanze NAT. AWS Network Firewall può estendere la protezione oltre i livelli di controllo dei gruppi di sicurezza e degli accessi alla rete, proteggendo a livello di route e offrendo regole stateless e stateful dai livelli da 3 a 7 nel modello OSI. Per ulteriori informazioni, consulta Modelli di distribuzione per AWS Network Firewall. Se la tua organizzazione ha scelto un prodotto di terze parti che offre funzionalità avanzate come il filtro degli URL, distribuisci il servizio nel tuo VPC Internet in uscita. Questo può sostituire i gateway NAT o le istanze NAT. Segui le linee guida fornite dal fornitore terzo.

## Locale

Quando è richiesta la connettività alle risorse locali, in particolare per le istanze AppStream 2.0 unite ad Active Directory, stabilisci una connessione altamente resiliente tramite. AWS Direct Connect

# Endpoint VPC

## Endpoint VPC Amazon S3

Molte distribuzioni di Amazon AppStream 2.0 richiedono la persistenza dello stato utente tramite le cartelle home e le impostazioni delle applicazioni. Abilita la comunicazione privata verso queste postazioni Amazon Simple Storage Service (Amazon S3), in modo da evitare l'uso della rete Internet pubblica. È possibile ottenere ciò tramite un gateway endpoint VPC. Un gateway endpoint VPC è preferito a quello per Amazon AWS PrivateLinkS3 perché:

- È ottimizzato in termini di costi per i requisiti di accesso alla AppStream rete 2.0
- L'accesso al bucket Amazon S3 non è richiesto da risorse locali
- È possibile utilizzare un documento di policy personalizzato per limitare l'accesso solo dalle istanze 2.0 AppStream

Una volta creato il gateway endpoint VPC, è consigliabile proteggere la connessione privatizzata creando una policy personalizzata. La policy personalizzata inizia con l'Amazon Resource Name (ARN) del ruolo Identity and Access Management del servizio AppStream 2.0. Specificate in modo esplicito le azioni S3 necessarie per la persistenza dello stato utente.

> **Note**
>
> L'esempio seguente nella `Resources` sezione specifica prima il percorso della cartella principale dello stato e poi il percorso delle impostazioni delle applicazioni.

