Best practice per distribuire Amazon WorkSpaces

Accesso alla rete, servizi di directory e sicurezza

Luglio 2016

Note

Il presente documento è fornito a solo scopo informativo. In esso sono illustrate le attuali offerte di prodotti e le prassi di AWS alla data di pubblicazione del documento, offerte che sono soggette a modifica senza preavviso. È responsabilità dei clienti effettuare una propria valutazione indipendente delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi di AWS, ciascuno dei quali viene fornito "così com'è", senza garanzie di alcun tipo, né esplicite né implicite. Il presente documento non dà origine a garanzie, rappresentazioni, impegni contrattuali, condizioni o assicurazioni da parte di AWS, delle sue società affiliate, dei suoi fornitori o dei licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Indice

Sintesi

In questo whitepaper vengono illustrate una serie di best practice per la distribuzione di Amazon WorkSpaces. Nel documento sono presenti considerazioni su rete, servizi di directory, autenticazione degli utenti, sicurezza, monitoraggio e log.

Il documento è stato suddiviso in quattro parti per un accesso più rapido alle informazioni di interesse. Il presente documento è rivolto a tecnici che si occupano di reti, directory e sicurezza.

Introduzione

Amazon WorkSpaces è un servizio di desktop gestiti basato sul cloud. Amazon WorkSpaces elimina la difficoltà di reperire o di distribuire hardware oppure di installare software complessi. Questa soluzione offre un'esperienza desktop attraverso pochi clic sulla console di gestione AWS, l'interfaccia a riga di comando (CLI) AWS oppure le API. Con Amazon WorkSpaces è possibile lanciare un desktop in pochi minuti oppure collegarsi e accedere al software del proprio desktop da una rete esterna o locale in modo sicuro, veloce e affidabile.
È possibile:

- Sfruttare la propria Microsoft Active Directory (AD) locale già esistente con AWS Directory Service: AD Connector.
- Estendere la propria directory al cloud AWS.
- Creare una directory gestita con AWS Directory Service: Microsoft AD o Simple AD per gestire utenti e workspace.

È inoltre possibile sfruttare il server RADIUS locale o in ambiente cloud con AD Connector per fornire ai workspace un'autenticazione a più fattori (MFA, Multi-Factor Authentication).

È possibile automatizzare il provisioning di Amazon WorkSpaces utilizzando l'interfaccia a riga di comando (CLI) oppure le API. Amazon WorkSpaces può quindi essere integrato nel flusso di provisioning già esistente.

Per quanto riguarda la sicurezza, oltre alla crittografia di rete integrata offerta dal servizio WorkSpaces, è possibile anche abilitare la crittografia dei dati residenti per i workspace (vedere Workspace crittografati nella sezione sulla sicurezza).

È possibile distribuire le applicazioni ai diversi workspace usando strumenti in locale già esistenti, come Microsoft System Center Configuration Manager (SCCM), oppure usando Amazon WorkSpaces Application Manager (Amazon WAM).

La sezione che segue offre informazioni dettagliate su Amazon WorkSpaces, relativamente al funzionamento del servizio e a cosa sia necessario avere per lanciarlo, e presenta le opzioni e le funzionalità di cui è possibile avvalersi.

Requisiti di WorkSpaces

Per essere distribuito con successo il servizio Amazon WorkSpaces ha bisogno di tre componenti:

- **L'applicazione WorkSpaces per il client**. Un dispositivo client supportato da Amazon WorkSpaces. Un elenco completo di piattaforme e dispositivi supportati è disponibile qui.

  Per collegarsi a WorkSpaces si può usare anche uno zero client con tecnologia Personal Computer over Internet Protocol (PCoIP). Per avere un elenco dei dispositivi disponibili vedere Zero client con PCoIP per Amazon WorkSpaces.

- **Un servizio di directory per autenticare gli utenti e fornire l'accesso ai workspace**. Amazon WorkSpaces funziona attualmente con AWS Directory Service e Active Directory. È possibile usare il proprio server locale Active Directory con AWS Directory Service per supportare le credenziali degli utenti aziendali già esistenti con WorkSpaces.

- **Amazon Virtual Private Cloud (Amazon VPC) in cui eseguire Amazon WorkSpaces**. Per la distribuzione di WorkSpaces è necessario avere almeno due sottoreti, poiché ogni configurazione AWS Directory Service richiede due sottoreti in una implementazione Multi-AZ.

Considerazioni sulla rete

Ogni workspace è associato a una configurazione Amazon VPC e AWS Directory Service specifica utilizzata per crearlo. Tutte le configurazioni AWS Directory Service (Simple AD, AD Connector e Microsoft AD) hanno bisogno di due sottoreti, ognuna in zone di disponibilità diverse. Le sottoreti vengono associate in modo definitivo alla configurazione Directory Service e non possono essere modificate dopo la creazione di un AWS Directory Service. È pertanto fondamentale stabilire le dimensioni corrette delle sottoreti prima di creare la configurazione Directory Service. Prima di creare le sottoreti valutare attentamente questi aspetti:

- Quanti workspace verranno creati nel tempo? Qual è il tasso di crescita atteso?
- Quale tipologia di utenti ne usufruirà?
- Quante connessioni Active Directory Domain saranno presenti?
- Dove risiedono gli account utente aziendali?