Example

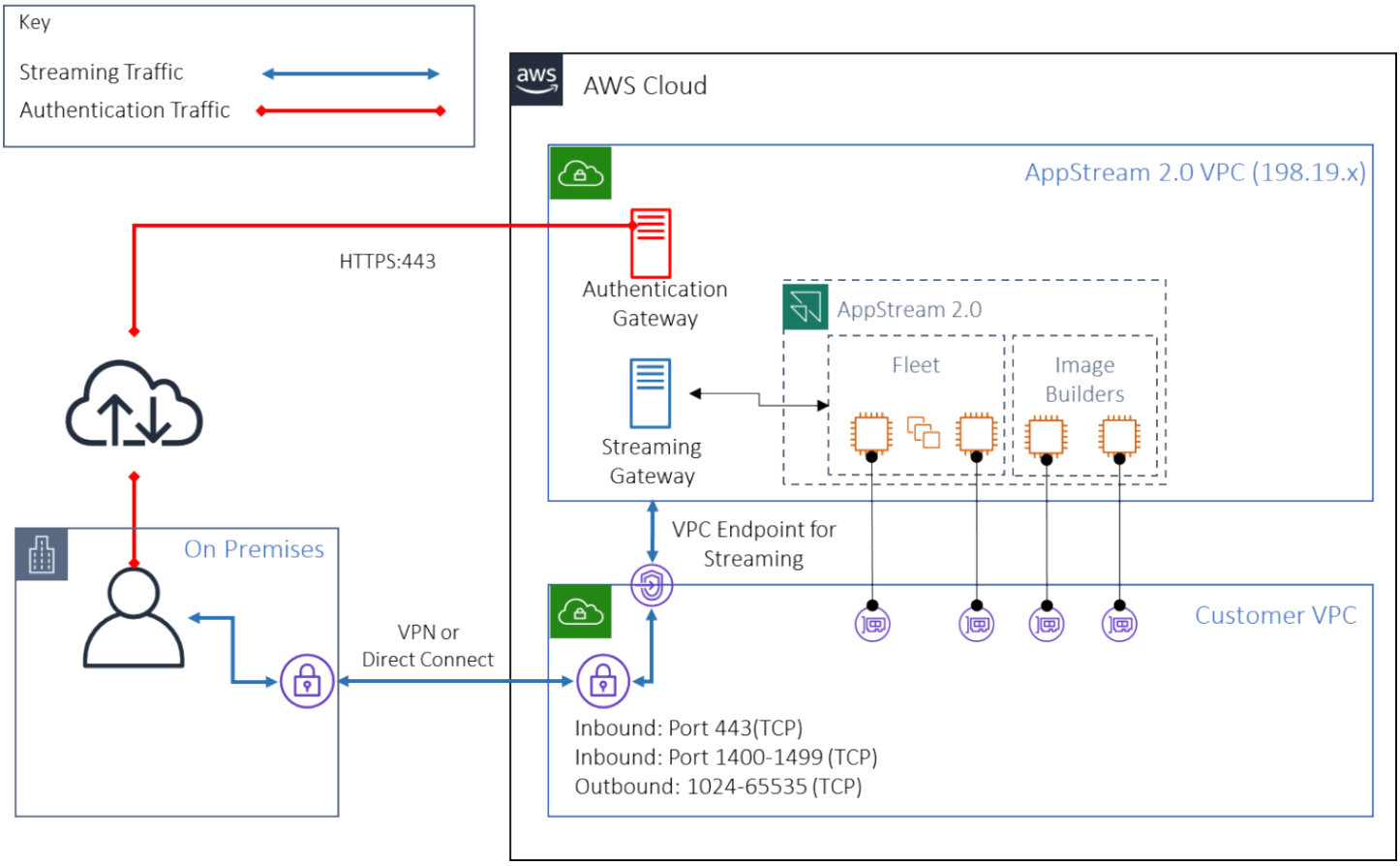
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-AppStream-to-access-home-folder-and-
application-settings",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:sts::account-id-without-hyphens:assumed-
role/AmazonAppStreamServiceAccess/AppStream2.0"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*"
      ]
    }
  ]
}
```

## Endpoint VPC con interfaccia API Amazon AppStream 2.0

Negli scenari di progettazione in cui i comandi API e CLI di Amazon AppStream 2.0 hanno origine nel tuo VPC, privatizza queste chiamate programmatiche tramite un endpoint VPC di interfaccia.

# Endpoint VPC con interfaccia di streaming Amazon AppStream 2.0

Sebbene sia possibile [indirizzare il traffico di streaming di Amazon AppStream 2.0 attraverso un endpoint VPC di interfaccia](), usa questa configurazione con cautela. Il comportamento di streaming predefinito attraverso la rete Internet pubblica è il metodo di distribuzione più efficiente e performante per il traffico di streaming di Amazon AppStream 2.0.




Endpoint VPC con interfaccia di streaming Amazon AppStream 2.0

Come illustrato nella figura precedente, l'Internet pubblico è il percorso più efficiente verso Amazon AppStream 2.0 Streaming Gateways. Il routing tramite VPC e rete gestiti dal cliente aggiunge complessità e latenza. Inoltre, aggiunge i costi di trasferimento dei dati. AWS Direct Connect

> **Note**
>
> L'endpoint VPC supporta solo lo streaming e l'autenticazione deve comunque avvenire sulla rete Internet pubblica. L'accesso preliminare come SAML Single Sign-On (SSO) Identity Provider (IdP) rimane un requisito accessibile solo tramite la rete Internet pubblica.

# Creazione e gestione delle immagini

Quando si avvia una flotta o un generatore di immagini nella AppStream versione 2.0, è necessario selezionare una delle immagini di base AppStream 2.0. Gli amministratori possono quindi basarsi sull'immagine di base per aggiungere le proprie applicazioni e impostazioni di configurazione.

Quando si crea un'immagine, ci sono considerazioni fondamentali per garantire che le applicazioni funzionino correttamente e in modo sicuro. Inoltre, vi sono considerazioni di progettazione relative al modo in cui verrà mantenuta l'immagine.

## Creazione di un' AppStream immagine 2.0

Quando si crea una nuova immagine, è importante considerare quanto segue:

- Sistema operativo
- Applicazioni
- Profilo utente
- Sicurezza
- Prestazioni
- Versione dell'agente
- CLI di Image Assistant

## Creazione di un' AppStream immagine 2.0

Nel novembre 2021, AppStream 2.0 ha lanciato il supporto per Amazon Linux 2. Con questo annuncio, la AppStream versione 2.0 ora supporta quattro tipi di piattaforme:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Amazon Linux 2

È possibile che tu debba scegliere una piattaforma particolare in base a ciò che è richiesto dall'applicazione (ad esempio, se l'applicazione richiede Windows, Amazon Linux 2 non sarà

un'opzione). Oltre ai requisiti dell'applicazione, fai riferimento alla seguente matrice di confronto per aiutarti a scegliere il tipo di piattaforma più adatto al tuo caso d'uso e al tuo ambiente:

Tabella 1 — Tipi di piattaforme, quando utilizzarle e prezzi

| Tipo di piattaforma | Quando usare | Prezzi della flotta* |
| --- | --- | --- |
| Windows Server (2012 R2, 2016 o 2019) | L'applicazione può essere eseguita solo in Windows (e non supporta Amazon Linux 2). Desideri aggiungere un dominio alle tue istanze di streaming. Desideri utilizzare i criteri di gruppo esistenti sulle istanze di streaming AppStream 2.0 (Linux non aderisce ai criteri di gruppo, ma puoi utilizzare gli script di sessione per automatizzare la configurazione all'avvio di una sessione). Utilizzerai Desktop View e i tuoi utenti preferiranno l'esperienza desktop di Windows. Preferisci utilizzare l'applicazione Image Assistant, che fornisce una step-by-step procedura guidata, per creare il catalogo e l'immagine dell'applicazione. Attualmente, devi creare la tua immagine Amazon Linux 2 usando i comandi del terminale (consulta questo tutorial per maggiori informazioni). Vuoi usare Application Settings Persistence. L'abilitazione della persistenza delle | Tariffa RDS SAL (Microsoft Remote Desktop Services Subscriber Access License) di 4,19 USD al mese per ogni utente unico** più quanto segue:<br>1. 0,10 USD all'ora per le flotte Always-On e On-Demand<br>2. 0,15 USD all'ora per le flotte Elastic |

| Tipo di piattaforma | Quando usare | Prezzi della flotta* |
| --- | --- | --- |
| | impostazioni delle applicazioni non è attualmente supportata per gli stack basati su Linux. | |
| Amazon Linux 2 | Vuoi sfruttare le istanze di streaming a basso costo ed evitare i costi di licenza RDS SAL. Le tue applicazioni sono compatibili con Amazon Linux 2 | Le istanze Linux hanno un costo inferiore rispetto alle istanze Windows. Con Linux, non paghi le tariffe RDS SAL e le seguenti tariffe orarie:<br>1. 0,084 USD all'ora per le flotte Always-On e On-Demand<br>2. 0,112 USD all'ora per le flotte Elastic |

* Basato su stream.standard.medium nella regione della Virginia settentrionale

** I clienti idonei possono portare la propria licenza per eliminare i costi di AWS RDS SAL. Per ulteriori dettagli, consulta la pagina dei prezzi AppStream 2.0. I clienti del settore Education possono inoltre avere diritto a un'offerta speciale. Le scuole, le università e alcuni istituti pubblici possono beneficiare di una tariffa utente ridotta per Microsoft RDS SAL.

## Applicazioni

Prima di installare le applicazioni, è importante esaminare i requisiti delle applicazioni, come le dipendenze delle applicazioni e i requisiti hardware. Dopo aver installato correttamente le applicazioni sulle istanze di Image Builder, assicuratevi di cambiare utente e testare le applicazioni nel contesto dell'utente di test.

Quando pianificate la distribuzione delle applicazioni, tenete presente gli endpoint e le quote del servizio. Inoltre, pulite i file di installazione e di supporto per ottimizzare lo spazio totale sull'unità C prima di creare un'immagine. Come promemoria, le istanze AppStream 2.0 hanno un volume a dimensione fissa da 200 GB. L'ottimizzazione dello spazio su disco dopo l'installazione è una procedura consigliata per garantire che il volume a dimensione fissa non venga mai superato.

Se desideri modificare il catalogo di applicazioni a cui gli utenti possono accedere in tempo reale, il framework applicativo dinamico fornisce operazioni API. Le applicazioni gestite dai provider di app dinamiche possono essere all'interno dell'immagine oppure possono essere fuori dall'istanza, ad esempio in una condivisione di file di Windows o una tecnologia di virtualizzazione dell'applicazione. Questa funzionalità richiede una flotta AppStream 2.0 aggiunta a un dominio Microsoft Active Directory. Per ulteriori informazioni, consulta Utilizzo di Active Directory con AppStream 2.0.

# Blocchi di app

I blocchi di app rappresentano lo script di configurazione e i file dell'applicazione necessari per avviare le applicazioni che verranno utilizzate dagli utenti. Il disco rigido virtuale (VHD) può essere qualsiasi oggetto di Amazon S3. È consigliabile che questo oggetto abbia una dimensione inferiore a 1,5 GB, poiché deve essere scaricato completamente prima che l'utente possa accedere all'applicazione.

## Ottimizzazione dei blocchi delle app

Per le flotte basate su Windows, si consiglia di creare un file VHDX per contenere l'applicazione. Per le flotte basate su Linux, si consiglia di creare un'immagine (IMG). Questi dischi virtuali devono essere creati con le dimensioni più ridotte possibile, per ospitare i file dell'applicazione. I dischi virtuali possono essere compressi per ridurne ulteriormente le dimensioni. Nello script di installazione, è necessario decomprimere il disco prima del montaggio. Lo script di PowerShell installazione di Windows di esempio include la funzionalità di decompressione. Esiste un compromesso tra l'espansione di un archivio (zip) e la velocità di download. Potrebbero essere necessari alcuni test per trovare un equilibrio che offra il tempo di avvio delle applicazioni più rapido.

## Aggiornamento delle applicazioni

Le applicazioni possono presentare modifiche sia minori che importanti. Per aggiornamenti minori, usa abilita il controllo delle versioni sul bucket Amazon S3 che ospita i file di blocco dell'app. Questa impostazione consente agli amministratori di ripristinare le versioni precedenti di un'applicazione specifica modificando la versione dell'oggetto VHD dell'applicazione in questione senza modificare la configurazione del blocco dell'app. Con gli aggiornamenti principali, create un nuovo blocco App per il VHD aggiornato. Ciò consentirà agli amministratori di separare le principali modifiche alle applicazioni a livello di blocco dell'app anziché a livello di controllo delle versioni, il che fornisce un approccio più organizzato per la gestione amministrativa delle applicazioni.

# Personalizzazione del profilo utente

Amazon AppStream 2.0 è, per sua natura, un'applicazione e una soluzione desktop non persistente. Quando una sessione utente viene terminata, vengono interrotte anche le modifiche al sistema e all'utente. Abilita la persistenza delle impostazioni dell'applicazione solo quando necessario. Può aggiungere un sovraccarico al processo di accesso e considerare i costi dello storage S3 richiesto.

In situazioni in cui è richiesta la persistenza delle impostazioni dell'applicazione, AWS consiglia di proteggere tale connessione tramite policy personalizzate e endpoint gateway VPC S3. Valuta le dimensioni complessive delle impostazioni dell'applicazione e riduci al minimo le impostazioni salvate nella persistenza delle impostazioni dell'applicazione per ottimizzare costi e prestazioni.

La personalizzazione del profilo utente può essere configurata su un'istanza AppStream 2.0 Image Builder. Ciò include l'aggiunta e la modifica di chiavi di registro, l'aggiunta di file e altre configurazioni specifiche dell'utente. A partire da Image Assistant AppStream 2.0, è disponibile un'opzione per creare un profilo utente. In questo modo il profilo utente del modello viene copiato nel profilo utente predefinito. Dopo aver distribuito l'immagine in una flotta, agli utenti finali che trasmettono sessioni dal parco utenti verrà creato il proprio profilo utente a partire dal profilo utente predefinito. È importante considerare la possibilità di ridurre al minimo le dimensioni del profilo utente, soprattutto quando la persistenza delle impostazioni dell'applicazione è abilitata. Per impostazione predefinita, la dimensione massima del file vHDx per il profilo utente è di 1 GB. Ogni volta che inizia una sessione di streaming, un file vHDx del profilo utente viene scaricato da un bucket S3. Ciò aumenta il tempo di preparazione della sessione di streaming e comporta il rischio di superare il limite, con conseguente interruzione del montaggio del profilo utente mediante il file vHDx.

Per i casi d'uso che richiedono un profilo utente più grande di 1 GB, AWS consiglia di utilizzare metodi alternativi per archiviare i profili. Ad esempio, utilizzando profili di roaming o contenitori di profili FSLogix su storage condiviso come Amazon FSx for Windows File Server. Per ulteriori informazioni, consulta Use Amazon FSx for Windows File Server e FSLogix per ottimizzare la persistenza delle impostazioni delle applicazioni su Amazon 2.0. AppStream

# Sicurezza

Esistono diverse misure di sicurezza che gli sviluppatori devono prendere in considerazione. AppStream gli amministratori sono responsabili dell'installazione e della manutenzione degli aggiornamenti per il sistema operativo Windows, le applicazioni e le relative dipendenze. Per ulteriori indicazioni su come mantenere aggiornate le immagini di base, consulta Keep Your AppStream 2.0 Image Update per ulteriori indicazioni su come mantenere aggiornate le immagini di base.

Per impostazione predefinita, la AppStream versione 2.0 consente agli utenti o alle applicazioni di avviare qualsiasi programma sull'istanza, oltre a quanto specificato nel catalogo delle applicazioni di immagini. Ciò è utile quando l'applicazione si basa su un'altra applicazione come parte di un flusso di lavoro, ma non si desidera che l'utente sia in grado di avviare direttamente l'applicazione dipendente. Ad esempio, l'applicazione avvia il browser per fornire istruzioni di aiuto dal sito Web del fornitore dell'applicazione, ma non si desidera che l'utente avvii il browser direttamente. In alcune situazioni, potresti voler controllare quali applicazioni possono essere avviate sulle istanze di streaming. Microsoft AppLocker è un software di controllo delle applicazioni che utilizza criteri di controllo espliciti per abilitare o disabilitare le applicazioni che un utente può eseguire.

Il software antivirus può influire negativamente sulle sessioni di streaming e sulle istanze di Image Builder. AWSconsiglia di non abilitare gli aggiornamenti automatici per il software antivirus. Per ulteriori informazioni su Windows Defender, fare riferimento a Software antivirus.

## Prestazioni

Prima di creare una nuova immagine, è importante testare le applicazioni come utente di prova. Il test come utente di test consente di garantire che le applicazioni possano essere eseguite in un contesto utente non amministratore. Inoltre, controllate le prestazioni delle applicazioni e l'esperienza utente utilizzando strumenti integrati come Task Manager e Performance Monitor. È consigliabile monitorare l'utilizzo di risorse come CPU, memoria e memoria GPU. In caso di limitazioni di risorse di memoria per CPU, memoria o GPU, valuta la possibilità di aggiornare il tipo di istanza. Per migliorare le prestazioni:

- Disattiva le finestre pop-up del browser
- Disattiva la sicurezza avanzata di IE

## AppStream Selezione della versione dell'agente 2.0

Quando si crea una nuova immagine, è possibile scegliere di utilizzare l'ultimo software dell'agente AppStream 2.0 o di non eseguire l'aggiornamento. Ogni versione del software AppStream 2.0 Agent include correzioni di bug e miglioramenti delle funzionalità. Conserva la tua immagine con la maggior parte dei software. up-to-date Esamina i meccanismi a riguardo nella sezione Aggiornamenti delle immagini di questo documento.

Puoi scegliere l'opzione Usa l'agente più recente. Questa opzione assicura che all'avvio sia sempre installato l'agente AppStream 2.0 più recente. Tuttavia, modifiche impreviste possono influire sulle esperienze degli utenti e un aggiornamento dell'agente può aumentare il tempo necessario per

avviare un'istanza. L'aggiornamento di un'immagine di base richiede la ricreazione dell'immagine. È inoltre importante eseguire dei test prima di distribuire l'immagine aggiornata alla produzione per ridurre al minimo i tempi di avvio.

# Interfaccia a riga di comando (CLI) di Image Assistant

Per gli sviluppatori che desiderano automatizzare o creare a livello di codice immagini AppStream 2.0, utilizzate l'interfaccia CLI di Image Assistant. Questa funzionalità è disponibile sui generatori di immagini con il software AppStream 2.0 agent rilasciato a partire dal 26 luglio 2019. La seguente panoramica di alto livello descrive il processo di creazione programmatica di un'immagine 2.0: AppStream

1. Usa l'automazione di installazione dell'applicazione per installare le applicazioni necessarie per l'image builder. Questa installazione può includere le applicazioni che gli utenti lanceranno, eventuali dipendenze e le applicazioni in background.
2. Determinare i file e le cartelle da ottimizzare.
3. Se applicabile, utilizzate l'operazione `add-application` CLI di Image Assistant per specificare i metadati dell'applicazione e il manifesto di ottimizzazione per l' AppStream immagine 2.0.
4. Per specificare applicazioni aggiuntive per l'immagine AppStream 2.0, ripetere i passaggi da 1 a 3 per ciascuna applicazione, se necessario.
5. Se applicabile, utilizzare l'operazione `update-default-profile` CLI di Image Assistant per sovrascrivere il profilo Windows predefinito e creare l'applicazione e le impostazioni Windows predefinite per gli utenti.
6. Utilizzare l'operazione `create-image` dell'interfaccia a riga di comando di Image Assistant per creare l'immagine.

Per ulteriori informazioni, fare riferimento a Creare l'immagine AppStream 2.0 a livello di codice utilizzando le operazioni CLI di Image Assistant.

# Gestione dell'esperienza di streaming degli utenti

## Personalizzazione tramite script di sessione

AppStream 2.0 fornisce script di sessione su istanza. Puoi utilizzare questi script per eseguire script personalizzati quando si verificano determinati eventi in sessioni di streaming degli utenti. Ad esempio, è possibile utilizzare script personalizzati per preparare l'ambiente AppStream 2.0

prima dell'inizio delle sessioni di streaming degli utenti. Puoi anche utilizzare script personalizzati per eliminare le istanze di streaming dopo che gli utenti hanno completato le proprie sessioni di streaming.

Specificate gli script di sessione all'interno di un'immagine 2.0 AppStream . Per ulteriori informazioni sulla configurazione degli script di sessione, consulta la sezione della guida all'amministrazione sull'utilizzo degli script di sessione per gestire l'esperienza dell'utente. Utilizzati con una condivisione di rete o un profilo AWS Identity and Access Management(IAM), è possibile utilizzare gli script di sessione per recuperare script aggiuntivi da una posizione di archiviazione. Con questo script aggiuntivo, puoi ottimizzare ulteriormente l'esperienza utente. In questo modo è possibile ridurre al minimo il numero di immagini e flotte necessarie per fornire ambienti applicativi agli utenti.

## Utilizzo dei criteri di gruppo di Active Directory

Se prevedi di utilizzare flotte AppStream 2.0 in un dominio Active Directory, puoi utilizzare Group Policies Objects (GPO) per gestire l'esperienza utente. I GPO possono essere assegnati all'unità organizzativa (OU) in cui vengono create le istanze AppStream 2.0. Per semplificare la creazione di immagini, avvia l'immagine AppStream 2.0 di base in un'unità organizzativa che blocchi l'ereditarietà. In questo modo si evita che altre politiche di dominio influiscano sulle esperienze utente AppStream 2.0. L'implementazione di ogni flotta nella relativa unità organizzativa dedicata, con GPO esclusivi che stabiliscono l'ambiente consente di sfruttare i vantaggi one-to-many consolidati della gestione delle AppStream immagini 2.0.

Un esempio di utilizzo delle policy di gruppo consiste nello specificare set di immagini diverse home page di Internet Explorer per ogni flotta 2.0. AppStream

# Aggiornamenti delle immagini

L'applicazione di patch al software è fondamentale per la sicurezza e le prestazioni delle risorse di elaborazione. L'applicazione frequente di patch è elencata come best practice nel Security Pillar del Well-Architected Framework.

Una volta creata e distribuita l'immagine, esistono quattro categorie di software che richiedono l'applicazione di patch all'immagine 2.0: AppStream

- Applicazioni e dipendenze: è responsabilità dell'utente applicare le patch alle applicazioni e alle dipendenze nelle immagini.
- Sistema operativo Microsoft Windows: l'utente è responsabile dell'installazione e della manutenzione degli aggiornamenti per Windows.

- Componenti software: si tratta di driver, agenti e altro software necessario per il funzionamento AppStream 2.0 (ad esempio, l' CloudWatchagente Amazon). AppStream 2.0 rilascia periodicamente nuove immagini di base che contengono nuovi agenti e driver. È possibile ricostruire l'immagine utilizzando la base più recente per riportare i componenti software delle relative immagini ai valori di riferimento più recenti. Il processo di ricostruzione di un'immagine sulla base più recente può essere dispendioso in termini di tempo e complessità in presenza di molte applicazioni o con installazioni di applicazioni complesse.
- AppStream Agente 2.0: è possibile scegliere Usa sempre l'ultima versione dell'agente in Image Assistant. Con questa opzione, le istanze di streaming avviate dall'immagine utilizzano automaticamente la versione più recente dell'agente.

È possibile mantenere aggiornata l'immagine AppStream 2.0 effettuando una delle seguenti operazioni:

- Aggiornare un'immagine utilizzando Managed AppStream 2.0 Image Updates: questo metodo di aggiornamento fornisce gli aggiornamenti più recenti del sistema operativo Windows e dei driver e il software più recente dell'agente AppStream 2.0. Questo metodo gestito aggiorna i componenti del servizio e del sistema operativo Microsoft, ma non consente di aggiornare i componenti dell'applicazione. È consigliabile utilizzare questo metodo quando le installazioni delle applicazioni sono complesse o richiedono una configurazione manuale.
- Aggiornamento del software AppStream 2.0 Agent utilizzando le versioni Managed AppStream 2.0 Image: questo metodo di aggiornamento fornisce il software dell'agente AppStream 2.0 più recente. Questo metodo consente di aggiornare i componenti dell'applicazione.

# Personalizzazione della flotta

## Tipo di flotta

Quando creano una flotta, i clienti devono scegliere un tipo di flotta. Ogni tipo di flotta offre diversi vantaggi in termini di esperienza utente, costi e spese generali di manutenzione. Indipendentemente dal tipo di parco macchine scelto, ogni opzione supporta sia i tipi di piattaforma Windows e Linux, sia Desktop View o Application View.

I clienti possono ora scegliere tra i seguenti tipi di parco veicoli:

- Always-On: questo tipo di flotta offre agli utenti l'accesso immediato alle proprie app. Ti verranno addebitati i costi per tutte le istanze in esecuzione nel tuo parco istanze, anche se nessun utente utilizza app in streaming.
- On-Demand: seleziona questo tipo di flotta per ottimizzare i costi di streaming. Con una flotta on-demand, gli utenti avranno un tempo di inizio di circa uno o due minuti per la sessione. Tuttavia, ti verranno addebitate le tariffe delle istanze di streaming solo quando gli utenti sono connessi e una piccola tariffa oraria per ogni istanza del parco istanze che non sono app di streaming.
- Elastico: le flotte elastiche possono essere utilizzate per applicazioni che non richiedono installazione e possono essere eseguite da un disco rigido virtuale (VHD). Le flotte elastiche non supportano immagini AppStream 2.0 e non richiedono politiche di scalabilità. Ti viene addebitato solo per la durata di una sessione di streaming.

Tabella 2 — Tipi di flotte Amazon AppStream 2.0

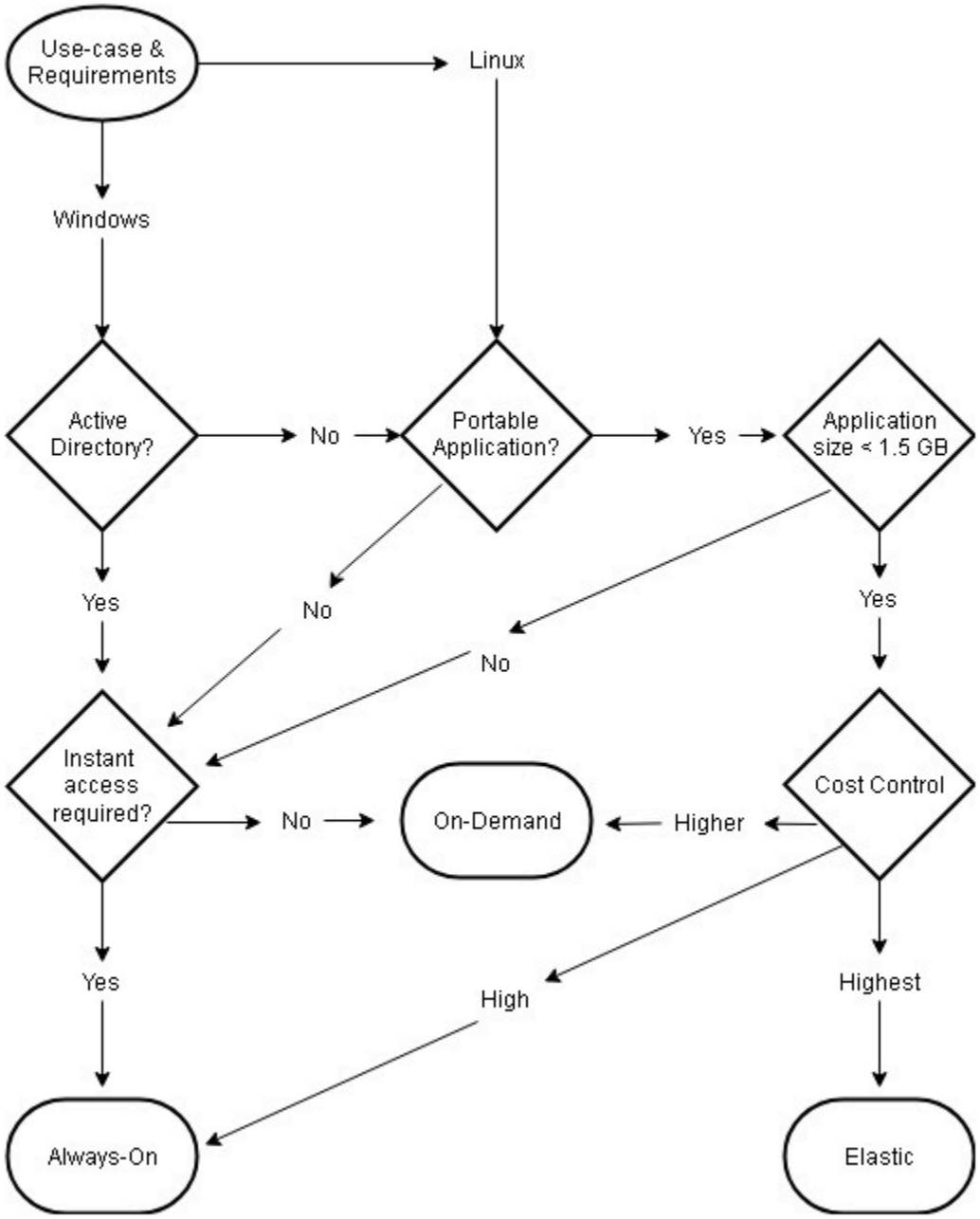
| Tipo di flotta | Quando usare | Esperienza utente | Modello tariffario | Note |
| --- | --- | --- | --- | --- |
| Sempre attivo | Gli utenti richiedon o l'accesso immediato alle applicazi oni all'avvio di una sessione. | Accesso istantaneo alle applicazioni | Paghi il prezzo pieno per ogni istanza disponibi le nel tuo parco istanze (indipend entemente dal fatto che venga | Supporta politiche di immagine e ridimensi onamento personalizzate. |

| Tipo di flotta | Quando usare | Esperienza utente | Modello tariffario | Note |
|---|---|---|---|---|
| | Non avrete un eccesso di capacità significativo nella vostra flotta, forse perché i modelli di utilizzo sono prevedibili e potete controllare in modo affidabile i costi con politiche di scalabilità. | | utilizzata per una sessione). | |

| Tipo di flotta | Quando usare | Esperienza utente | Modello tariffario | Note |
|---|---|---|---|---|
| Su richiesta | È necessari o mantenere una notevole capacità in eccesso nelle flotte. Desiderat e l'ambiente più ottimizza to in termini di costi e non volete pagare il prezzo pieno per la capacità inutilizzata. Gli utenti possono attendere uno o due minuti prima di accedere alle loro applicazioni dopo l'avvio di una sessione. State utilizzan do tipi di istanze più grandi. Il costo orario di un'istanza in esecuzion e è molto più costoso della tariffa per le istanze interrotte. | Gli utenti attendono da uno a due minuti per accedere alle proprie applicazi oni dopo l'avvio di una sessione. | Pagherai il prezzo pieno solo per le istanze di streaming con una sessione attiva e poi un piccolo costo orario per le istanze inattive. | Supporta politiche di immagine e ridimensi onamento personalizzate. |

| Tipo di flotta | Quando usare | Esperienza utente | Modello tariffario | Note |
|---|---|---|---|---|
| Elastic | L'applicazione e le sue dipendenze sono inferiori a ~ 1,5 GB. Ogni volta che un utente avvia una sessione in una flotta Elastic, il file del disco rigido virtuale (VHD) deve essere scaricato da Amazon S3 nella sessione. Di conseguenza, file VHD più grandi (ovvero di dimensioni superiori a 1,5 GB) comporteranno un'esperienza utente finale scadente. L'applicazione è portabile. In altre parole, la tua applicazione e tutte le sue dipendenze possono essere collocate su un VHD e lanciate dal VHD.Non sono necessari | L'utente attende da 45 secondi a 3 minuti per accedere alle applicazioni dopo l'avvio della sessione (il tempo di attesa dipende dalla dimensione del disco rigido virtuale). | Ti viene addebitato solo per la durata di una sessione di streaming . Poiché non esiste il concetto di istanze inattive con le flotte Elastic, non è previsto alcun addebito per le istanze non utilizzate. | Non supporta immagini personalizzate (il cliente fornisce VHD con le applicazioni) o politiche di scalabilità. Supporti `stream.standard.small` e `stream.standard.medium` istanze attualmente. Se il tuo caso d'uso richiede un tipo di istanza diverso, contatta il team AWS del tuo account. |

| Tipo di flotta | Quando usare | Esperienza utente | Modello tariffario | Note |
|---|---|---|---|---|
| | e istanze di streaming unite al dominio (l'aggiunta al dominio non è attualmen te disponibile con le flotte Elastic) Vuoi pagare solo per le sessioni attive (cioè non paghi per la capacità inutilizzata del tuo parco) .I tuoi utenti possono attendere 45 secondi o più per accedere alle loro applicazioni dopo l'avvio di una sessione. Vuoi che AWS gestisca la scalabilità per tu (nessuna politica di scalabilità da gestire). | | | |




Casi d'uso e requisiti relativi al tipo di flotta

# Dimensionamento della flotta

## Capacità minima e scalabilità programmata

Quando si ridimensiona la flotta AppStream 2.0, ci sono diverse considerazioni che si ripercuotono direttamente sull'esperienza utente e sui costi. Il valore inserito per Capacità minima garantisce che il

numero di istanze AppStream 2.0 sia raramente inferiore a questo valore. Al termine di una sessione AppStream 2.0, se il totale di AppStream 2,0 istanze è inferiore al valore di capacità minima, viene avviata una nuova istanza del parco istanze. Come sempre, è importante ricordare che un'istanza AppStream 2.0 viene mappata direttamente a una sessione utente, influendo direttamente sul valore della capacità minima.

L'immissione di un valore per la capacità minima superiore alla concorrenza prevista comporta un aumento dei costi, anche se l'esperienza utente non ne risente. Un valore troppo basso comporta costi bassi, ma influisce sull'esperienza utente quando le richieste totali superano la capacità disponibile. Gli amministratori osserveranno gli errori di «Capacità insufficiente» in questo tipo di situazione. Ad esempio, waiting for `PendingCapacity` become `AvailableCapacity` è un uso inefficiente del tempo dell'utente quando il numero di connessioni previste all'inizio della giornata è un valore prevedibilmente costante.

Inizia con una capacità minima adatta alle tipiche ore non di punta, quindi utilizza una politica di scalabilità pianificata per ripristinare efficacemente la capacità minima prima dell'inizio della giornata lavorativa. Non dimenticare di creare un'altra politica di scalabilità pianificata per riportare la capacità minima alle ore non di punta. Per ulteriori informazioni sulle politiche di scalabilità e su come implementarle, consulta la sezione Fleet auto-scaling strategies di questo documento.

## Capacità massima e quote di servizio

L'impostazione della capacità massima può sembrare un valore arbitrario, ma se prevista e impostata correttamente, ottimizza il consumo e i costi totali delle risorse. Un valore inserito superiore alla quota di servizio per la flotta AppStream 2.0 del tuo parco auto Account AWS può sembrare valido, ma, quando gli eventi di auto scaling tentano di scalare le risorse fino alla capacità massima, non riescono ad avviarsi, poiché il valore della capacità massima supera la quota di servizio disponibile. Assicuratevi che venga effettuata una richiesta di quota di servizio per la capacità massima desiderata per garantire che la scalabilità automatica funzioni come previsto dall'organizzazione.

Un'altra considerazione importante quando si imposta un valore massimo di capacità è il costo. Per ulteriori informazioni, consulta la sezione Ottimizzazione dei costi con la scelta del tipo di flotta di questo documento.

# Scelta della visualizzazione desktop o della visualizzazione delle applicazioni

La scelta di una visualizzazione dell'applicazione o della visualizzazione desktop non ha alcun impatto sulle prestazioni o sui costi. È accessibile una sola visualizzazione alla volta per flotta AppStream 2.0. È possibile modificare l'opzione di visualizzazione Stream. Pianifica questa modifica durante le ore lavorative non di punta, poiché la modifica della visualizzazione dello stream richiede il riavvio del parco veicoli.

Non esiste un'unica best practice per la visualizzazione in streaming. L'impatto delle opzioni di visualizzazione dello stream è riassunto come segue:

- Report dettagliati sull'utilizzo delle applicazioni tramite la funzionalità Rapporti di utilizzo per gli amministratori
- Esperienza e flusso di lavoro complessivi per gli utenti finali (ad esempio, un desktop completo soddisfa le esigenze del caso d'uso o è sufficiente visualizzare solo le applicazioni?).

## Visualizzazione desktop

Nei casi d'uso in cui tutto il flusso di lavoro dell'utente viene eseguito in sessione, Desktop View semplifica l'esperienza utente mantenendo tutte le applicazioni concentrate in un unico ambiente. Desktop View può offrire un'esperienza utente più coerente per le implementazioni di più di 3-5 applicazioni che richiedono l'integrazione con il sistema operativo (OS). Desktop View è efficace quando si gestiscono due ambienti separati e distinti. Ad esempio, un utente può avere accesso simultaneo a un ambiente desktop di produzione e di preproduzione per convalidare le modifiche al layout, alla configurazione e all'accesso alle applicazioni.

AppStream 2.0 Usage Reports crea un rapporto giornaliero sulle applicazioni per Desktop View. L'output risultante per l'applicazione è semplicemente «desktop», mappato direttamente alla sessione AppStream 2.0. Per ulteriori informazioni, consultate la sezione Monitoraggio dell'utilizzo da parte degli utenti di questo documento.

## Visualizzazione solo per le applicazioni

La visualizzazione Solo applicazioni è efficace anche quando lo stack AppStream 2.0 è destinato a fornire alcune applicazioni che sono richieste in modo intermittente. Negli ambienti kiosk,

una distribuzione sicura e protetta delle applicazioni viene fornita tramite Application View. Con Application View, AppStream 2.0 sostituisce la shell predefinita di Windows con una shell personalizzata. Questa shell personalizzata presenta solo le applicazioni in esecuzione, riducendo al minimo la superficie di attacco del sistema operativo.

Per i casi d'uso in cui la AppStream versione 2.0 viene utilizzata per potenziare l'ambiente desktop di un'organizzazione esistente, è preferibile la visualizzazione Solo applicazioni. Implementa il client Windows AppStream 2.0 in modalità applicazione nativa per ridurre al minimo la confusione tra gli utenti grazie al pieno utilizzo delle scorciatoie da tastiera.

Amazon 2.0 Usage Reports crea un rapporto giornaliero sulle applicazioni per la visualizzazione delle applicazioni. Per un reporting più granulare sull'utilizzo delle applicazioni e delle esecuzioni, prendi in considerazione una soluzione di terze parti per la creazione di report a livello di sistema operativo. Puoi utilizzare Microsoft AppLocker in modalità di reporting o prendere in considerazione soluzioni disponibili inMarketplace AWS, come Stratusphere UX di Liquidware.

# Configurazione del ruolo AWS Identity and Access Management

Se un carico di lavoro richiede agli utenti finali AppStream 2.0 di accedere ad altri AWS servizi dall'interno della sessione, è consigliabile delegare l'accesso tramite l'uso di AWS Identity and Access Management ruoli (IAM). I ruoli IAM possono essere collegati direttamente alla sessione dell'utente finale tramite l'assegnazione a livello di flotta. Per ulteriori best practice sull'utilizzo dei ruoli IAM con AppStream 2.0, consulta questa sezione della guida per l'amministratore.

## Utilizzo di credenziali statiche

Alcuni carichi di lavoro possono richiedere input statici per le chiavi di accesso IAM anziché ereditarli dal ruolo associato. Esistono due metodi per ricevere queste credenziali. Il primo metodo prevede l'archiviazione delle chiavi di accesso all'interno di un AWS servizio e la successiva concessione agli utenti finali di un accesso IAM esplicito per estrarre quel valore specifico dal servizio. Due esempi di meccanismi di archiviazione delle chiavi di accesso utilizzano AWS Secrets ManagerAWSSSM Parameter Store. Il secondo metodo consiste nell'utilizzare il provider di credenziali AppStream 2.0 per accedere alle chiavi di accesso del ruolo allegato. Questo può essere fatto richiamando il fornitore di credenziali e analizzando l'output della chiave di accesso e della chiave segreta. Di seguito è riportato un esempio di come eseguire questa azione. PowerShell