Amazon consiglia di definire singoli o gruppi di utenti in base al tipo di accesso e di autenticazione utente previsti nel processo di pianificazione. Queste risposte sono utili quando è necessario limitare gli accessi a risorse o applicazioni specifiche. È possibile definire profili di utenti per segmentare e limitare gli accessi tramite AWS Directory Service, liste di controllo degli accessi alla rete, tabelle di routing e security group VPC. Ogni configurazione AWS Directory Service usa due sottoreti e applica le stesse impostazioni a tutti i workspace presenti nella stessa configurazione. Ad esempio, è possibile usare un security group che si applica a tutti i workspace collegati a un AD Connector per specificare se è richiesta l'autenticazione MFA o se l'utente finale può avere l'accesso in locale come amministratore al proprio workspace.

> **Nota** Ogni AD Connector si collega a un'unità organizzativa (OU) di Microsoft Active Directory. Per sfruttare questa funzionalità è necessario configurare il servizio di directory in modo che tenga conto dei profili utente.

In questa sezione vengono descritte le best practice da seguire per il dimensionamento di sottoreti, VPC e flussi di traffico, nonché per valutare le implicazioni relative alla progettazione dei servizi di directory.

Progettazione VPC

Ecco alcuni aspetti da considerare nella fase di progettazione di VPC, sottoreti, security group, politiche di routing e ACL di rete per creare un ambiente Amazon WorkSpaces che rispetti principi di scalabilità, sicurezza e facilità di gestione.

- **VPC**. Consigliamo di usare un VPC separato e specifico per la distribuzione di workspace. Con un VPC separato è possibile specificare gli aspetti di governance e sicurezza fondamentali per i workspace attraverso una separazione del traffico.
- **Servizi di directory**. Ogni configurazione AWS Directory Service richiede un paio di sottoreti per una suddivisione altamente disponibile del servizio di directory tra le zone di disponibilità Amazon.
- **Dimensione delle sottoreti**. La distribuzione dei workspace dipende dalla configurazione della directory e risiede nelle stesse sottoreti VPC dell'AWS Directory Service scelto. Alcune considerazioni:
  - Le dimensioni delle sottoreti sono definitive e non possono essere modificate; è quindi importante lasciare ampio spazio per le esigenze di crescita future.
  - È possibile specificare un security group predefinito per l'AWS Directory Service prescelto; il security group si applica a tutti i workspace associati alla configurazione AWS Directory Service specifica.
  - Diversi AWS Directory Service possono usare la stessa sottorete.

Nella fase di progettazione di un VPC è importante pensare ai piani di sviluppo futuro. Per esempio, l'organizzazione potrebbe decidere di aggiungere componenti di gestione come un server antivirus, un server per la gestione delle patch oppure un server Active Directory o RADIUS MFA. Per soddisfare tali requisiti è importante prevedere, nella progettazione VPC, indirizzi IP aggiuntivi.

Per una guida dettagliata e per altre considerazioni sulla progettazione VPC e sul dimensionamento delle sottoreti fare riferimento alla presentazione su **re:Invent** In che modo Amazon.com si muove verso Amazon WorkSpaces.

Interfacce di rete

Ogni workspace possiede due interfacce network elastiche (ENI), un'interfaccia di gestione della rete (eth0) e un'interfaccia di rete primaria (eth1). AWS usa l'interfaccia di gestione della rete per gestire il workspace; si tratta dell'interfaccia relativa alla connessione del client. AWS sfrutta per questa interfaccia intervalli di indirizzi IP privati. Per fare in modo che il routing di rete funzioni correttamente non è possibile usare tale spazio indirizzi privato su qualsiasi rete in grado di comunicare con il VPC di WorkSpaces.

Per un elenco degli indirizzi IP privati utilizzati in base alle regioni fare riferimento a Dettagli su Amazon WorkSpaces.

> **Nota** Amazon WorkSpaces e le interfacce di gestione di rete associate non risiedono nel VPC e non è possibile visualizzare l'interfaccia di gestione della rete o l'ID dell'istanza Amazon Elastic Compute Cloud (Amazon EC2) nella console di gestione AWS (vedere Figura 4, Figura 5 e Figura 6). Tuttavia, è possibile visualizzare e modificare le impostazioni del security group dell'interfaccia di rete primaria (eth1) nella console di gestione AWS. L'interfaccia di rete primaria di ogni workspace viene inoltre conteggiata ai fini dei limiti ENI Amazon EC2 in termini di risorse. Per distribuzioni significative di workspace è necessario provvedere all'ampliamento dei limiti ENI con una richiesta di intervento da parte del supporto tramite la console di gestione AWS.