```
$CMD = 'C:\Program Files\Amazon\Photon\PhotonRoleCredentialProvider
\PhotonRoleCredentialProvider.exe'
$role = 'Machine'
```

```
$output = & $CMD --role=$role
$parsed = $output | ConvertFrom-Json

$access_key = $parsed.AccessKeyId
$secret_key = $parsed.SecretAccessKey
$session_token = $parsed.SessionToken
```

## Proteggi il tuo AppStream bucket 2.0 S3

Se il carico di lavoro AppStream 2.0 è configurato con Home Folder e/o Application Persistence, è consigliabile proteggere il bucket Amazon S3 in cui vengono archiviati i dati persistenti da accessi non autorizzati o eliminazioni accidentali. Il primo livello di protezione consiste nell'aggiungere una policy sui bucket Amazon S3 per impedire l'eliminazione accidentale del bucket. Il secondo livello di protezione consiste nell'aggiungere una policy sui bucket che si allinea al principio del privilegio minimo. L'allineamento al principio può essere fatto solo consentendo l'accesso ai bucket alle parti necessarie.

# Strategie di scalabilità automatica della flotta

## Comprendere le AppStream istanze 2.0

AppStream Le istanze con parco istanze 2.0 hanno un rapporto utente/parco istanze di 1:1. Ciò significa che ogni utente ha la propria istanza di streaming. Il numero di utenti connessi contemporaneamente determinerà la dimensione del parco veicoli.

## Policy di dimensionamento

AppStream Le flotte 2.0 vengono lanciate in un Application Auto Scaling Group. Ciò consente alla flotta di scalare in base all'utilizzo per soddisfare la domanda. Con l'aumento dell'utilizzo, la flotta si ridimensiona e, man mano che gli utenti si disconnettono, la flotta si ridimensiona nuovamente. Questo è controllato impostando politiche di scalabilità. È possibile impostare politiche di ridimensionamento pianificate, scalabilità dei passaggi e tracciamento degli obiettivi. Per ulteriori informazioni su queste politiche di scalabilità, consulta Fleet Auto Scaling for AppStream Amazon 2.0.

### Scalabilità graduale

Queste politiche aumentano o diminuiscono la capacità del parco macchine di una percentuale rispetto alla dimensione attuale del parco macchine o a un numero specifico di istanze. Le politiche di scalabilità graduale sono attivate da CloudWatch metriche AppStream 2.0 di`Capacity Utilization`, o. `Available Capacity` `Insufficient Capacity Errors`

Quando si utilizzano politiche di scalabilità graduale, si AWS consiglia di aggiungere una percentuale di capacità e non un numero fisso di istanze. Ciò garantisce che le azioni di scalabilità siano proporzionali alle dimensioni del parco macchine. Ti aiuterà a evitare situazioni in cui la scalabilità è troppo lenta (perché hai aggiunto un numero limitato di istanze rispetto alle dimensioni del tuo parco macchine) o troppe istanze quando il parco macchine è piccolo.

### Monitoraggio degli obiettivi

Con questa politica si specifica un livello di utilizzo della capacità per la flotta. Application Autoscaling crea e gestisce gli CloudWatch allarmi che attivano la politica di scalabilità. Ciò aggiunge o rimuove la capacità necessaria per mantenere il parco veicoli pari o vicino al valore target specificato. Per garantire la disponibilità delle applicazioni, la flotta viene ridimensionata proporzionalmente alla metrica il più velocemente possibile, ma in modo più graduale. Quando configuri il tracciamento

degli obiettivi, considera il tempo di attesa della scalabilità per garantire che lo scale-out e lo scale-in avvengano negli intervalli desiderati.

Il tracciamento degli obiettivi è efficace in situazioni di abbandono elevato. Il tasso di abbandono si verifica quando un gran numero di utenti inizia o termina una sessione in un breve periodo di tempo. Puoi identificare il tasso di abbandono esaminando le CloudWatch metriche relative alla tua flotta. I periodi di tempo in cui la capacità in sospeso della flotta è superiore a zero senza modifiche (o con variazioni minime) della capacità desiderata indicano che è probabile che si verifichi un tasso di abbandono elevato. In situazioni di abbandono elevato, configura politiche di tracciamento degli obiettivi in cui (100 — percentuale di utilizzo target) sia superiore al tasso di abbandono registrato in un periodo di 15 minuti. Ad esempio, se il 10% della tua flotta verrà interrotto entro 15 minuti a causa del turnover degli utenti, stabilisci un obiettivo di utilizzo della capacità pari o inferiore al 90% per compensare l'elevato tasso di abbandono.

## Scalabilità pianificata

Queste politiche consentono di impostare la capacità della flotta desiderata in base a una pianificazione temporale. Questa politica è efficace quando si comprende il comportamento di accesso e si possono prevedere le variazioni della domanda.

Ad esempio, all'inizio della giornata lavorativa, potresti aspettarti che 100 utenti richiedano connessioni di streaming alle 9:00. Puoi configurare una politica di scalabilità pianificata per impostare la dimensione minima della flotta su 100 alle 8:40. Ciò consente di creare e rendere disponibili le istanze del parco istanze all'inizio della giornata lavorativa e consente a 100 utenti di connettersi contemporaneamente. È quindi possibile impostare un'altra politica pianificata per ampliare il parco veicoli fino a un minimo di dieci alle 17:00. Ciò consente di risparmiare sui costi, poiché la richiesta di sessioni fuori orario è inferiore rispetto alla giornata lavorativa.

## Politiche di scalabilità nella produzione

Puoi scegliere di combinare diversi tipi di politiche di scalabilità in un'unica flotta per contribuire a definire politiche di scalabilità precise per il comportamento degli utenti. Nell'esempio precedente, è possibile combinare la politica di scalabilità pianificata con le politiche di tracciamento degli obiettivi o di scalabilità per fasi per mantenere un livello di utilizzo specifico. La combinazione di scalabilità pianificata e scalabilità mirata al monitoraggio degli obiettivi può aiutare a ridurre l'impatto di un forte aumento dei livelli di utilizzo quando la capacità è necessaria immediatamente.

Gli utenti connessi alle sessioni di streaming quando una politica di scalabilità modifica il numero desiderato di istanze non sono influenzati da una scalabilità verticale o orizzontale. Le politiche di

scalabilità non porranno fine alle sessioni di streaming esistenti. Le sessioni esistenti continueranno senza interruzioni fino alla fine della sessione da parte dell'utente o a seguito di una politica di timeout del parco veicoli.

Il monitoraggio dell'utilizzo della AppStream versione 2.0 con CloudWatch metriche può aiutarti a ottimizzare le tue politiche di scalabilità nel tempo. Ad esempio, è normale che si verifichi un eccesso di risorse durante la configurazione iniziale e si potrebbero verificare lunghi periodi di scarso utilizzo. In alternativa, se il parco macchine non è sufficientemente fornito, potrebbero verificarsi errori di utilizzo della capacità elevata e di «capacità insufficiente». La revisione CloudWatch delle metriche può aiutare a modificare le politiche di scalabilità per mitigare questi errori. Per ulteriori informazioni ed esempi di politiche di scalabilità AppStream 2.0 che puoi utilizzare, consulta Ridimensiona le tue flotte Amazon 2.0. AppStream

# Le migliori pratiche per la scalabilità della progettazione delle politiche

## Combina le politiche di scalabilità

Molti clienti scelgono di combinare diversi tipi di politiche di scalabilità in un'unica flotta per aumentare la potenza e la flessibilità di Auto Scaling AppStream in 2.0. Ad esempio, è possibile configurare una politica di scalabilità pianificata per aumentare il parco veicoli almeno alle 6:00 prima che gli utenti inizino la giornata lavorativa e ridurre il numero minimo del parco veicoli alle 16:00 prima che gli utenti smettano di lavorare. È possibile combinare questa politica di scalabilità pianificata con politiche di tracciamento degli obiettivi o di scalabilità graduale per mantenere un livello di utilizzo specifico e scalare in o in verticale durante il giorno per gestire i picchi di utilizzo. La combinazione di scalabilità pianificata e scalabilità con tracciamento degli obiettivi può aiutare a ridurre l'impatto di un forte aumento dei livelli di utilizzo quando la capacità è necessaria immediatamente.

## Evita il tasso di scalabilità e abbandono

Valuta se la tua flotta potrebbe subire un elevato tasso di abbandono a causa del tuo caso d'uso. Il tasso di abbandono si verifica quando un gran numero di utenti inizia e termina le sessioni in un breve periodo di tempo. Ciò può verificarsi quando più utenti accedono contemporaneamente a un'applicazione del tuo parco applicazioni solo per pochi minuti prima di disconnettersi.

In tali situazioni, le dimensioni del parco macchine potrebbero scendere ben al di sotto della capacità desiderata, poiché le istanze terminano quando gli utenti terminano le sessioni. Le politiche di scalabilità graduale potrebbero non aggiungere istanze abbastanza velocemente da compensare il tasso di abbandono e, di conseguenza, il parco istanze rimane bloccato a determinate dimensioni.

Puoi identificare il tasso di abbandono CloudWatch esaminando le metriche relative alla tua flotta. I periodi di tempo in cui la capacità in sospeso della flotta è superiore a zero senza variazioni (o con variazioni minime) della capacità desiderata indicano che è probabile che si verifichi un tasso di abbandono elevato. Per tenere conto delle situazioni di abbandono elevato, utilizzate le politiche di scalabilità di Target Tracking e scegliete un target di utilizzo in modo che (100, percentuale di utilizzo target) sia superiore al tasso di abbandono in un periodo di 15 minuti. Ad esempio, se il 10% del parco veicoli verrà eliminato entro 15 minuti a causa del turnover degli utenti, stabilisci un obiettivo di utilizzo della capacità pari o inferiore al 90% per compensare l'elevato tasso di abbandono.

# Comprendi la percentuale massima di approvvigionamento

I clienti che gestiscono flotte AppStream 2.0 per un gran numero di utenti dovrebbero considerare la possibilità di prevedere dei limiti tariffari. Questo limite influirà sulla velocità con cui le istanze possono essere aggiunte a una flotta o a tutte le flotte all'interno di un. Account AWS

Esistono due limiti da considerare:

- Per una singola flotta, AppStream 2,0 forniture a una velocità massima di 20 istanze al minuto.
- Per una singola unitàAccount AWS, AppStream 2,0 forniture a una velocità di 60 istanze al minuto (con una raffica di 100 istanze al minuto).

Se più di tre flotte vengono ampliate in parallelo, il limite di velocità di provisioning degli account viene condiviso tra queste flotte (ad esempio, sei flotte con scalabilità parallela potrebbero fornire ciascuna fino a 10 istanze al minuto). Inoltre, considera il tempo impiegato da una determinata istanza di streaming per completare il provisioning in risposta a un evento di scalabilità. Per le flotte non unite a un dominio Active Directory, in genere si tratta di 15 minuti. Per le flotte unite a un dominio Active Directory, questa operazione può richiedere fino a 25 minuti.

Alla luce di questi vincoli, considera i seguenti esempi:

- Se desideri scalare un singolo parco istanze da 0 a 1000 istanze, occorreranno 50 minuti (1000 istanze/20 istanze al minuto) per completare il provisioning e poi altri 15-25 minuti affinché tutte le istanze diventino disponibili per gli utenti finali, per un totale di 65-75 minuti.
- Se desideri scalare contemporaneamente tre flotte da 0 a 333 istanze (per un totale di 999 istanze nelAccount AWS), occorreranno circa 17 minuti (999/60 istanze al minuto) per completare il provisioning di tutti i parchi veicoli e poi altri 15 minuti affinché tali istanze diventino disponibili per gli utenti finali, per un totale di 32-42 minuti.

# Utilizza più zone di disponibilità

Scegli più AZ nella regione per l'implementazione della tua flotta. Quando selezioni più AZ per la tua flotta, aumenti la probabilità che il tuo parco macchine sia in grado di aggiungere istanze in risposta a un evento di scalabilità. La CloudWatch metrica PendingCapacity è un punto di partenza per valutare l'ottimizzazione del design AZ della flotta nelle implementazioni di flotte di grandi dimensioni. Un valore elevato e sostenuto per PendingCapacity può indicare la necessità di estendere la scalabilità

orizzontale (tra le AZ). Per ulteriori informazioni, consulta Monitoring Amazon AppStream 2.0 Resources.

Ad esempio, se la scalabilità automatica tenta di fornire istanze per aumentare le dimensioni della flotta e la zona di disponibilità selezionata ha una capacità insufficiente, la scalabilità automatica aggiungerà invece istanze nelle altre AZ che hai specificato per la tua flotta. Per ulteriori informazioni sulle zone di disponibilità e sulla progettazione AppStream 2.0, consulta la sezione Zone di disponibilità in questo documento.

## Monitora le metriche relative agli errori di capacità insufficiente

«Insufficient Capacity Error» è una CloudWatch metrica per flotte AppStream 2.0. Questa metrica specifica il numero di richieste di sessione rifiutate a causa della mancanza di capacità.

Quando si apportano modifiche alle politiche di scalabilità, è utile creare un CloudWatch allarme per avvisare l'utente quando si verificano errori di capacità insufficiente. Ciò consente di modificare rapidamente le politiche di scalabilità per ottimizzare la disponibilità per gli utenti. La guida all'amministrazione fornisce passaggi dettagliati per monitorare le risorse AppStream 2.0.

# Metodi di connessione

Durante le sessioni di streaming in AppStream versione 2.0, gli utenti hanno a disposizione due metodi di connessione:

- Accesso tramite browser Web: è supportato qualsiasi browser compatibile con HTML5. Non sono necessari plug-in o download.
- AppStream Client Windows 2.0

Come procedura consigliata, considera i requisiti di funzionalità e dispositivo per il caso d'uso dell'utente per allineare il browser o il dispositivo che meglio supporta i suoi requisiti.

> **Note**
>
> AppStream 2.0 non è supportato su dispositivi con risoluzioni dello schermo inferiori a 1024 x 768 pixel.

## Riepilogo delle funzionalità e del supporto dei dispositivi

Tabella 3 — Funzionalità di riepilogo e supporto del dispositivo

| | Accesso tramite browser Web | AppStream Client Windows 2.0 |
|---|---|---|
| Monitor multiplo (risoluzione fino a 2k) | Supportato | Supportato |
| Monitor multiplo (risoluzione fino a 4k) | N/D | Supportato |
| Supporto per tablet da disegno | Supportato* | Supportato |
| Supporto per dispositivi touchscreen | Supportato | N/D |
| Supporto per dispositivi USB passthrough | N/D | Supportato |

| | Accesso tramite browser Web | AppStream Client Windows 2.0 |
|---|---|---|
| Tasti di scelta rapida | Supportato | Supportato |
| Offset relativo del mouse | Supportato | Supportato |
| Trasferimento di file | Supportato | Supportato |
| Reindirizzamento della stampante locale | N/D | Supportato |
| Reindirizzamento dell'unità locale | N/D | Supportato |
| Supporto per web-cam | Supportato | Supportato |

*Solo Google Chrome e Mozilla Firefox

## Accesso tramite browser Web

AppStream L'accesso tramite browser Web 2.0 consente l'accesso alle applicazioni senza la necessità di installare un client dedicato. Gli utenti possono connettersi utilizzando un browser compatibile con HTML5 supportato. Non è richiesto alcun plug-in o estensione del browser.

L'accesso tramite browser Web offre un'ampia scelta di sistemi operativi e tipi di dispositivi finali.

## AppStream Client 2.0 per Windows

Il client AppStream 2.0 per Windows è un'applicazione che puoi installare sul tuo PC Windows. Questa applicazione offre funzionalità aggiuntive che non sono disponibili quando si accede alla AppStream versione 2.0 utilizzando un browser Web. Ad esempio, il AppStream client consente di eseguire le seguenti operazioni:

- Utilizza più di due monitor o una risoluzione 4K
- Usa i tuoi dispositivi USB con applicazioni trasmesse in streaming tramite 2.0 AppStream
- Accedi alle unità e alle cartelle locali durante le sessioni di streaming

- Reindirizza i lavori di stampa dall'applicazione di streaming a una stampante collegata al computer locale
- Utilizzate la webcam locale per conferenze video e audio durante le sessioni di streaming
- Usa le scorciatoie da tastiera nelle applicazioni a cui accedi durante le sessioni di streaming
- Interagisci con le tue applicazioni di streaming remoto più o meno allo stesso modo in cui interagisci con le applicazioni installate localmente

## AppStream modalità di connessione client 2.0

Il client AppStream 2.0 offre due modalità di connessione: modalità applicazione nativa e modalità classica. La modalità di connessione scelta determina le opzioni disponibili durante lo streaming delle applicazioni e il funzionamento e la visualizzazione delle applicazioni di streaming. Gli amministratori possono controllare la capacità degli utenti di passare dalla modalità applicativa nativa alla modalità classica.

- La modalità classica trasmette le applicazioni nella finestra della sessione AppStream 2.0. È simile al modo in cui gli utenti finali trasmettono le applicazioni in un browser Web. Utilizzate la modalità classica se gli utenti finali preferiscono eseguire lo streaming delle applicazioni allo stesso modo dei browser, utilizzando al contempo funzionalità aggiuntive come la connessione per il reindirizzamento locale di file e stampanti. La modalità di connessione predefinita consigliata è la modalità di connessione classica. La modalità classica è l'unica modalità supportata per Desktop View.
- La modalità applicativa nativa consente agli utenti finali di lavorare con le applicazioni di streaming remoto in modo simile alle altre applicazioni installate localmente. Se gli utenti finali sono abituati a lavorare con applicazioni installate localmente, la modalità applicativa nativa offre un'esperienza senza interruzioni. L'applicazione di streaming remoto funziona più o meno allo stesso modo di un'applicazione installata localmente. L'icona dell'applicazione viene visualizzata nella barra delle applicazioni del PC locale, proprio come fanno le icone delle applicazioni locali. A differenza delle icone delle applicazioni locali, le icone delle applicazioni di streaming in modalità applicazione nativa includono il logo AppStream 2.0. La modalità applicazione nativa è la modalità di connessione consigliata quando gli utenti desiderano utilizzare le scorciatoie da tastiera dell'applicazione e passare facilmente da singole applicazioni locali a singole applicazioni remote utilizzando le scorciatoie da tastiera.

## Implementazione e gestione dei client

Gli utenti possono installare autonomamente il client AppStream 2.0 oppure gli amministratori possono installare il client AppStream 2.0 per loro eseguendo PowerShell script in remoto o riconfezionando il client AppStream 2.0 con impostazioni personalizzate.

Devi qualificare i dispositivi USB che vuoi abilitare per gli utenti che li usano con la sessione di streaming. Se il dispositivo USB non è qualificato, non verrà rilevato dalla AppStream versione 2.0 e non potrà essere condiviso con la sessione. Una volta qualificati i dispositivi, gli utenti devono condividerli con la AppStream versione 2.0 ogni volta che iniziano una nuova sessione di streaming.

Quando si distribuisce il client AppStream 2.0 su larga scala, AWS consiglia di utilizzare l'Enterprise Deployment Tool. L'Enterprise Deployment Tool include i file di installazione AppStream del client e un modello amministrativo di Group Policy.

# Domini personalizzati

Quando si implementa la AppStream versione 2.0 a livello di codice, è possibile creare un dominio personalizzato in grado di fornire agli utenti un'esperienza familiare per le sessioni di streaming. Nelle implementazioni SAML 2.0 IdP 2.0, è importante sottolineare che l'accesso AppStream degli utenti inizia dall'IdP, non dalla 2.0. AppStream Gli utenti non richiedono URL AppStream 2.0, in quanto vengono forniti dall'IdP dopo l'autenticazione. Pertanto, i nomi di dominio personalizzati non sono necessari per le distribuzioni IdP SAML 2.0.

# Autenticazione

Con la AppStream versione 2.0, l'autenticazione può avvenire al di fuori di Amazon AppStream 2.0 o come parte del servizio AppStream 2.0. La scelta del modo in cui avverrà l'autenticazione per la distribuzione AppStream 2.0 è una considerazione fondamentale della progettazione. Non è raro che un'organizzazione disponga di più implementazioni della AppStream versione 2.0 per diversi casi d'uso. Ogni caso d'uso può avere un metodo di autenticazione diverso.

Esistono tre tipi di metodi di autenticazione per AppStream la versione 2.0:

- SAML 2.0
- Pool di utenti
- Programmatico

## Determinazione del metodo ottimale

Amazon AppStream 2.0 è progettato per essere flessibile e può essere applicato alla maggior parte dei requisiti di progettazione organizzativa. Nel determinare il metodo ottimizzato per l'autenticazione, è consigliabile considerare gli obiettivi e le finalità di coloro che utilizzano il servizio, nonché le politiche e le procedure organizzative.

Ecco alcuni esempi di combinazione di casi d'uso con obiettivi organizzativi.

Tabella 4 — Casi d'uso con obiettivi organizzativi

| Esempio | Descrizione | Autenticazione |
| --- | --- | --- |
| Sono necessarie istanze del parco istanze del parco istanze aggiunte al dominio | Le applicazioni installate sull' AppStream immagine sono accessibili solo alle risorse aggiunte al dominio. | SAML 2.0 |
| Integrazione completa con i servizi Microsoft | Dipendenza organizzativa dallo sviluppo di Microsoft Group Policies e dall'infr astruttura di backend | SAML 2.0 |

| Esempio | Descrizione | Autenticazione |
| --- | --- | --- |
| Single Sign-on (SSO) aziendale esistente | Tutti i nuovi servizi devono sfruttare una soluzione SSO aziendale che preveda diversi processi di reporting e sicurezza. | SAML 2.0 |
| Supporto tramite smart card per le applicazioni | Smart card (come Private Identity Verification e Common Access Card) per l'autenti cazione durante la sessione di applicazioni in streaming tramite un lettore di smart card. | SAML 2.0 |
| Forza lavoro stagionale con personale temporaneo | Alcuni mesi all'anno, ai lavoratori temporanei viene assegnata una piccola serie di applicazioni che non includono risorse interne per il completamento delle attività. | Pool di utenti |
| Supporto IT limitato | Organizzazioni più piccole con meno di 50 utenti e personale IT limitato, che cercano di eliminare il sovraccarico legato alla manutenzione di un Identity Provider (IdP) | Pool di utenti |
| Fornitore di software indipendente (ISV) | Soluzione proprietaria creata dall'organizzazione che include i diritti e l'autenti cazione degli utenti, che estende la AppStream versione 2.0 come parte della soluzione. * | Programmatico |

| Esempio | Descrizione | Autenticazione |
| --- | --- | --- |
| Vetrina tecnologica | Ambiente completamente effimero che presenta una tecnologia proprietaria come parte di una visita guidata della soluzione senza la necessità di memorizzare le informazioni dell'utente. | Programmatico |
| Esperienza interattiva sul sito | Rendi interattivo il tuo sito Web con lo streaming di applicazioni Windows. ** | Programmatico |

*Per ulteriori informazioni, consulta i fornitori di software: distribuisci le tue applicazioni a qualsiasi dispositivo utente.

**Per ulteriori informazioni, consulta Embed AppStream 2.0 Streaming Sessions.

Se l'organizzazione ha un caso d'uso o una politica che non sono elencati negli esempi forniti in precedenza, è consigliabile prevedere lo stato finale desiderato del consumo del flusso di lavoro AppStream 2.0 per garantire che la soluzione di autenticazione non sia in conflitto con esso.

# Configurazione del provider di identità

## SAML 2.0

Security Assertion Markup Language (SAML) 2.0 è un'opzione di distribuzione comune per consentire agli utenti di utilizzare le risorse. AWS Vari provider di identità SAML 2.0 di terze parti supportano la versione 2.0. AppStream Indipendentemente dal fatto che le tue risorse AppStream 2.0 appartengano o meno a un dominio, SAML 2.0 IdP richiede l'utilizzo di IAM.

Poiché la maggior parte IdPs genera un file metadata.xml univoco con attributi SAML specifici per ogni applicazione SAML, ogni stack AppStream 2.0 richiede un ruolo che abbia una relazione di fiducia con l'IdP SAML e una policy che disponga di un'unica autorizzazione per AppStream:Stream con condizioni che corrispondono ai requisiti dell'IdP SAML e dell'ARN dello stack 2.0. AppStream

La guida all'amministrazione 2.0 fornisce un esempio di configurazione per la progettazione di un AppStream singolo stack 2.0. AppStream Per le distribuzioni a più stack, consulta i passaggi facoltativi per l'utilizzo del catalogo di applicazioni multi-stack SAML 2.0.

## Bacino d'utenza

La scheda User Pool nella AppStream versione 2.0 è un'opzione valida per dimostrazioni concettuali di piccole dimensioni. Come best practice, è consigliabile evitare i pool di utenti per qualsiasi caso d'uso e organizzazione che utilizzi la AppStream versione 2.0 per fornire applicazioni di produzione.

Un aspetto importante da tenere presente sui pool di utenti è che gli indirizzi e-mail degli utenti fanno distinzione tra maiuscole e minuscole; è quindi consigliabile assicurarsi che gli utenti siano istruiti su come inserire correttamente le credenziali utente.

## URL di streaming

Per le implementazioni che richiamano risorse AppStream 2.0 da un servizio centralizzato (in genere ISV), l'autenticazione programmatica si basa su un'applicazione a cui effettuare chiamate programmatiche per passare dinamicamente le informazioni e creare una sessione 2.0 AWS per i suoi utenti. AppStream Utilizzate il metodo di autenticazione API (comunemente denominato «programmatico») per creare URL di streaming utilizzando l'operazione URL. CreateStreaming L'utente che effettua la `CreateStreamingURL` chiamata deve utilizzare un utente o un ruolo valido con autorizzazione per. `appstream:CreateStreamingURL`

Quando si crea la policy per l'accesso programmatico, è consigliabile proteggere l'accesso specificando l'esatto AppStream 2.0 Stack ARN nella sezione Risorse al posto del valore predefinito '*'. Per esempio:

Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appstream:createStreamingURL"
            ],
            "Resource": "arn:aws:appstream:us-east-
1:031421429609:stack/BestPracticesStack"
```

```
        }
    ]
}
```

> **Note**
>
> Puoi recuperare rapidamente gli ARN dei tuoi stack AppStream 2.0 utilizzando l'API describe stacks o la CLI di AWS.

AppStream Le istanze 2.0 devono iniziare come istanze generiche. Tramite le informazioni trasmesse dall'applicazione, l'istanza AppStream 2.0 stabilisce l'ambiente utilizzando il contesto della sessione per rendere le cose dinamiche per l'utente.

Sebbene sia possibile utilizzare i GPO locali per specificare le impostazioni all'accesso dell'utente, il contesto della sessione è una procedura consigliata quando si utilizzano `CreateStreamingURL` e si passano attributi chiave come l'ID cliente o le impostazioni di connessione al database, da utilizzare nella sessione. AppStream

## Autorizzazione della domanda

AppStream 2.0 può creare dinamicamente il catalogo delle applicazioni che viene presentato agli utenti. I permessi delle applicazioni si basano sugli attributi SAML 2.0 o utilizzando AppStream 2.0 Dynamic Application Framework.

I diritti applicativi basati sugli attributi che utilizzano SAML 2.0 sono consigliati nella maggior parte degli scenari. Per gestire la consegna dei pacchetti applicativi, si consiglia Dynamic Application Framework.

# Integrazione con Microsoft Active Directory

I generatori di immagini e le flotte di Amazon AppStream 2.0 possono essere integrati con Microsoft Active Directory. Ciò consente di fornire un metodo centralizzato per l'autenticazione e l'autorizzazione degli utenti e di applicare le politiche del gruppo Active Directory alle istanze 2.0 aggiunte AppStream al dominio. L'utilizzo di AppStream flotte unite a un dominio offre gli stessi vantaggi amministrativi di un ambiente locale. Ciò include la gestione centralizzata delle condivisioni di file di rete, dei diritti utente alle app, dei profili di roaming, dell'accesso alle stampanti e di altre impostazioni basate su policy.

Quando si integra un ambiente AppStream 2.0 con Active Directory, è importante notare che l'autenticazione iniziale allo stack AppStream 2.0 è ancora gestita da un IdP SAML2.0. Dopo che l'utente è stato autenticato con successo sull'IdP, quando avvia una sessione, deve inserire la password del dominio o un'autenticazione con smart card per il dominio Active Directory.

Durante la progettazione dell'ambiente Active Directory Domain Services (ADDS) che verrà utilizzato con la AppStream versione 2.0, sono disponibili due opzioni di servizio e molti scenari di distribuzione. Inoltre, assicuratevi che la rete AppStream 2.0 venga esaminata con il proprietario della topologia del sito Active Directory.

## Opzioni di servizio

Active Directory può anche essere distribuito utilizzando AWSManaged Microsoft Active Directory (AD). AWS Managed Microsoft AD è un servizio completamente gestito che consente di eseguire Microsoft Active Directory. Microsoft Active Directory può essere utilizzato anche in un ambiente self-hosted, in esecuzione su EC2 o in locale.

## Scenari di distribuzione

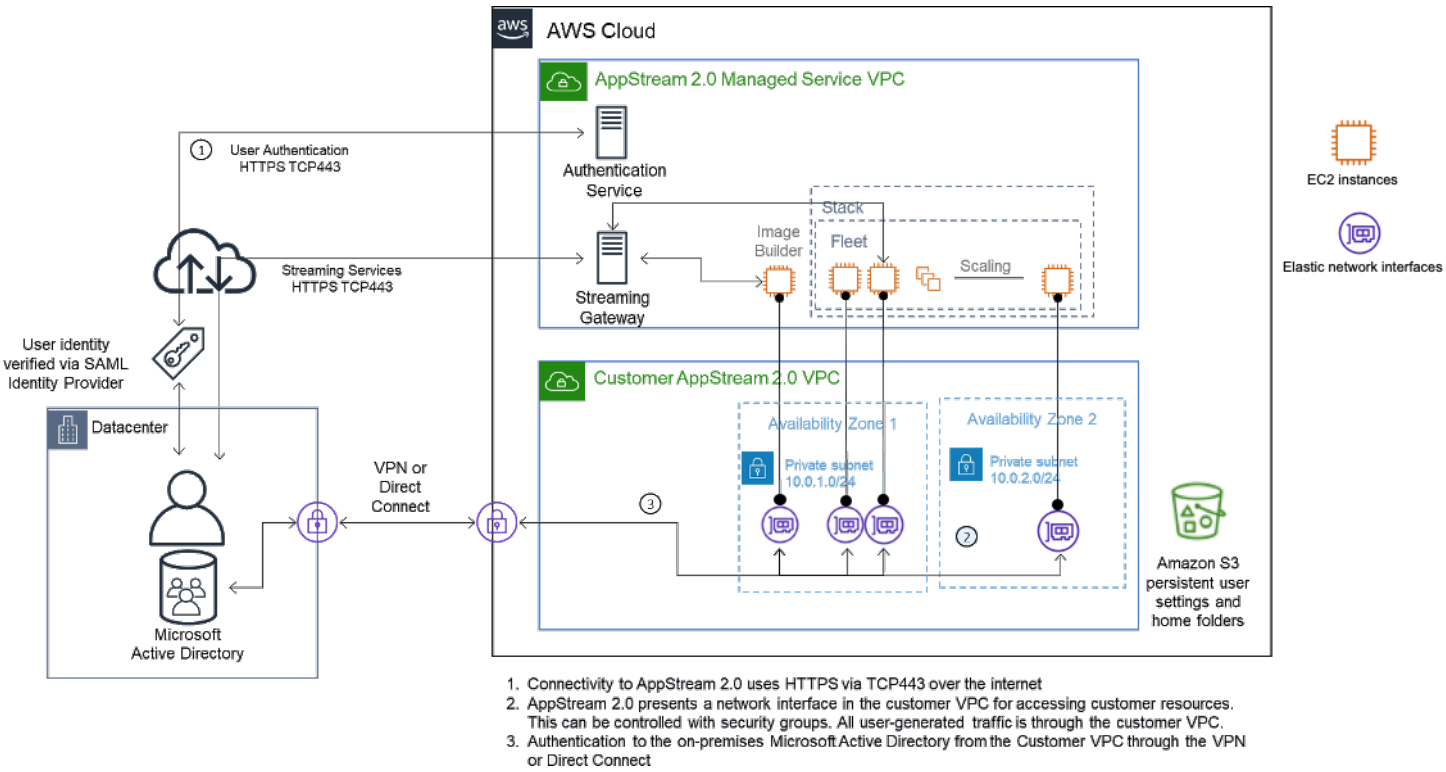
I seguenti scenari di distribuzione elencati sono opzioni di integrazione comunemente utilizzate e consigliate per AppStream 2.0 con Microsoft Managed AD o Active Directory autogestito del cliente. Tutti i diagrammi di architettura elencati di seguito utilizzano costrutti Amazon di base.

- Amazon Virtual Private Cloud (VPC): creazione di un Amazon VPC dedicato ai servizi AppStream 2.0 con almeno quattro sottoreti private distribuite su quattro AZ. Due delle sottoreti private vengono utilizzate per flotte e Image Builder. AppStream Le due sottoreti rimanenti vengono utilizzate per i controller di dominio su EC2 o Microsoft Managed AD).

- Set di opzioni DHCP (Dynamic Host Configuration Protocol): fornisce uno standard per il trasferimento delle informazioni di configurazione alla flotta AppStream 2.0 e agli Image Builder che verranno forniti nel VPC. Il set di opzioni DHCP è definito a livello di VPC. Consente ai clienti di definire un nome di dominio e impostazioni DNS specifici che verranno utilizzati con l'istanza AppStream 2.0 al momento del provisioning.
- AWSDirectory Services: Amazon Microsoft Managed AD può essere distribuito in due sottoreti private che verranno utilizzate insieme ai carichi di lavoro 2.0. AppStream
- AppStream Flotte 2.0: le flotte AppStream 2.0 o Image Builder sono ospitate nel VPC gestitoAWS. Ogni istanza AppStream 2.0 ha due Elastic Network Interface (ENI). L'interfaccia principale (`eth0`) viene utilizzata per scopi di gestione e intermediazione della connessione dell'utente finale all'istanza tramite il gateway di streaming. L'interfaccia secondaria (`eth1`) viene inserita nel Customer-VPC e può essere utilizzata per accedere ad altre risorse nel VPC personalizzato o in locale.

## Scenario 1: Active Directory Domain Services (ADDS) distribuito in locale

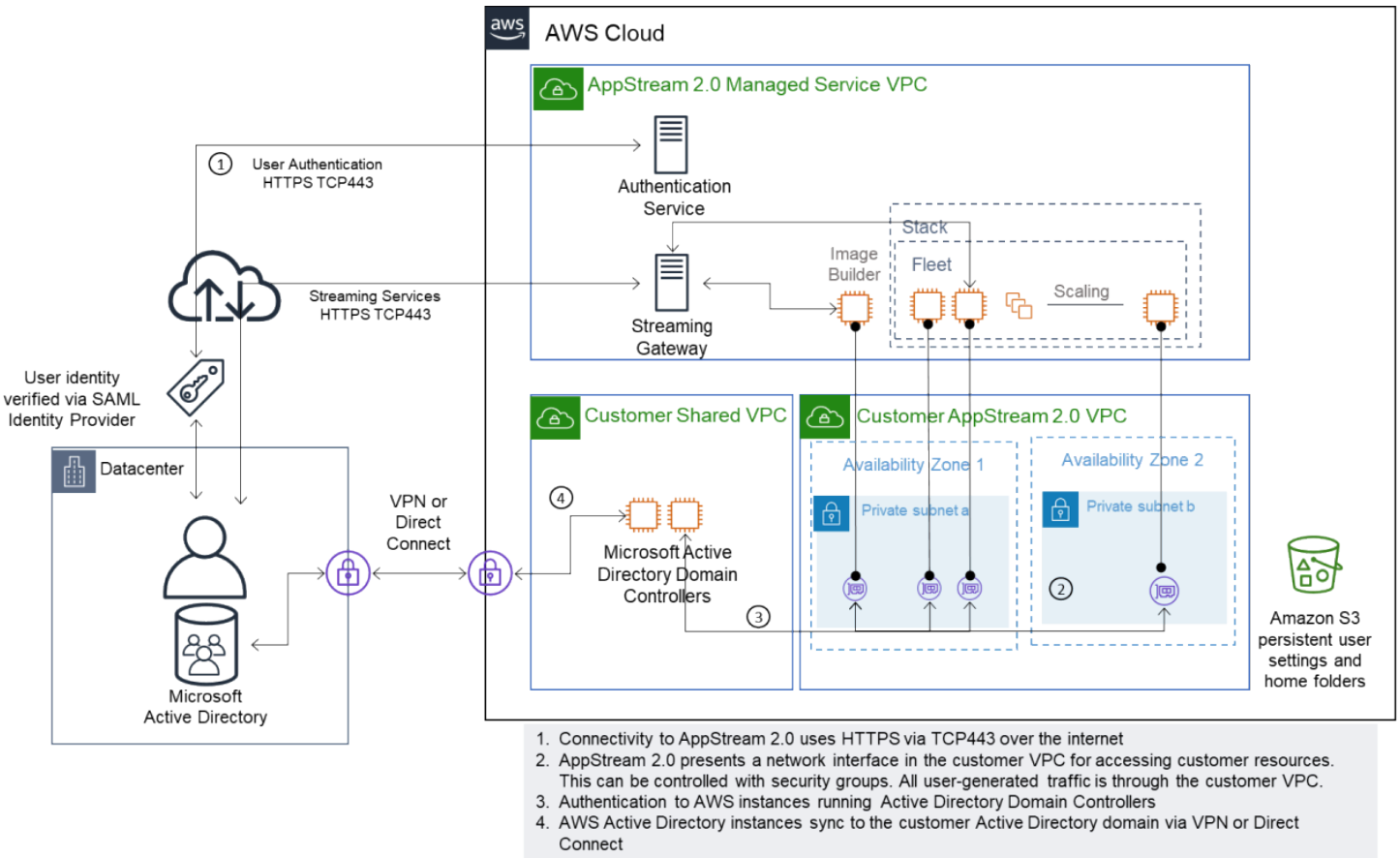
Tutto il traffico di autenticazione attraversa la connessione VPN o Direct Connect dal VPC del cliente al gateway del cliente. Il vantaggio di questo scenario è il vantaggio di utilizzare un ambiente AD probabilmente già distribuito senza dover fornire controller di dominio aggiuntivi nel VPC del cliente. Lo svantaggio è l'unica dipendenza dalla VPN o da Direct Connect per autenticare e autorizzare gli utenti della flotta 2.0. AppStream In caso di problemi di connettività di rete, la flotta AppStream 2.0 o gli Image Builders ne risentirebbero direttamente. Fornire due tunnel VPN o connessioni Direct Connect con percorsi diversi mitiga questo rischio potenziale.




Scenario 1: Active Directory Domain Services (ADDS) distribuito in locale

## Scenario 2: estensione di Active Domain Services (ADDS) nel AWS VPC del cliente

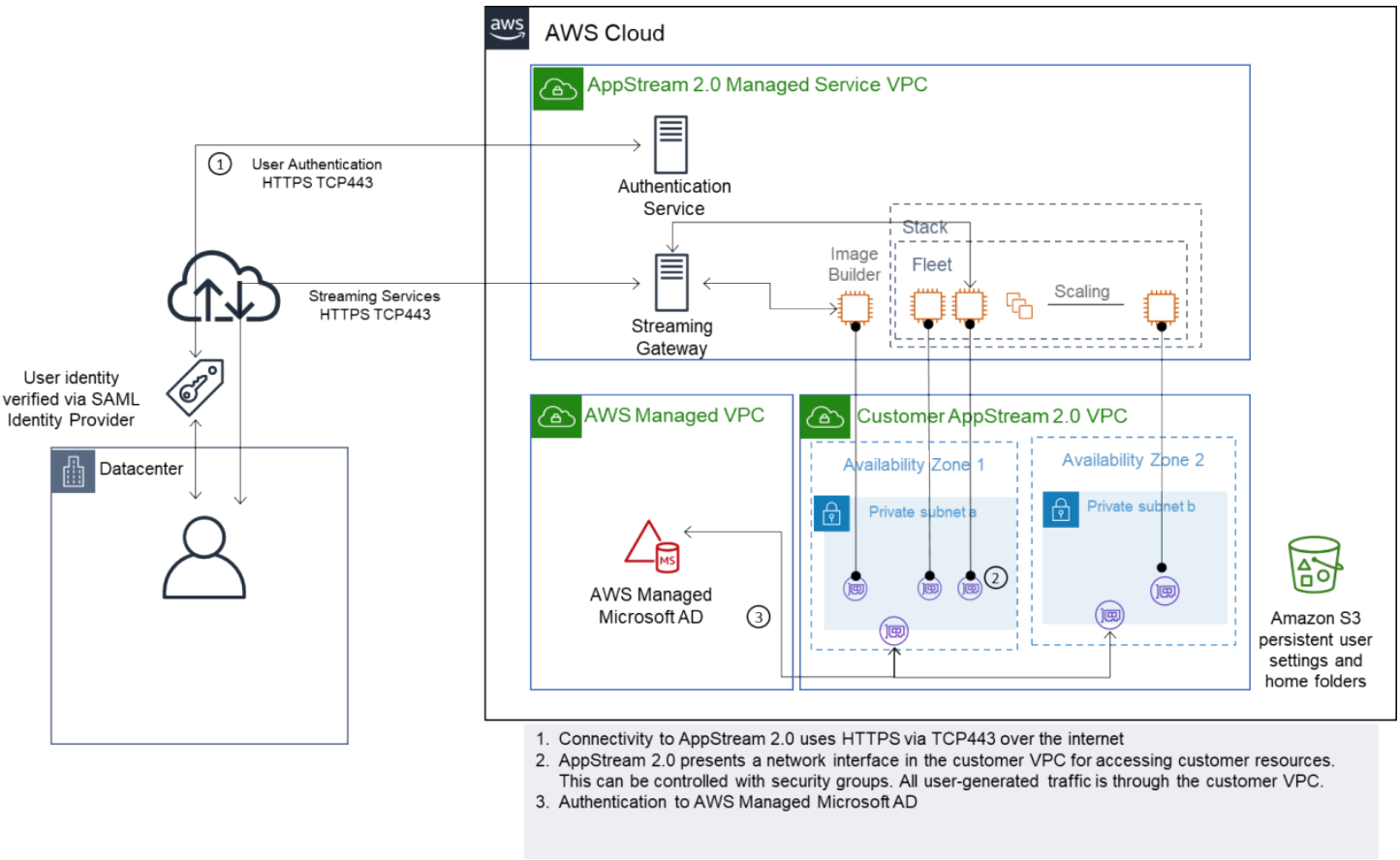
Active Directory è esteso al VPC del cliente. È necessario creare un sito Active Directory per i nuovi controller di dominio nel VPC del cliente. Il traffico di autenticazione viene indirizzato ai controller di dominio nel AWS VPC del cliente anziché attraversare la connessione VPN o Direct Connect.




Scenario 2 — Estendere Active Domain Services nel AWS cloud privato virtuale del cliente

## Scenario 3: Microsoft Active Directory AWS gestita

AWSMicrosoft AD gestito viene distribuito e utilizzato come dominio di identità Cloud AWS e risorse per le flotte AppStream 2.0 e gli Image Builder.




Scenario 3 — Active AWS Directory gestita

# Topologia del sito di Active Directory Service

La topologia del sito di servizio Active Directory è una rappresentazione logica della rete fisica.