Flusso di traffico

È possibile suddividere il traffico di Amazon WorkSpaces in due categorie principali:

- Il traffico tra il dispositivo client e il servizio Amazon WorkSpaces
- Il traffico tra il servizio Amazon WorkSpaces e il traffico di rete del cliente

Nella prossima sezione affronteremo questi due aspetti.

Dal dispositivo client al workspace

Il dispositivo su cui viene eseguito il client Amazon WorkSpaces userà le stesse due porte per la connettività del servizio WorkSpaces (indipendentemente dalla sua posizione, in locale o remota). Il client usa l'https sulla porta 443 per tutte le informazioni relative all'autenticazione e alle sessioni, mentre usa la porta 4172 (porta PCoIP) con TCP e UDP per lo streaming di pixel di un dato workspace e per il controllo dello stato generale della rete. Il traffico su entrambe le porte è crittografato. Il traffico della porta 443 fa riferimento alle informazioni relative a sessioni e autenticazioni e sfrutta i certificati TLS per la crittografia dei dati. Il traffico derivante dallo streaming di pixel utilizza la crittografia AES a 256 bit per la comunicazione tra il client e l'eth0 del workspace, attraverso il gateway di streaming. È possibile reperire maggiori informazioni nella sezione Sicurezza, più avanti in questo documento.

Pubblichiamo gli intervalli di indirizzi IP per regione dei nostri gateway PCoIP di streaming e gli endpoint per il controllo dello stato generale della rete. È possibile limitare il traffico in uscita sulla porta 4172 dalla rete aziendale verso il gateway di streaming AWS e gli endpoint di controllo dello stato generale della rete, autorizzando così solo il traffico in uscita sulla porta 4172 verso le regioni AWS specifiche in cui viene utilizzato Amazon WorkSpaces. Per gli intervalli IP e gli endpoint per il controllo dello stato generale della rete vedere Intervalli IP per il Gateway PCoIP di Amazon WorkSpaces.

Il client Amazon WorkSpaces ha una funzione di controllo dello stato della rete già integrata. Grazie a questa utility gli utenti possono verificare attraverso un indicatore di stato, posto in fondo a destra all'interno dell'applicazione, se la rete è in grado di supportare una connessione. Una visione più dettagliata dello stato della rete è accessibile selezionando **Rete** in basso a destra nel client e ciò che viene visualizzato è illustrato nella Figura 1.

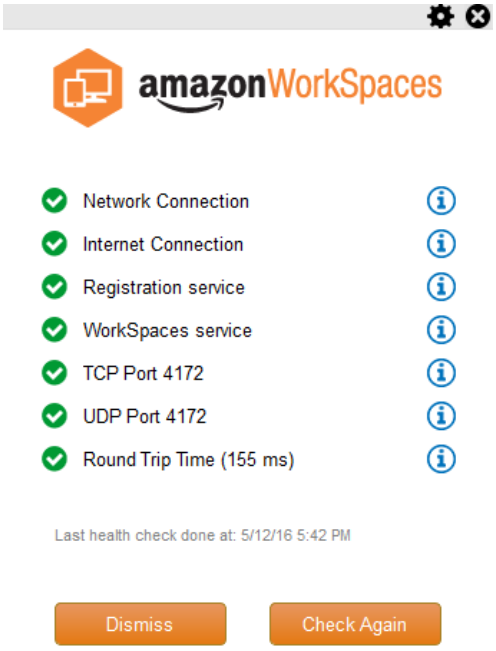

Figura 1: client WorkSpaces – controllo della rete

Un utente avvia una connessione dal proprio client al servizio Amazon WorkSpaces fornendo le proprie informazioni di accesso alla directory usata nella configurazione di Directory Service che coincide, in genere, con la directory aziendale. Le informazioni di accesso vengono inviate tramite https ai gateway di autenticazione del servizio Amazon WorkSpaces nella regione in cui si trova il workspace. Il gateway di autenticazione del servizio Amazon WorkSpaces inoltra quindi il traffico alla configurazione specifica del servizio AWS Directory Service associata al workspace in oggetto. Ad esempio, quando si usa AD Connector, quest'ultimo invia la richiesta di autenticazione direttamente al servizio Active Directory, che potrebbe essere in locale o in AWS VPC (vedere Scenari di distribuzione di AD DS). AD Connector non archivia le informazioni di autenticazione e funge da proxy stateless. Di conseguenza, è fondamentale che AD Connector abbia la connettività a un server Active Directory. AD Connector stabilisce a quale server Active Directory collegarsi tramite i server DNS definiti al momento della creazione di AD Connector.

Se si usa un AD Connector e si abilita MFA sulla directory, il token MFA viene verificato prima dell'autenticazione del servizio di directory. Nel caso in cui la verifica MFA non andasse a buon fine, le informazioni di accesso dell'utente non saranno inoltrate a AWS Directory Service.