La topologia del sito consente di indirizzare in modo efficiente le query dei client e il traffico di replica di Active Directory. Una topologia del sito ben progettata e gestita aiuta l'organizzazione a ottenere i seguenti vantaggi:

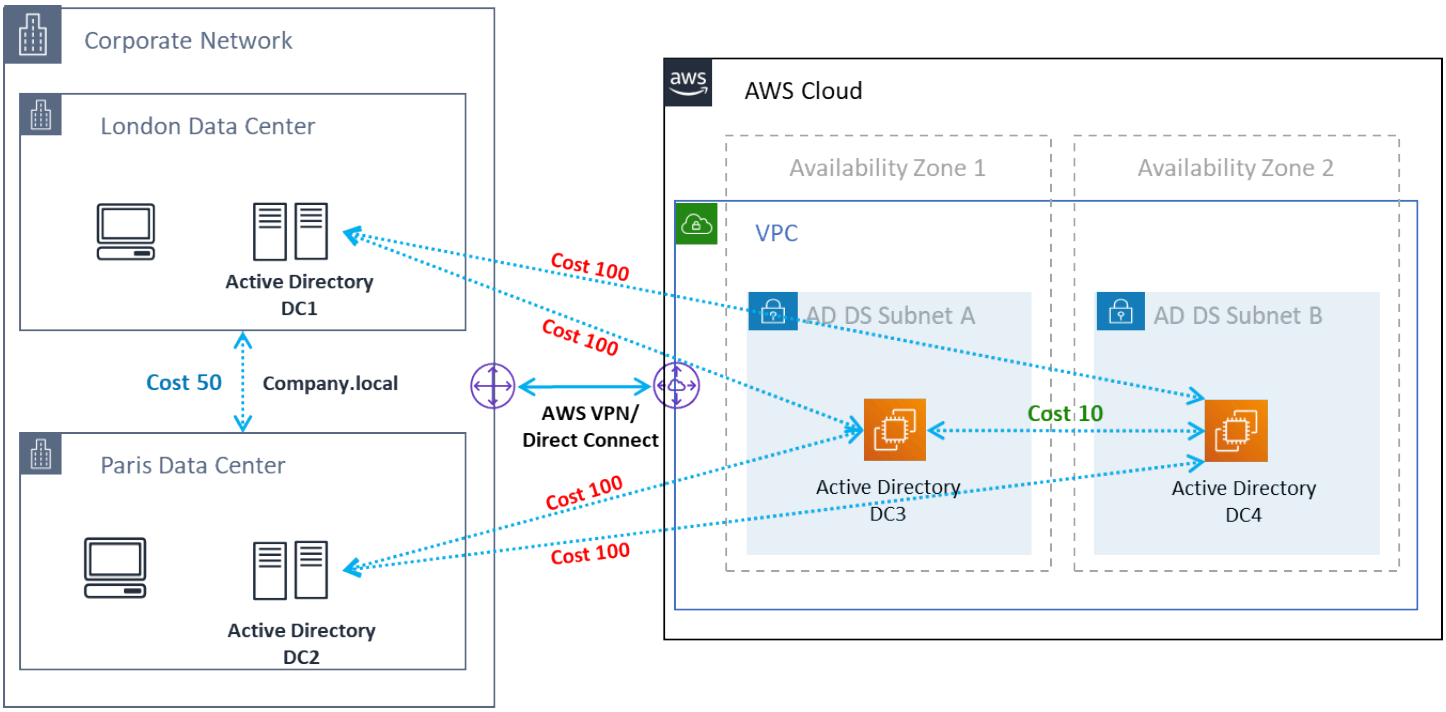
- Riduci al minimo il costo della replica dei dati di Active Directory durante la sincronizzazione tra sistemi locali e. Cloud AWS
- Ottimizza la capacità dei computer client di individuare le risorse più vicine, come i controller di dominio. Questo aiuta a ridurre il traffico di rete su collegamenti WAN (Wide Area Network) lenti, a migliorare i processi di accesso e disconnessione e ad accelerare le operazioni di accesso alle risorse.

Quando introduci i servizi AppStream 2.0, assicurati che gli intervalli di indirizzi utilizzati per le sottoreti delle istanze AppStream 2.0 siano assegnati al sito corretto per il tuo ambiente.

Per lo Scenario 1 e lo Scenario 2, i siti e i servizi sono componenti fondamentali per la migliore esperienza utente in termini di tempi di accesso e tempo di accesso alle risorse Active Directory.

La topologia del sito controlla la replica di Active Directory tra i controller di dominio all'interno dello stesso sito e tra i confini dei siti.

La definizione della topologia corretta del sito garantisce l'affinità con i client, il che significa che i client (in questo caso, le istanze di streaming AppStream 2.0) utilizzano il controller di dominio locale preferito.




Siti e servizi Active Directory: affinità con i clienti

> **Tip**
>
> Come best practice, definisci costi elevati per i collegamenti di sito tra AD DS locali e il cloud AWS. La figura precedente è un esempio dei costi da assegnare ai collegamenti ai siti (costo 100) per garantire l'affinità dei client indipendentemente dal sito.

Per ulteriori informazioni sulla topologia del sito, fare riferimento a Progettazione della topologia del sito.

# Unità organizzative di Active Directory

AWS consiglia di archiviare le unità organizzative (OU) configurate in un singolo AppStream oggetto Directory Config 2.0. È consigliabile che ogni stack AppStream 2.0 abbia una propria unità organizzativa. Ciò consente la flessibilità necessaria per disporre di GPO specifici per stack. Assicuratevi che le unità organizzative siano dedicate agli oggetti informatici AppStream 2.0 per evitare di combinare policy AppStream specifiche della versione 2.0 con desktop locali. Prendi in considerazione l'utilizzo di unità organizzative secondarie per ciascuna Regione AWS delle quali distribuisci la versione 2.0. AppStream

# Pulizia degli oggetti del computer con Active Directory

AppStream Le istanze 2.0 sono effimere. Una flotta crea e riutilizza oggetti informatici di Active Directory man mano che le flotte si ridimensionano orizzontalmente e si espandono verso l'alto.

AWSconsiglia di creare un processo di pulizia AD per eliminare gli oggetti informatici obsoleti di Active Directory che possono esistere dopo la rimozione di un AppStream parco di oggetti.

# Sicurezza

La sicurezza cloud di Amazon Web Services (AWS) è la priorità più alta. Sicurezza e conformità sono una responsabilità condivisa tra AWS e il cliente. Per ulteriori informazioni, fare riferimento al Modello di responsabilità condivisa. In qualità di cliente AWS e AppStream 2.0, è importante implementare misure di sicurezza su diversi livelli come stack, fleet, image e networking.

A causa della sua natura effimera, la AppStream versione 2.0 viene spesso preferita come soluzione sicura per la distribuzione di applicazioni e desktop. Valuta se le soluzioni antivirus comuni nelle distribuzioni di Windows sono pertinenti nei casi d'uso per un ambiente predefinito ed eliminato alla fine di una sessione utente. L'antivirus aggiunge un sovraccarico alle istanze virtualizzate, quindi è una best practice per mitigare le attività non necessarie. Ad esempio, la scansione del volume di sistema (che è temporaneo) all'avvio, ad esempio, non aumenta la sicurezza complessiva della versione 2.0. AppStream

Le due domande chiave per la sicurezza AppStream 2.0 sono incentrate su:

- La persistenza dello stato utente oltre la sessione è un requisito?
- Quanto accesso deve avere un utente all'interno di una sessione?

# Protezione dei dati persistenti

Le implementazioni della AppStream versione 2.0 possono richiedere che lo stato dell'utente persista in qualche modo. Potrebbe trattarsi di rendere persistenti i dati per singoli utenti o di rendere persistenti i dati per la collaborazione utilizzando una cartella condivisa. AppStreamLo storage di istanze 2.0 è temporaneo e non prevede alcuna opzione di crittografia.

AppStream 2.0 fornisce la persistenza dello stato utente tramite le cartelle home e le impostazioni delle applicazioni in Amazon S3. Alcuni casi d'uso richiedono un maggiore controllo sulla persistenza dello stato utente. Per questi casi d'uso, AWS consiglia di utilizzare una condivisione di file Server Message Block (SMB).

## Stato e dati dell'utente

Poiché la maggior parte delle applicazioni Windows offre prestazioni migliori e più sicure se collocate insieme ai dati delle applicazioni creati dall'utente, è consigliabile mantenere questi dati all'interno delle Regione AWS stesse flotte di applicazioni AppStream 2.0. La crittografia di questi dati è una

procedura consigliata. Il comportamento predefinito della cartella home dell'utente consiste nel crittografare file e cartelle inattivi utilizzando chiavi di crittografia gestite da Amazon S3 dai servizi di gestione delle AWS chiavi (). AWS KMS È importante notare che gli utenti AWS amministrativi con accesso alla AWS console o al bucket Amazon S3 potranno accedere direttamente a tali file.

Nei progetti che richiedono un target Server Message Block (SMB) proveniente da una condivisione di file di Windows per archiviare file e cartelle utente, il processo è automatico o richiede una configurazione.

Tabella 5 — Opzioni per la protezione dei dati degli utenti

| Obiettivo SMB | E ncryption-at-rest | E ncryption-in-transit | Antivirus (AV) |
|---|---|---|---|
| FSx per File Server Windows | Automatico tramite KMS AWS | Automatico tramite crittografia SMB | L'AV installato su un'istanza remota esegue la scansione sull'unità mappata |
| Gateway di file, Gateway AWS di archiviazione | Per impostazione predefinita, tutti i dati archiviati da AWS Storage Gateway S3 sono crittogra fati lato server con Amazon S3 Managed Encryptio n Keys (SSE-S3). Facoltativamente, puoi configurare diversi tipi di gateway per crittografare i dati archiviati con (KMS) AWS Key Management Service | Tutti i dati trasferiti tra qualsiasi tipo di dispositivo gateway e AWS storage sono crittografati tramite SSL. | L'AV installato su un'istanza remota esegue la scansione sull'unità mappata |
| File server Windows basati su EC2 | Abilita la crittografia EBS | PowerShell; `Set-SmbServer Configuration` | L'AV installato sul server esegue la scansione sulle unità locali |

| Obiettivo SMB | E ncryption-at-rest | E ncryption-in-transit | Antivirus (AV) |
| --- | --- | --- | --- |
| | | `- EncryptData $True` | |

# Sicurezza degli endpoint e antivirus

La breve natura effimera delle istanze Amazon AppStream 2.0 e la mancanza di persistenza dei dati richiedono un approccio diverso per garantire che l'esperienza utente e le prestazioni non siano compromesse da attività che sarebbero necessarie su un desktop persistente. Gli agenti di Endpoint Security vengono installati in immagini AppStream 2.0 quando esiste una politica organizzativa o quando vengono utilizzati con dati esterni, ad esempio e-mail, ingresso di file, navigazione Web esterna.

## Rimozione di identificatori univoci

Gli agenti di Endpoint Security possono avere un identificatore univoco globale (GUID) che deve essere reimpostato durante il processo di creazione del parco istanze. I fornitori dispongono di istruzioni sull'installazione dei loro prodotti nelle immagini che assicureranno la generazione di un nuovo GUID per ogni istanza generata da un'immagine.

Per garantire che il GUID non venga generato, installa l'agente Endpoint Security come ultima azione prima di eseguire l'Assistente AppStream 2.0 per generare l'immagine.

## Ottimizzazione delle prestazioni

I fornitori di Endpoint Security forniscono switch e impostazioni che ottimizzano le prestazioni della versione 2.0. AppStream Le impostazioni variano da un fornitore all'altro e sono disponibili nella relativa documentazione, in genere in una sezione dedicata alla VDI. Alcune impostazioni comuni includono, a titolo esemplificativo ma non esaustivo:

- Disattiva le scansioni di avvio per garantire che i tempi di creazione, avvio e accesso delle istanze siano ridotti al minimo
- Disattiva le scansioni pianificate per evitare scansioni non necessarie
- Disattiva le cache delle firme per impedire l'enumerazione dei file
- Abilita le impostazioni IO ottimizzate per VDI
- Esclusioni richieste dalle applicazioni per garantire le prestazioni

I fornitori di sicurezza degli endpoint forniscono istruzioni per l'uso con ambienti desktop virtuali che ottimizzano le prestazioni.

- Supporto Trend Micro Office Scan per l'infrastruttura desktop virtuale - Apex One/ OfficeScan (trendmicro.com)
- CrowdStrike e come installare Falcon nel CrowdStrike data center
- Sophos e Sophos Central Endpoint: Come eseguire l'installazione su un'immagine gold per evitare identità duplicate e Sophos Central: best practice per l'installazione di Windows Endpoint in ambienti desktop virtuali
- McAfee e il provisioning e la distribuzione degli McAfee agenti su sistemi di infrastruttura desktop virtuale
- Microsoft Endpoint Security e configurazione di Microsoft Defender Antivirus per macchine VDI non persistenti - Microsoft Tech Community

## Esclusioni dalla scansione

Se il software di sicurezza è installato in istanze AppStream 2.0, il software di sicurezza non deve interferire con i seguenti processi.

Tabella 6 — AppStream 2.0 Il software di sicurezza dei processi non deve interferire con i seguenti processi.

| Servizio | Processes |
| --- | --- |
| AmazonCloudWatchAgent | "C:\Program Files\ Amazon\AmazonCloud WatchAgent\ start-amazon- cloudwatch-agent.exe» |
| AmazonSSMagent | «C:\Program Files\ Amazon\ SSM\ .exe» amazon-ssm-agent |
| BEL DCV | "C:\Program Files\ NICE\ DCV\ Server\ bin\ dcvserver.exe» "C:\Program Files\ NICE\ DCV\ Server\ bin\ dcvagent.exe» |
| AppStream 2.0 | «C:\ProgramFiles\ Amazon\ AppStream 2\StorageConnector\ StorageConnector .exe» |

| Servizio | Processes |
| --- | --- |
| | Nella cartella "C:\Program Files\ Amazon\ Photon\»<br><br>». \ Agente\ PhotonAgent .exe»<br><br>». \WebServer\ PhotonAgentWebServer .exe»<br><br>». \CustomShell\ PhotonWindowsAppSw itcher .exe»<br><br>». \CustomShell\ PhotonWindowsCusto mShell .exe»<br><br>». \CustomShell\ PhotonWindowsCusto mShellBackground .exe» |

## Cartelle

Se il software di sicurezza è installato in istanze AppStream 2.0, il software non deve interferire con le seguenti cartelle:

Example

```
C:\Program Files\Amazon\*
C:\ProgramData\Amazon\*
C:\Program Files (x86)\AWS Tools\*
C:\Program Files (x86)\AWS SDK for .NET\*
C:\Program Files\NICE\*
C:\ProgramData\NICE\*
C:\AppStream\*
C:\Program Files\Internet Explorer\*
C:\Program Files\nodejs\
```

## Igiene della console di sicurezza degli endpoint

Amazon AppStream 2.0 creerà nuove istanze uniche ogni volta che un utente si connette oltre i timeout di inattività e disconnessione. Le istanze avranno un nome univoco e verranno inserite nelle condoglianze relative alla gestione della sicurezza degli endpoint. L'impostazione dell'eliminazione delle macchine obsolete non utilizzate più vecchie di 4 o più giorni (o meno a seconda dei timeout delle sessioni AppStream 2.0) ridurrà al minimo il numero di istanze scadute nella console.

# Esclusioni di rete

L'intervallo della rete di gestione AppStream 2.0 (`198.19.0.0/16`) e le porte e gli indirizzi seguenti non devono essere bloccati da alcuna soluzione di sicurezza/firewall o antivirus all'interno delle istanze AppStream 2.0.

Tabella 7 — Il software di sicurezza delle porte delle istanze di streaming AppStream 2.0 non deve interferire con

| Porta | Utilizzo |
| --- | --- |
| 8300, 3128 | Viene utilizzato per stabilire la connessione di streaming |
| 8000 | Viene utilizzato per gestire l'istanza di streaming entro AppStream la versione 2.0 |
| 8443 | Viene utilizzato per gestire l'istanza di streaming entro AppStream la versione 2.0 |
| 5.3 | DNS |

Tabella 8 — AppStream 2.0 indirizzi dei servizi gestiti con cui il software di sicurezza non deve interferire

| Porta | Utilizzo |
| --- | --- |
| 169.254.169123 | NTP |
| 169,254,169,249 | Servizio di licenza NVIDIA GRID |

| Porta | Utilizzo |
| --- | --- |
| 169,254,169,250 | KMS |
| 169,254,169,251 | KMS |
| 169,254,169,253 | DNS |
| 169,254,169,254 | Metadati |

# Proteggere una sessione AppStream

## Limitazione dei controlli delle applicazioni e del sistema operativo

AppStream 2.0 offre all'amministratore la possibilità di specificare esattamente quali applicazioni possono essere avviate dalla pagina Web in modalità streaming delle applicazioni. Tuttavia, ciò non garantisce che possano essere eseguite solo le applicazioni specificate.

Le utilità e le applicazioni di Windows possono essere avviate tramite il sistema operativo con mezzi aggiuntivi. AWSconsiglia di utilizzare Microsoft AppLocker per garantire che possano essere eseguite solo le applicazioni richieste dall'organizzazione. Le regole predefinite devono essere modificate, in quanto garantiscono a tutti l'accesso tramite percorsi alle directory di sistema critiche.

> **Note**
>
> Windows Server 2016 e 2019 richiedono l'esecuzione del servizio Windows Application Identity per applicare le regole AppLocker . L'accesso alle applicazioni dalla AppStream versione 2.0 tramite Microsoft AppLocker è descritto in dettaglio nella Guida per l'AppStream amministratore.

Per le istanze del parco istanze unite a un dominio Active Directory, utilizza Group Policy Objects (GPO) per fornire impostazioni utente e di sistema per proteggere l'accesso alle applicazioni e alle risorse degli utenti.

# Firewall e routing

Quando si crea una flotta AppStream 2.0, è necessario assegnare sottoreti e un gruppo di sicurezza. Le sottoreti hanno assegnazioni esistenti di elenchi di controllo dell'accesso alla rete (NACL) e tabelle di routing. È possibile associare fino a cinque gruppi di sicurezza durante l'avvio di un nuovo generatore di immagini o durante la creazione di una nuova flotta. I gruppi di sicurezza possono avere fino a cinque assegnazioni tra i gruppi di sicurezza esistenti. Per ogni gruppo di sicurezza, aggiungi regole che controllano il traffico di rete in uscita e in entrata da e verso le tue istanze

Un NACL è un livello di sicurezza opzionale per il tuo VPC che funge da firewall stateless per controllare il traffico in entrata e in uscita da una o più sottoreti. Si possono impostare liste di controllo accessi di rete con regole simili a quelle del gruppo di sicurezza, in modo tale da aggiungere un ulteriore livello di sicurezza al VPC. Per ulteriori informazioni sulle differenze tra gruppi di sicurezza e ACL di rete, consulta la pagina di confronto tra gruppi di sicurezza e NACL.

Quando progetti e applichi le regole Security Group e NACL, prendi in considerazione le best practice di AWS Well-Architected per il privilegio minimo. Il privilegio minimo è un principio che prevede la concessione solo delle autorizzazioni necessarie per completare un'attività.

Per i clienti che dispongono di una rete privata ad alta velocità che collega il proprio ambiente locale ad AWS (tramite AWS Direct Connect), potresti prendere in considerazione l'utilizzo degli endpoint VPC per AppStream, il che significa che il traffico di streaming verrà instradato tramite la connettività di rete privata anziché attraverso la rete Internet pubblica. Per ulteriori informazioni su questo argomento, consulta la sezione Endpoint VPC con interfaccia di streaming AppStream 2.0 di questo documento.

# Prevenzione della perdita di dati

Esamineremo due tipi di prevenzione della perdita di dati.

## Controlli per il trasferimento dei dati da istanza Client a AppStream 2.0

Tabella 9 — Linee guida per il controllo dell'ingresso e dell'uscita dei dati

| Impostazione | Opzioni | Guida |
| --- | --- | --- |
| Appunti | • Copia e incolla solo nella sessione remota | La disabilitazione di questa impostazione non disabilita il |

| Impostazione | Opzioni | Guida |
| --- | --- | --- |
| | • Copia solo su dispositivo locale<br>• Disabilitato | copia e incolla all'interno della sessione. Se è necessario copiare i dati nella sessione, scegliete Incolla solo nella sessione remota per ridurre al minimo il rischio di perdita di dati. |
| Trasferimento di file | • Caricare e scaricare<br>• Solo caricamento<br>• Solo download<br>• Disabilitato | Evita di abilitare questa impostazione per prevenire la perdita di dati. |
| Stampa su dispositivo locale | • Abilitato<br>• Disabilitato | Se è necessaria la stampa, utilizzate stampanti mappate di rete controllate e monitorate dall'organizzazione. |

Considerate i vantaggi della soluzione esistente per il trasferimento dei dati organizzativi rispetto alle impostazioni dello stack. Queste configurazioni non sono progettate per sostituire una soluzione completa e sicura per il trasferimento dei dati.

## Controllo del traffico in uscita dall'istanza 2.0 AppStream

Se la perdita di dati è un problema, è importante nascondere a cosa può accedere un utente una volta entrato nella propria istanza AppStream 2.0. Che aspetto ha il percorso di uscita (o uscita) della rete? La disponibilità dell'accesso pubblico a Internet per l'utente finale all'interno dell'istanza AppStream 2.0 è un requisito comune, pertanto è necessario prendere in considerazione l'inserimento di una WebProxy o più soluzioni di filtraggio dei contenuti nel percorso di rete. Altre considerazioni includono un'applicazione antivirus locale e altre misure di sicurezza degli endpoint all'interno dell' AppStream istanza (per ulteriori informazioni, consulta la sezione «Endpoint Security and Antivirus»).

# Utilizzo dei servizi AWS

## AWS Identity and Access Management

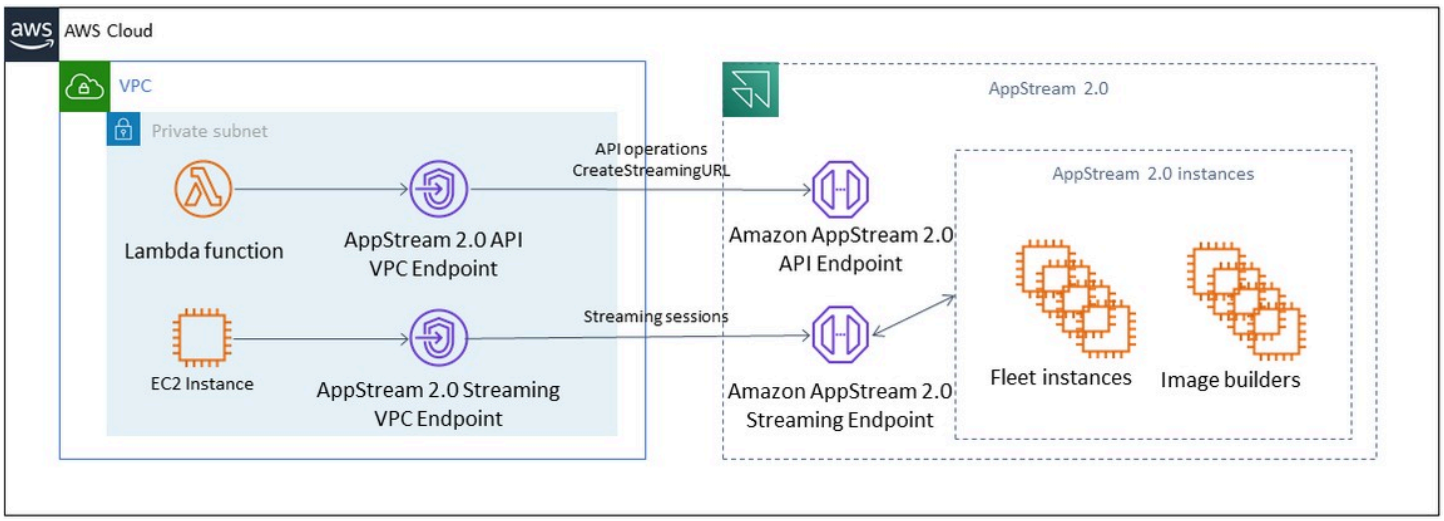
L'utilizzo di un ruolo IAM per accedere ai AWS servizi e la specificità della policy IAM ad esso associata è una best practice che consente l'accesso solo agli utenti delle sessioni AppStream 2.0 senza dover gestire credenziali aggiuntive. Segui le best practice per l'utilizzo di IAM Roles con AppStream 2.0.

Crea policy IAM per proteggere i bucket Amazon S3 creati per rendere persistenti i dati utente sia nelle cartelle home che nella persistenza delle impostazioni delle applicazioni. Ciò impedisce l'accesso agli amministratori non AppStream 2.0.

## Endpoint VPC

Un endpoint VPC consente connessioni private tra il VPC e i servizi AWS supportati e i servizi di endpoint VPC basati su AWS PrivateLink. AWS PrivateLink è una tecnologia che consente di accedere privatamente ai servizi tramite indirizzi IP privati. Il traffico tra il VPC e gli altri servizi non lascia la rete Amazon. Se l'accesso pubblico a Internet è richiesto solo per AWS i servizi, gli endpoint VPC eliminano completamente il requisito dei gateway NAT e dei gateway Internet.

Negli ambienti in cui le routine di automazione o gli sviluppatori richiedono di effettuare chiamate API per la AppStream versione 2.0, crea un endpoint VPC di interfaccia AppStream per le operazioni API 2.0. Ad esempio, se sono presenti istanze EC2 in sottoreti private senza accesso pubblico a Internet, è possibile utilizzare un endpoint VPC per l'API AppStream 2.0 per AppStream richiamare operazioni API 2.0 come l'URL. CreateStreaming Il diagramma seguente mostra un esempio di configurazione in cui gli endpoint API AppStream 2.0 e VPC di streaming vengono utilizzati dalle funzioni Lambda e dalle istanze EC2.




## Endpoint VPC

L'endpoint VPC di streaming consente di trasmettere sessioni tramite un endpoint VPC. L'endpoint dell'interfaccia di streaming gestisce il traffico di streaming all'interno del VPC. Il traffico in streaming include pixel, USB, input utente, audio, appunti, caricamento e download di file e traffico di stampanti. Per utilizzare l'endpoint VPC, l'impostazione dell'endpoint VPC deve essere abilitata nello stack 2.0. AppStream Ciò rappresenta un'alternativa allo streaming di sessioni utente sulla rete Internet pubblica da postazioni con accesso limitato a Internet e che trarrebbero vantaggio dall'accesso tramite un'istanza Direct Connect. Lo streaming delle sessioni utente tramite un endpoint VPC richiede quanto segue:

- I gruppi di sicurezza associati all'endpoint di interfaccia devono consentire l'accesso in entrata alla porta `443` (TCP) e alle porte `1400-1499` (TCP) dall'intervallo di indirizzi IP da cui gli utenti si connettono.
- L'elenco di controllo dell'accesso alla rete per le sottoreti deve consentire il traffico in uscita dalle porte di rete temporanee `1024-65535` (TCP) all'intervallo di indirizzi IP da cui gli utenti si connettono.
- La connettività Internet è necessaria per autenticare gli utenti e fornire le risorse Web necessarie alla versione 2.0 per funzionare. AppStream

Per ulteriori informazioni sulla limitazione del traffico ai AWS servizi con la AppStream versione 2.0, consulta la guida amministrativa per la creazione e lo streaming da endpoint VPC.

Quando è richiesto l'accesso pubblico completo a Internet, è consigliabile disattivare Internet Explorer Enhanced Security Configuration (ESC) su Image Builder. Per ulteriori informazioni, consulta la guida

all'amministrazione AppStream 2.0 per disabilitare la configurazione di sicurezza avanzata di Internet Explorer.

# Ripristino di emergenza

Amazon AppStream 2.0 ha una ridondanza integrata in un massimo di tre zone di disponibilità. Ciò significa che se un utente ha una sessione attiva in una zona di disponibilità che si deteriora, può semplicemente disconnettersi e riconnettersi, per riservargli una sessione in una zona di disponibilità integra, a patto che la capacità sia disponibile. Sebbene ciò offra un'elevata disponibilità all'interno della regione, non fornisce una soluzione di disaster recovery se il servizio presenta problemi a livello regionale.

Per fornire un piano di disaster recovery per gli utenti della AppStream versione 2.0, è innanzitutto necessario creare un ambiente AppStream 2.0 nella regione secondaria. Dal punto di vista della progettazione, questo ambiente dovrebbe avere connessioni ridondanti all'ambiente locale, se applicabile, e non dovrebbe dipendere dalla regione principale. Ad esempio, se il parco macchine AppStream 2.0 appartiene al dominio, è necessario disporre di controller di dominio aggiuntivi nella regione secondaria con Siti e servizi configurati. Da una prospettiva AppStream 2.0, questo ambiente dovrebbe includere le stesse impostazioni di flotta e stack presenti nella regione principale. La flotta stessa dovrebbe eseguire la stessa immagine di base, che può essere copiata nella regione secondaria tramite la console o a livello di programmazione. Se le applicazioni eseguite nelle sessioni AppStream 2.0 hanno una dipendenza dal backend legata alla regione principale, anche questa dovrebbe avere una ridondanza regionale per garantire che gli utenti possano continuare ad accedere al backend dell'applicazione se la regione primaria non funziona. I limiti del livello di servizio nella regione di destinazione devono corrispondere alla regione principale.

# Routing delle identità

Esistono due metodi distinti per fornire l'accesso alle applicazioni in uno scenario di DR. Ad un livello elevato, i due metodi differiscono in base al modo in cui gli utenti vengono indirizzati alla regione di failover. Il primo metodo viene eseguito con una singola configurazione dell'applicazione AppStream 2.0 nell'IdP e il secondo metodo prevede due configurazioni di applicazione separate.

## Metodo 1: modifica dello stato di inoltro dell'applicazione

Quando gli utenti accedono alla AppStream versione 2.0 da un Identity Provider (IdP), dopo l'autenticazione vengono inoltrati a un URL specifico che si allinea alla regione e allo stack a cui devono avere accesso. Per ulteriori informazioni sull'URL Relay State, consulta la Amazon 2.0 Administration Guide. AppStream L'amministratore può configurare uno stack interregionale basato

sulla stessa immagine AppStream 2.0 della regione principale su cui gli utenti possano effettuare il failover. L'amministratore può controllare questo failover semplicemente aggiornando l'URL Relay State in modo che punti allo stack di failover. Affinché questo metodo funzioni correttamente, le policy IAM associate dovranno riflettere l'accesso a entrambi gli stack, primario e di failover. Per maggiori dettagli su come devono essere configurate queste policy IAM, consulta la seguente policy di esempio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
            "Resource": [
            "arn:aws:appstream:PrimaryRegion:190836837966:stack/StackName",
            "arn:aws:appstream:FailoverRegion:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

## Metodo 2: configurazione di due applicazioni AppStream 2.0 all'interno del tuo IdP

Questo metodo richiede all'amministratore di creare due applicazioni separate per AppStream 2.0 all'interno dell'IdP. Possono quindi presentare entrambe le applicazioni e consentire all'utente di scegliere dove andare, oppure bloccare/nascondere un'applicazione fino al momento del failover. Questo metodo è più adatto al caso d'uso in cui gli utenti globali si spostano spesso. Questi utenti devono eseguire lo streaming dall'endpoint più vicino, pertanto l'assegnazione di entrambe le applicazioni offre loro la possibilità di scegliere l'applicazione configurata per la regione più vicina. Questa operazione può anche essere automatizzata, per maggiori informazioni consulta questo post del blog.

# Persistenza dello storage

Quando si sfruttano le funzionalità di persistenza dei dati incluse nella AppStream versione 2.0, come Application Persistence e Home Folder Synchronization, sarà necessario replicare tali dati nella regione di failover. Queste funzionalità archiviano i dati persistenti in un bucket Amazon S3 nella regione 2.0 specificata AppStream. Per far sì che i dati persistano in tutte le regioni, sarà necessario replicare tutte le modifiche sul bucket di origine nel bucket delle regioni di failover 2.0. AppStream Questa operazione può essere eseguita con funzionalità native di Amazon S3, come la replica interregionale di Amazon S3. I dati persistenti di ogni utente risiederanno in una cartella contenente il suo nome utente con hash. Poiché al nome utente verrà applicato l'hash nella stessa area geografica, la semplice replica dei dati garantirà la persistenza dei dati nella regione secondaria. Per ulteriori informazioni sui bucket Amazon S3 utilizzati dalla AppStream versione 2.0, consulta questa guida.

# Monitoraggio

## Utilizzo dei pannelli di controllo

Il monitoraggio dell'utilizzo della flotta è un'attività regolare che può essere eseguita tramite CloudWatch metriche e la creazione di una dashboard. In alternativa, dalla console AppStream 2.0, utilizza la scheda Fleet Usage. Monitora regolarmente l'utilizzo della flotta, poiché il comportamento degli utenti non è sempre prevedibile e la domanda può superare anche una pianificazione iniziale di prim'ordine. Un elenco completo delle metriche e delle dimensioni della AppStream versione 2.0 è disponibile nella guida all'amministrazione della AppStream versione 2.0 in Monitoring Resources. CloudWatch

## Anticipazione della crescita

Ogni volta che si verifica un grande salto`PendingCapacity`, si verifica un evento di auto scaling. È importante confermarlo `AvailableCapacity` e `PendingCapacity` mantenere una relazione inversa man mano che nuove istanze della flotta AppStream 2.0 saranno disponibili per ospitare le sessioni utente. Crea un CloudWatch allarme per ogni flotta AppStream 2.0 `InsufficientCapacityError` per avvisare gli amministratori e garantire che la scalabilità automatica non sia inferiore alla domanda.

Se la domanda supera la capacità e i valori `InsufficientCapacityError` metrici sono comuni, prendi in considerazione l'idea di aumentare la capacità minima attraverso una politica di scalabilità programmata per l'inizio della giornata lavorativa. Inoltre, disponi di una seconda politica di Scheduled Scaling per ridurre la capacità minima dopo che la domanda è stata soddisfatta. Tieni presente che la riduzione del valore della capacità minima non ha alcun impatto sulle sessioni esistenti. La riduzione della capacità minima prima della fine della giornata lavorativa consente effettivamente alla bilancia di funzionare come previsto, abbassando il valore di. `ActualCapacity` In questo modo si ottimizzano i costi.

Se la domanda è costantemente imprevedibile, utilizza la politica di scalabilità di Target Tracking per garantire che la flotta AppStream 2.0 sia adeguata `AvailableCapacity` a soddisfare la domanda determinando al contempo i modelli di utilizzo. Continua a monitorare poiché Target Tracking utilizza una percentuale del consumo della flotta. Con l'aumento del numero totale di istanze del parco istanze, il numero totale di istanze del parco istanze inutilizzate si moltiplica. Ciò può diventare uno spreco a meno che la capacità massima non sia impostata su un valore conservativo. Utilizza diversi

tipi di politiche di scalabilità (ad esempio, Scheduled e Target Tracking) per bilanciare l'affidabilità con l'ottimizzazione dei costi.

## Monitoraggio dell'utilizzo degli utenti

Monitoraggio degli utenti unici, in quanto ciò comporta un costo sotto forma di tariffe per gli utenti. Questo costo per gli utenti è dovuto alle licenze di accesso per abbonati (SAL) di Image Assistant (RDS). La valutazione degli utenti unici può essere eseguita tramite report dall'IdP, dove viene eseguita l'autenticazione, o tramite report sull'utilizzo.

I report sull'utilizzo vengono archiviati come `.csv` file separati nel bucket S3, che puoi scaricare e analizzare utilizzando strumenti di business intelligence (BI) di terze parti. Puoi analizzare i dati di utilizzo AWS senza scaricare i report o creare report su intervalli di date personalizzati senza concatenare più file. `.csv` Ad esempio, puoi utilizzare Amazon Athena e Amazon QuickSight per creare report e visualizzazioni personalizzati dei tuoi AppStream dati di utilizzo 2.0.