Una volta completata l'autenticazione dell'utente, comincia il traffico dello streaming attraverso la porta 4172 (porta PCoIP) e il gateway AWS di streaming verso il workspace. Le informazioni relative alla sessione continuano a essere scambiate in questa fase tramite https. Il traffico dello streaming usa la prima ENI del workspace (eth0 nel workspace) non collegata al VPC. La connessione di rete dal gateway di streaming alla ENI viene gestita da AWS. In caso di errore nella connessione dai gateway di streaming alla ENI di streaming dei workspace, viene generato un evento CloudWatch (vedere la sezione di questo whitepaper relativa a Monitorare o effettuare l'accesso con Amazon CloudWatch).

La quantità di dati trasmessa tra il servizio Amazon WorkSpaces e il client dipende dal livello di attività dei pixel. Per garantire un'esperienza ottimale per gli utenti consigliamo che il round trip time (RTT) tra il client WorkSpaces e la regione AWS in cui si trova il workspace sia inferiore a 100 ms. In genere questo significa che il client Workspaces si trova a meno di 3218 chilometri dalla regione in cui è ospitato il workspace. Forniamo una pagina Web per il Controllo dello stato della connessione a cui fare riferimento per stabilire la regione AWS ottimale a cui collegarsi per il servizio Amazon WorkSpaces.

Servizio Amazon WorkSpaces e VPC

Dopo l'autenticazione della connessione di un client ad Amazon WorkSpaces e l'avvio del traffico di streaming, il client WorkSpaces mostrerà un desktop Windows (il workspace) collegato al VPC, mentre la rete dovrebbe mostrare l'esistenza di una connessione. L'ENI primaria di Amazon WorkSpaces, identificata come eth1, avrà un indirizzo IP assegnato dal servizio Dynamic Host Configuration Protocol (DHCP) fornito dalla rete VPC (in genere dalle stesse sottoreti di AWS Directory Service). L'indirizzo IP rimane legato al workspace per tutta la sua durata. L'ENI presente nel VPC ha accesso a tutte le risorse del VPC e a qualsiasi rete a esso connessa (attraverso un VPC in peering, una connessione AWS Direct Connect o una connessione VPN).

L'accesso ENI alle risorse di rete viene stabilito dal security group predefinito (per altre informazioni sui security group vedere qui) che AWS Directory Service configura per ogni workspace e da eventuali security group aggiuntivi assegnati a ENI. È possibile aggiungere security group alla ENI relativa alla rete VPC attraverso la console di gestione AWS o CLI. Oltre ai security group è possibile usare un host-based firewall su un workspace specifico per limitare l'accesso della rete alle risorse presenti all'interno del VPC.

Figura 4 in Scenari di distribuzione di AD DS, più avanti in questo whitepaper, viene illustrato il flusso di traffico descritto in precedenza.

Esempio di una configurazione tipica

Prendiamo ora in considerazione uno scenario in cui esistono due tipologie di utente e il servizio AWS Directory usa Active Directory centralizzata per l'autenticazione degli utenti:

- **Lavoratori che hanno bisogno di un accesso totale da qualsiasi luogo** (ad esempio, i dipendenti a tempo pieno). Tali utenti avranno il pieno accesso a Internet e alla rete interna e passeranno attraverso un firewall dal VPC alla rete locale.
- **Lavoratori a cui è consentito solo un accesso limitato alla rete aziendale** (ad esempio, appaltatori e consulenti). Tali utenti avranno un accesso limitato a Internet (a siti specifici) attraverso un server proxy nel VPC, alla rete nel VPC e alla rete locale.

Ai dipendenti a tempo pieno vogliamo dare la possibilità di avere un accesso in locale come amministratori al proprio workspace per installare eventuali software e offrire un'autenticazione a due fattori con MFA. Vogliamo anche consentire ai dipendenti a tempo pieno di accedere sempre a Internet dal proprio workspace.

Per gli appaltatori invece è necessario bloccare l'accesso come amministratori in locale in modo tale che possano utilizzare solo applicazioni specifiche preinstallate. Per questi workspace si desidera applicare controlli severi sull'accesso alla rete attraverso security group. È necessario quindi aprire le porte 80 e 443 solo per siti Web interni specifici e bloccare l'accesso a Internet.

In questo scenario sono presenti due tipologie diverse di profili utente con requisiti diversi in termini di reti e di accesso ai desktop. Si consiglia pertanto di gestire e di configurare i workspace in modo diverso. A questo scopo, è necessario creare due AD Connector, uno per ogni profilo utente. Ogni AD Connector richiede due sottoreti che hanno bisogno di indirizzi IP sufficienti per rispondere alle stime di crescita in termini d'uso dei workspace.

> **Nota** Ogni sottorete AWS VPC usa cinque indirizzi IP (i primi quattro e l'ultimo indirizzo IP) a scopi di natura gestionale e ogni AD Connector usa un indirizzo IP in ogni sottorete in cui è presente.

Di seguito altre considerazioni su questo scenario:

- Le sottoreti AWS VPC dovrebbero essere sottoreti private, in modo tale che il traffico (come nel caso degli accessi a Internet) sia controllato attraverso un gateway NAT, un server Proxy-NAT nel cloud oppure sia instradato attraverso un sistema di gestione del traffico in locale.
- Per il traffico del VPC previsto in locale viene installato un firewall.
- Il server Microsoft Active Directory e i server MFA RADIUS sono in sede (vedere Scenario 1: usare AD Connector come proxy per le autenticazioni di AD DS in **locale**) o sono parte dell'implementazione AWS Cloud (vedere gli scenari 2 e 3, Scenari di distribuzione di AD DS).

Considerato che a tutti i workspace sarà concesso un accesso a Internet sotto forme diverse e considerato che saranno ospitati in una sottorete privata, è necessario anche creare sottoreti pubbliche che possono accedere a Internet tramite gateway. Sarà pertanto necessario disporre di un gateway NAT per i dipendenti a tempo pieno, per consentire loro di accedere a Internet, e di un

server Proxy-NAT per i consulenti e gli appaltatori, per limitare il loro accesso ad alcuni siti web interni. Per prevedere eventuali guasti, progettare l'alta disponibilità e limitare i costi di traffico tra le diverse AZ, è importante avere due gateway NAT e server NAT o proxy in due sottoreti diverse per una implementazione Multi-AZ. Le due AZ selezionate come sottoreti pubbliche coincideranno con le due AZ usate come sottoreti per i workspace nelle regioni che hanno più di due AZ. È possibile instradare tutto il traffico proveniente da ogni AZ dei workspace verso la sottorete pubblica corrispondente per limitare i costi di traffico tra AZ diverse e offrire una gestione semplificata. La figura 2 mostra una configurazione VPC.

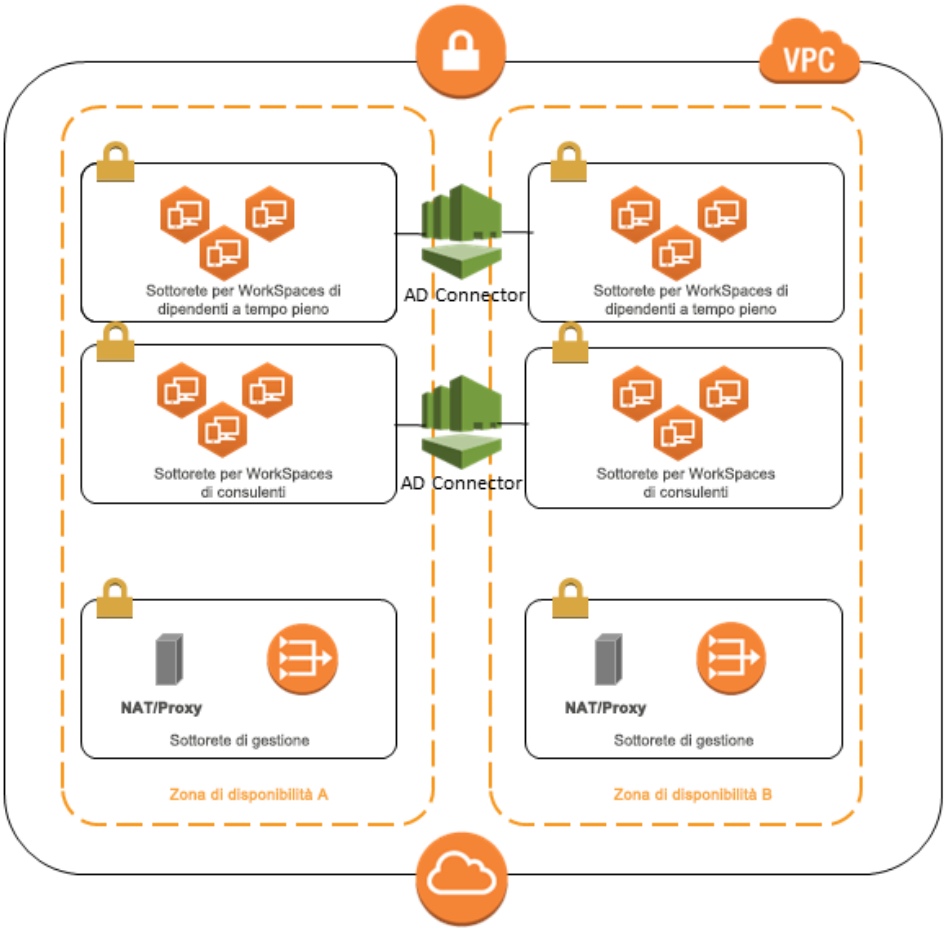

Figura 2: progettazione VPC di alto livello

Le informazioni che seguono illustrano come configurare le due tipologie di workspace descritte in precedenza.