## Registrazione persistente dei registri degli eventi di applicazioni e Windows

Quando una sessione di istanza AppStream 2.0 è completa, l'istanza viene terminata. Ciò significa che tutti i registri degli eventi delle applicazioni e di Windows utilizzati nella sessione vengono persi. Se è necessario mantenere questi registri degli eventi di applicazioni e Windows, un metodo consiste nell'utilizzare Amazon Data Firehose per distribuirli in tempo reale a S3 ed eseguire ricerche con Amazon OpenSearch Service (Service). OpenSearch Se non si prevede che le query siano frequenti, per ottimizzare i costi, utilizza Amazon Athena per la ricerca anziché utilizzare Amazon Service. OpenSearch

## Controllo della rete e delle attività amministrative

Se non è già configurato, è consigliabile eseguire AWS CloudTrailla configurazione Account AWS con Amazon AppStream 2.0. Per controllare specificamente le chiamate all'API AppStream 2.0, utilizza la sorgente degli eventi di filtro con un valore di`appstream.amazonaws.com`.

Abilita i log di flusso VPC per controllare l'accesso alle risorse gestite dal cliente. I log di flusso VPC possono essere pubblicati in CloudWatch Logs per eseguire query quando è necessario il controllo.

Il monitoraggio dell'allocazione IP delle sottoreti è importante man mano che le flotte 2.0 crescono. AppStream Crea report sull'assegnazione degli IP eseguendo la CLI describe-subnets per

riportare gli indirizzi IP disponibili in ogni sottorete assegnata alle flotte. Assicuratevi che la vostra organizzazione disponga di una capacità di indirizzi IP sufficiente a soddisfare la domanda di tutte le flotte che operano alla massima capacità.

# Ottimizzazione dei costi

L'ottimizzazione dei costi si concentra sull'evitare costi non necessari. Gli argomenti chiave includono la comprensione e il controllo di dove vengono spesi i soldi e la scelta del numero più appropriato e corretto di tipi di risorse. Analizza la spesa nel tempo e la scalabilità per soddisfare le esigenze aziendali. Le seguenti risorse AppStream 2.0 sono a pagamento: pay-as-you-go

- Istanze con parco istanze Always-On
- Istanze con parco istanze on-demand
- Tariffa per le istanze interrotte On-Demand
- Istanze dello sviluppatore di immagini
- Commissioni per gli utenti

Per informazioni aggiornate sui prezzi, consulta il AWS sito Web per i prezzi di Amazon AppStream 2.0.

## Progettazione di implementazioni AppStream 2.0 efficienti in termini di costi

Il primo passo nella pianificazione e nella progettazione dell'implementazione AppStream 2.0 consiste nell'utilizzare un semplice strumento di determinazione dei prezzi per stimare le AWS tariffe di base relative all'utilizzo. Fornisci il numero totale di utenti, l'utilizzo simultaneo effettivo per ora, il tipo di istanza e l'utilizzo del parco veicoli e lo strumento di determinazione dei prezzi stima il prezzo per utente. Mostra anche i risparmi di prezzo stimati quando si utilizza una flotta On-Demand anziché una flotta Always-On.

I clienti apprezzano il modello di prezzo AppStream 2.0 che prevede il pagamento solo per le istanze fornite per soddisfare le esigenze di streaming degli utenti. Questo modello è diverso dagli ambienti di streaming delle applicazioni esistenti. Questi si basano in genere sulla fornitura di capacità di picco, anche durante le notti, i fine settimana e i giorni festivi, quando il carico è inferiore. Lo strumento prezzi di Amazon AppStream 2.0 fornisce solo una stima delle tariffe AWS relative all'utilizzo della AppStream versione 2.0 e non include eventuali imposte applicabili. Le tariffe effettive dipendono da una serie di fattori, incluso l'utilizzo effettivo dei servizi AWS.

Lo strumento di determinazione dei prezzi AppStream 2.0 viene fornito come foglio di calcolo Microsoft Excel o OpenOffice Calc che consente di inserire informazioni di base sulla flotta, quindi

fornisce una stima dei costi per l'ambiente AppStream 2.0 per flotte on-demand e sempre attive in base al modello di utilizzo. È possibile simulare i costi in base alle tendenze di utilizzo storiche o previste. Le flotte elastiche liberano l'amministratore dalla necessità di prevedere l'utilizzo, creare e mantenere politiche e immagini di scalabilità grazie a queste funzionalità integrate. Le flotte e le istanze elastiche che eseguono Amazon Linux 2 (tutti i tipi di flotte) vengono fatturate per la durata della sessione di streaming, in secondi, con un minimo di 15 minuti.

## Ottimizzazione dei costi con la scelta del tipo di istanza

Per le istanze Fleet e Image Builder, sono disponibili diverse famiglie e tipi di istanze tra cui scegliere per la propria applicazione.

Test con l'utente finale: il passaggio successivo consiste nel distribuire la flotta AppStream 2.0 a un gruppo di utenti pilota per i test e convalidare il tipo di istanza da noi scelto. È importante richiedere agli utenti pilota di testare tutti i loro flussi di lavoro regolari e pesanti per acquisire metriche relative a memoria, CPU e grafica in modo da poter acquisire metriche prestazionali di base. Il gruppo pilota deve contenere i vari ruoli utente che utilizzano l'applicazione per garantire che venga testata da più esperienze utente. Il test di accettazione degli utenti consente di raccogliere feedback sull'esperienza della sessione di streaming. Quando si crea o si aggiorna uno stack, è possibile utilizzare un URL di feedback personalizzato. Gli utenti vengono reindirizzati a questo URL dopo aver scelto il link Invia feedback per inviare feedback sulla loro esperienza di streaming dell'applicazione. In caso di problemi di prestazioni, utilizzate le metriche prestazionali di Windows per analizzare i vincoli relativi alle risorse. Ad esempio, se l'attuale tipo di istanza del parco istanze stream.standard.medium mostra un vincolo di risorse, aggiorna il tipo di istanza a stream.standard.large. Al contrario, se le metriche delle prestazioni mostrano livelli elevati di sottoutilizzo delle risorse, prendi in considerazione la possibilità di effettuare il downgrade del tipo di istanza.

## Ottimizzazione dei costi con la scelta del tipo di flotta

Quando creano una nuova flotta AppStream 2.0, gli sviluppatori devono scegliere un tipo di flotta Always On o On-Demand. Nella scelta del tipo di istanza dal punto di vista dei prezzi, è importante capire come la AppStream versione 2.0 gestisce le istanze del parco istanze. Per le flotte Always-On, le istanze del parco istanze rimangono in esecuzione. Pertanto, quando gli utenti cercano di eseguire lo streaming delle sessioni, le istanze Fleet sono sempre pronte per iniziare le sessioni di streaming.

Per le flotte On-Demand, dopo il lancio, le istanze del parco istanze vengono mantenute nello stato di interruzione. La tariffa per le istanze interrotte è inferiore alla tariffa per le istanze in esecuzione, il che può aiutare a ridurre i costi. Le istanze del parco istanze On-Demand devono essere avviate da

uno stato interrotto. Un utente deve attendere circa due minuti prima che la sessione di streaming sia disponibile.

Le flotte elastiche sono ottimi candidati per applicazioni autonome che possono essere installate su dischi rigidi virtuali salvati in un bucket Amazon Simple Storage Service (Amazon S3). Le flotte elastiche possono ridurre ulteriormente i costi in alcuni casi d'uso grazie alla fatturazione al secondo addebitata solo per la durata dello streaming. La tariffa è una funzione del tipo e delle dimensioni dell'istanza e del sistema operativo scelti al momento della creazione della flotta.

Se gli utenti finali necessitano di istanze del parco istanze durante l'orario lavorativo, è meglio mantenere le stesse sessioni di streaming. Questo perché le istanze del parco istanze vengono addebitate all'ora e ogni volta che inizia una nuova sessione di streaming, viene applicata un'altra tariffa per le istanze relative al parco istanze.

Tabella 10 — Confronto tra i AppStream tipi di flotta

| Tipo di flotta | Vantaggi | Considerazioni |
| --- | --- | --- |
| Sempre attivo | Minori tempi di attesa per le sessioni di streaming | Gli utenti pagano la tariffa oraria dell'istanza in quanto non è possibile mantenere le istanze in stato di arresto. |
| Su richiesta | Riduzione dei costi in quanto le istanze rimangono in stato di interruzione | Tempo di attesa più lungo per le sessioni di streaming |
| Elastic | La fatturazione al secondo può essere utile per i casi d'uso che presentano modelli di utilizzo sporadici per le applicazioni che possono essere installate su un disco rigido virtuale | Man mano che le dimension i del disco rigido virtuale dell'applicazione aumentano , il tempo necessario per montarlo su un'istanza di streaming può essere lungo |

AppStream 2.0 monitora l'utilizzo della flotta ed esegue regolazioni automatiche della capacità della flotta per soddisfare la domanda degli utenti al minor costo possibile. Le regolazioni della capacità vengono effettuate in base a politiche di scalabilità definite dall'utente, in base all'utilizzo corrente o in

base a una pianificazione. Esamina regolarmente le metriche di utilizzo della flotta per verificare che le politiche di scalabilità della flotta non abbiano livelli elevati di capacità inutilizzata.

## Policy di dimensionamento

Fleet Auto Scaling consente di ottimizzare le risorse della flotta evitando di impegnare eccessivamente le risorse in attesa che gli utenti effettuino l'accesso. Gli amministratori possono regolare le dimensioni della flotta in base a una varietà di utilizzo per soddisfare la domanda degli utenti. Utilizza CloudWatch AppStream 2.0 Fleet Metrics o strumenti di monitoraggio di terze parti per conoscere l'attività degli utenti e configurare politiche di scalabilità per espandere o ridurre le flotte AppStream 2.0 in base all'utilizzo previsto. I log degli utenti sono un meccanismo essenziale per comprendere l'utilizzo reale. Queste informazioni possono essere utilizzate per modificare dinamicamente le dimensioni della flotta in base all'Auto Scaling.

In molti casi, le flotte AppStream 2.0 vengono create in base al numero massimo di utenti e non adattate ai diversi momenti del giorno e della settimana, come le notti e i fine settimana. Spesso, il numero di utenti simultanei delle applicazioni in streaming è inferiore al numero totale di utenti, soprattutto quando gli utenti hanno la flessibilità necessaria per lavorare in remoto. È importante tenere in considerazione questi fattori durante la proiezione dei modelli di utilizzo. La sovrastima porta a un eccessivo approvvigionamento di istanze AppStream 2.0 con conseguenti costi aggiuntivi. Per ottenere una configurazione ottimale, potrebbe essere necessario combinare una o più politiche di scalabilità programmate con politiche di scalabilità orizzontale.

Per ulteriori informazioni sull'implementazione delle politiche di scalabilità, consulta Scaling your Amazon AppStream 2.0 flotte.

## Commissioni per gli utenti

Le tariffe per utente vengono addebitate per utente, al mese, per ogni utente in Regione AWS cui gli utenti eseguono lo streaming di applicazioni da una flotta di istanze AppStream 2.0. Invece di generare ID utente diversi, utilizza ID utente coerenti per gli utenti AppStream 2.0. Le tariffe per gli utenti non vengono addebitate per la connessione a Image Builder.

Le scuole, le università e alcuni istituti pubblici possono beneficiare di una tariffa utente ridotta di Microsoft RDS SAL pari a 0,44 USD per utente al mese. Per i requisiti di qualificazione, consulta le Condizioni e i documenti di licenza Microsoft.

Se disponi di Microsoft License Mobility, potresti avere diritto a portare le tue licenze Microsoft RDS Client Access (CAL) e utilizzarle con Amazon 2.0. AppStream Se sei coperto dalla tua licenza, non

dovrai sostenere costi utente mensili. Per ulteriori informazioni sulla possibilità di utilizzare le licenze Microsoft RDS CAL esistenti con Amazon AppStream 2.0, consulta la guida sulla mobilità delle AWS licenze o consulta il tuo rappresentante Microsoft per le licenze.

## Utilizzo di Image Builder

AppStream Le istanze 2.0 di Image Builder vengono addebitate ogni ora. Il costo dell'istanza di Image Builder include elaborazione, archiviazione e qualsiasi traffico di rete utilizzato dal protocollo di streaming. A tutte le istanze di Image Builder in esecuzione viene addebitata la tariffa applicabile per l'istanza in esecuzione. Questa tariffa si basa sul tipo e sulla dimensione dell'istanza, anche quando non è collegato alcun amministratore.

Come best practice per ottimizzare i costi, chiudi un'istanza di Image Builder quando non viene utilizzata. CloudWatch Le regole degli eventi possono essere utilizzate per pianificare un lavoro quotidiano, ad esempio richiamando una funzione Lambda per interrompere le istanze di Image Builder.

È possibile conservare l'immagine AppStream up-to-date 2.0 utilizzando gli aggiornamenti gestiti AppStream delle immagini 2.0. Questo metodo di aggiornamento fornisce gli ultimi aggiornamenti del sistema operativo Windows e gli aggiornamenti dei driver e il software dell'agente AppStream 2.0 più recente. Quando si utilizza questo metodo per aggiornare le immagini, un Image Builder viene avviato e interrotto automaticamente come parte del processo di servizio gestito.

# Conclusioni

Con la AppStream versione 2.0, puoi aggiungere facilmente le tue applicazioni desktop esistenti AWS e consentire agli utenti di trasmetterle in streaming all'istante. Gli utenti Windows possono utilizzare il client AppStream 2.0 o un browser Web compatibile con HTML5 per lo streaming delle applicazioni. Puoi mantenere una versione singola di ciascuna delle applicazioni, semplificandone la gestione. Gli utenti accederanno sempre alla versione più recente delle applicazioni. Le tue applicazioni vengono eseguite su risorse di AWS elaborazione e i dati non vengono mai archiviati sui dispositivi degli utenti, il che significa che ottengono sempre un'esperienza sicura e ad alte prestazioni.

A differenza delle tradizionali soluzioni locali per lo streaming di applicazioni desktop, AppStream offre pay-as-you-go prezzi, senza investimenti iniziali e senza infrastrutture da mantenere. Puoi scalare istantaneamente e a livello globale, assicurando che i tuoi utenti abbiano sempre un'esperienza eccezionale.

Amazon AppStream 2.0 è progettato per essere integrato nei sistemi e nei processi IT esistenti e questo white paper descrive le migliori pratiche per farlo. Il risultato del rispetto delle linee guida contenute in questo white paper è un'implementazione desktop cloud conveniente che può adattarsi in modo sicuro alla tua attività sull'infrastruttura globale. AWS

# Fattori determinanti

I contributori a questo documento includono:

- Andrew Wood, Architetto senior delle soluzioni, Amazon Web Services
- Andrew Morgan, specialista EUC SA, Amazon Web Services
- Arun PC, Senior EUC Specialist SA, Amazon Web Services
- Asriel Agronin, architetto senior delle soluzioni, Amazon Web Services
- Dustin Shelton, Senior EUC Specialist SA, Amazon Web Services
- Jeremy Schiefer, Architetto senior delle soluzioni, Amazon Web Services
- Navi Magee, Architetto principale delle soluzioni, Amazon Web Services
- Pete Fergus, ingegnere senior del supporto cloud, Amazon Web Services
- Phil Persson, principale specialista EUC SA, Amazon Web Services
- Richard Spaven, Senior EUC Specialist SA, Amazon Web Services
- Spencer DeBrosse, Architetto delle soluzioni senior, Amazon Web Services
- Stephen Stetler, architetto senior delle soluzioni, Amazon Web Services
- Taka Matsumoto, ingegnere senior del supporto cloud, Amazon Web Services
- Vasant Sirsat, Senior EUC Specialist SA, Amazon Web Services

# Approfondimenti

Per ulteriori informazioni, vedere:

- Guida all'amministrazione di Amazon AppStream 2.0
- Riferimento alle AppStream API Amazon
- Usa Amazon FSx for Windows File Server e FSLogix per ottimizzare la persistenza delle impostazioni delle applicazioni su Amazon 2.0 AppStream
- Monitoraggio di Amazon AppStream 2.0 con Amazon ElasticSearch e Amazon Firehose
- Analizza i report sull'utilizzo di Amazon AppStream 2.0 utilizzando Amazon Athena e Amazon QuickSight
- Espandi le tue flotte Amazon AppStream 2.0
- Utilizzo di Microsoft AppLocker per gestire l'esperienza delle applicazioni su Amazon AppStream 2.0
- Utilizzo di un dominio personalizzato con Amazon AppStream 2.0
- Come posso usare le mie CAL Microsoft RDS con AppStream 2.0?
- Strumento di determinazione dei prezzi Amazon AppStream 2.0
- Crea una versione di prova online del software con AppStream 2.0
- Crea un portale SaaS con Amazon 2.0 AppStream

# Revisioni del documento

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed RSS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Documento aggiornato | Aggiornamenti che includono flotte Elastic, diritti di accesso alle applicazioni basati su tributi, catalogo di applicazi oni multi-stack, flotte basate su Linux, ingresso e uscita dati, disaster recovery e altri aggiornamenti. | 14 giugno 2022 |
| Documento aggiornato | Versione HTML pubblicata. | 19 gennaio 2022 |
| Pubblicazione iniziale | Whitepaper pubblicato. | 8 giugno 2021 |

# Note

I clienti hanno la responsabilità di effettuare la propria valutazione indipendente delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWSi prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

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.