- **Dipendenti a tempo pieno:** nella console di gestione di Amazon WorkSpaces, selezionare l'opzione **Directory** nella barra del menu, scegliere la directory in cui sono presenti i dipendenti a tempo pieno e poi selezionare **Impostazioni amministratore in locale**. Abilitando questa opzione qualsiasi workspace creato da questo momento in poi avrà i privilegi come amministratore locale. Per consentire l'accesso a Internet è necessario configurare Network Address Translation (NAT) per l'accesso a Internet in uscita dalla rete VPC. Per abilitare MFA è importante specificare un server RADIUS, gli IP dei server, le porte e una preshared key.

  Per i workspace dei dipendenti a tempo pieno, il traffico in entrata verso il workspace sarà limitato al Remote Desktop Protocol (RDP) dalla sottorete dell'helpdesk con l'applicazione di un security group predefinito nelle impostazioni di AD Connector.

- **Appaltatori e consulenti:** nella console di gestione di Amazon WorkSpaces, disabilitare **Accesso a Internet** e **Impostazione amministratore locale**. Poi aggiungere un security group nella sezione relativa alle impostazioni del **Security Group** per applicare un security group a tutti i nuovi workspace creati sotto quella directory.

  Per i workspace dei consulenti, limitare il traffico in ingresso e in uscita da e per i workspace, applicando un security group predefinito, nelle impostazioni di AD Connector, a tutti i workspace associati ad AD Connector. Il security group impedisce l'accesso in uscita dai workspace (ad esclusione del traffico HTTP e HTTPS) e il traffico in entrata verso il Remote Desktop Protocol (RDP) dalla sottorete dell'helpdesk nella rete locale.

Nota Il security group viene applicato solo all'interfaccia ENI presente nel VPC (eth1 nel workspace); l'accesso al workspace dal client di WorkSpaces non è infatti limitato dal security group. La figura 3 mostra il progetto finale del VPC di WorkSpaces descritto in precedenza.

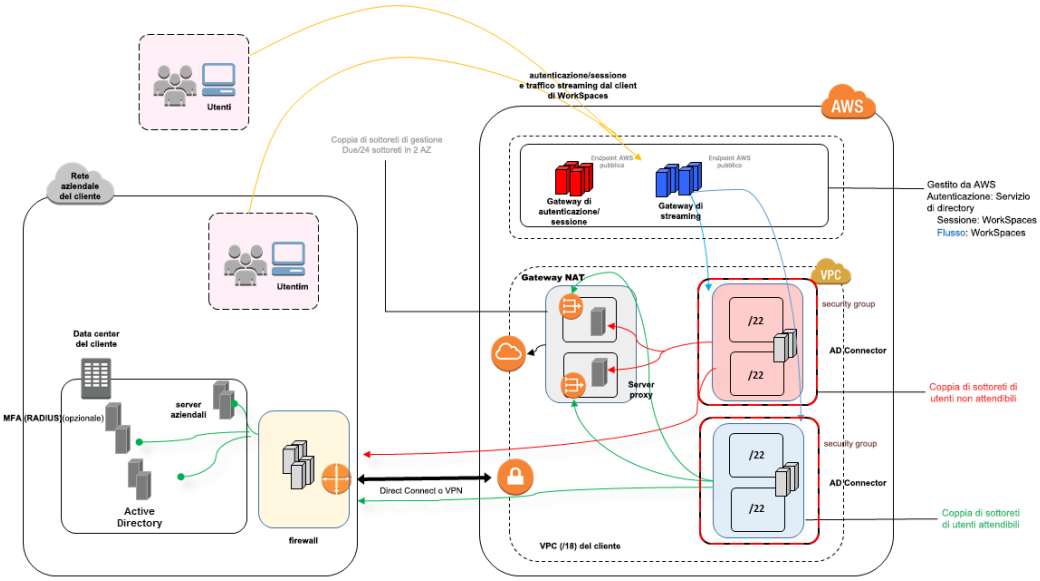

Figura 3: progetto di WorkSpaces con profili utente

AWS Directory Service

Come anticipato nell'introduzione, Amazon WorkSpaces è supportato da AWS Directory Service. Con AWS Directory Service è possibile creare tre tipi di directory. Le prime due risiedono in AWS Cloud:

- AWS Directory Service for Microsoft Active Directory (Enterprise Edition) o **Microsoft AD**, una Microsoft Active Directory gestita e supportata da Windows Server 2012 R2.
- **Simple AD**, un servizio di directory gestito e standalone, compatibile con Microsoft Active Directory e supportato da Samba 4.

Il terzo tipo, **AD Connector,** è un gateway di directory che consente di usare un proxy per le richieste di autenticazione e per le ricerche di utenti o gruppi nella propria Microsoft Active Directory locale già esistente.

La sezione che segue descrive i flussi di comunicazione per l'autenticazione tra il servizio Broker di Amazon WorkSpaces e AWS Directory Service, le best practice per implementare WorkSpaces con AWS Directory Service e concetti avanzati come MFA. Parleremo anche dell'architettura delle infrastrutture di Amazon WorkSpaces su larga scala, dei requisiti di Amazon VPC e di AWS Directory Service, inclusa l'integrazione con Microsoft Active Directory Domain Services (AD DS) in locale.

Scenari di distribuzione di AD DS

Amazon WorkSpaces è supportato da AWS Directory Service ed è fondamentale garantire una progettazione e una distribuzione corrette del servizio di directory. I tre scenari che seguono sono stati creati sulla base di *Microsoft Active Directory Domain Services* Guida Rapida e spiegano nel dettaglio le opzioni di distribuzione delle best practice per AD DS e, in modo specifico, l'integrazione con Amazon WorkSpaces. La *Considerazioni di natura progettuale* sezione di questo capitolo illustra i requisiti specifici e le best practice per l'uso di AD Connector per Amazon WorkSpaces, un aspetto che costituisce parte integrante del concetto di progetto generale di WorkSpaces.

- **Scenario 1: usare AD Connector come proxy per le autenticazioni di AD DS in locale.** In questo scenario viene garantita la connettività di rete (VPN/Direct Connect (DX)) presso il cliente e tutte le autenticazioni sono inviate come proxy attraverso AWS Directory Service (AD Connector) alla sottorete AD DS locale del cliente.
- **Scenario 2: estensione della sottorete AD DS locale in AWS (replica).** Questo scenario è simile al precedente ma, in questo caso, viene distribuita una replica della sottorete AD DS del cliente su AWS insieme a AD Connector, per ridurre la latenza delle richieste di autenticazione/di query alla sottorete AD DS e al catalogo globale AD DS.
- **Scenario 3: distribuzione standalone isolata con AWS Directory Service in AWS Cloud.** Si tratta di uno scenario isolato che non prevede la connettività verso il cliente per l'autenticazione. Tale approccio si basa su AWS Directory Service (Microsoft AD) e AD Connector. Sebbene questo scenario non presupponga la connettività verso il cliente per l'autenticazione, prevede comunque il supporto al traffico delle applicazioni, laddove richiesto, tramite VPN o DX.

Scenario 1: usare AD Connector come proxy per le autenticazioni di AD DS in locale

Questo scenario è stato pensato per quei clienti che non desiderano estendere AD DS in AWS o per quelle realtà che non contemplano la distribuzione di AD DS. La Figura 4: AD Connector verso una Active Directory locale illustra a un livello più alto ognuno dei componenti e mostra il flusso di autenticazione degli utenti.

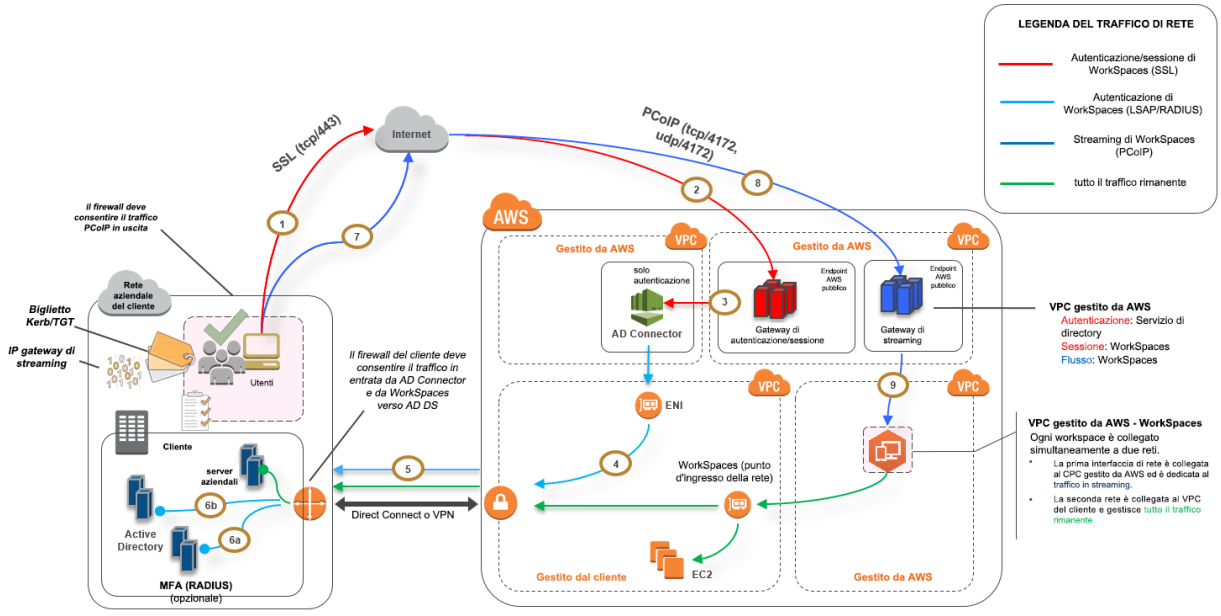

Figura 4: AD Connector verso una Active Directory locale

In questo scenario AWS Directory Service (AD Connector) viene usato per l'autenticazione MFA o di tutti gli utenti inviata come proxy attraverso AD Connector alla sottorete AD DS locale del cliente (Figura 5). Per maggiori dettagli sui protocolli o sulla crittografia usati per il processo di autenticazione vedere la sezione Sicurezza di questo whitepaper.

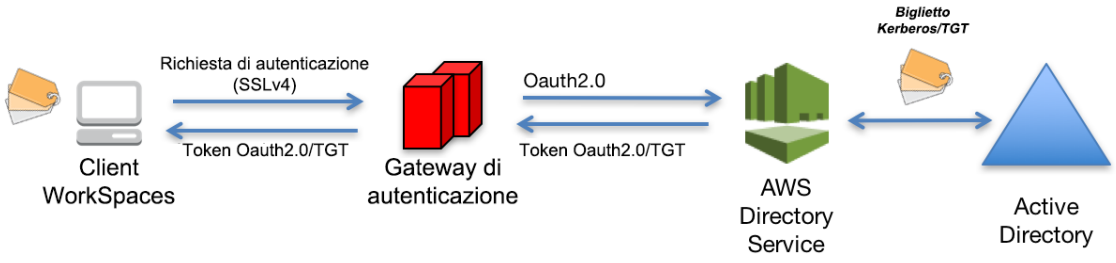

Figura 5: autenticazione degli utenti attraverso il gateway di autenticazione

Lo scenario 1 mostra un'architettura ibrida in cui il cliente potrebbe avere già risorse in AWS, oltre a risorse in un data center locale a cui è possibile accedere tramite WorkSpaces. Il cliente può usare i server AD DS e RADIUS già esistenti in locale per l'autenticazione MFA e degli utenti.

Questa architettura utilizza i seguenti componenti o la seguente configurazione.

Amazon Web Services:

- **Amazon VPC:** creazione di un Amazon VPC con almeno due sottoreti private in due zone di disponibilità.
- **Set di opzioni DHCP:** creazione di un set di opzioni Amazon VPC DHCP. Questo consente di definire il nome del dominio specifico per il cliente e i server dei nomi dei domini (DNS) (servizi locali) (per maggiori informazioni consultare Set di opzioni DHCP).
- **Gateway privato virtuale Amazon:** consente la comunicazione con la propria rete su un tunnel IPsec VPN o una connessione AWS Direct Connect.
- **AWS Directory Service**: AD Connector viene distribuito su una coppia di sottoreti private Amazon VPC.
- **Amazon WorkSpaces:** i workspace vengono distribuiti nelle stesse sottoreti private di AD Connector (vedere Considerazioni di natura progettuale, AD Connector).

Cliente:

- **Connettività della rete:** VPN aziendale o endpoint Direct Connect.
- **AD DS:** AD DS aziendale.
- **MFA (opzionale):** server aziendale RADIUS.
- **Dispositivi degli utenti finali:** i dispositivi degli utenti finali BYOL o aziendali (come Windows, Mac, iPad o tablet Android, zero client e Chromebook) usati per accedere al servizio Amazon WorkSpaces (vedere Dispositivi e piattaforme supportati).

Sebbene questa soluzione sia l'ideale per i clienti che non desiderano distribuire AD DS nel cloud, presenta dei punti di debolezza.

- **Garanzia di affidabilità della connettività:** se si perde la connettività al data center, nessun utente potrà accedere ai propri workspace e le

connessioni esistenti rimarranno attive per tutta la durata di Kerberos/TGT.

- **Latenza:** se esiste una latenza nella connessione (questo avviene più spesso con VPN che con DX), allora l'autenticazione di WorkSpaces e di qualsiasi attività relativa a AD DS, come l'applicazione di Group Policy (GPO), richiederà più tempo.
- **Costi relativi al traffico:** tutte le autenticazioni devono attraversare il link VPN o DX, per cui dipende dal tipo di connessione. Si tratta o del Data Transfer OUT da Amazon EC2 a Internet o del Data Transfer Out (DX).

> **Nota** AD Connector è un servizio di proxy. Non archivia né esegue il caching delle credenziali utente. Tutte le richieste di autenticazione, ricerca e gestione sono invece gestite da Active Directory. Nel servizio di directory è richiesto un account con privilegi di delega con i diritti per leggere tutte le informazioni degli utenti e collegare un computer al dominio.

Per maggiori dettagli su come configurare un utente nella directory per AD Connector, vedere Delegare i privilegi di connessione.

In generale, l'esperienza di Amazon WorkSpaces dipende in gran parte dall'elemento 5 mostrato nella Figura 4.

Scenario 2: estensione della sottorete AD DS locale in AWS (replica)

Questo scenario è simile allo scenario 1 ma, nello scenario 2, viene distribuita una replica della sottorete AD DS del cliente su AWS insieme a AD Connector. Questo consente di ridurre la latenza delle richieste di autenticazione o di query alla sottorete AD DS. La Figura 6 illustra a un livello più alto ognuno dei componenti e mostra il flusso di autenticazione degli utenti.

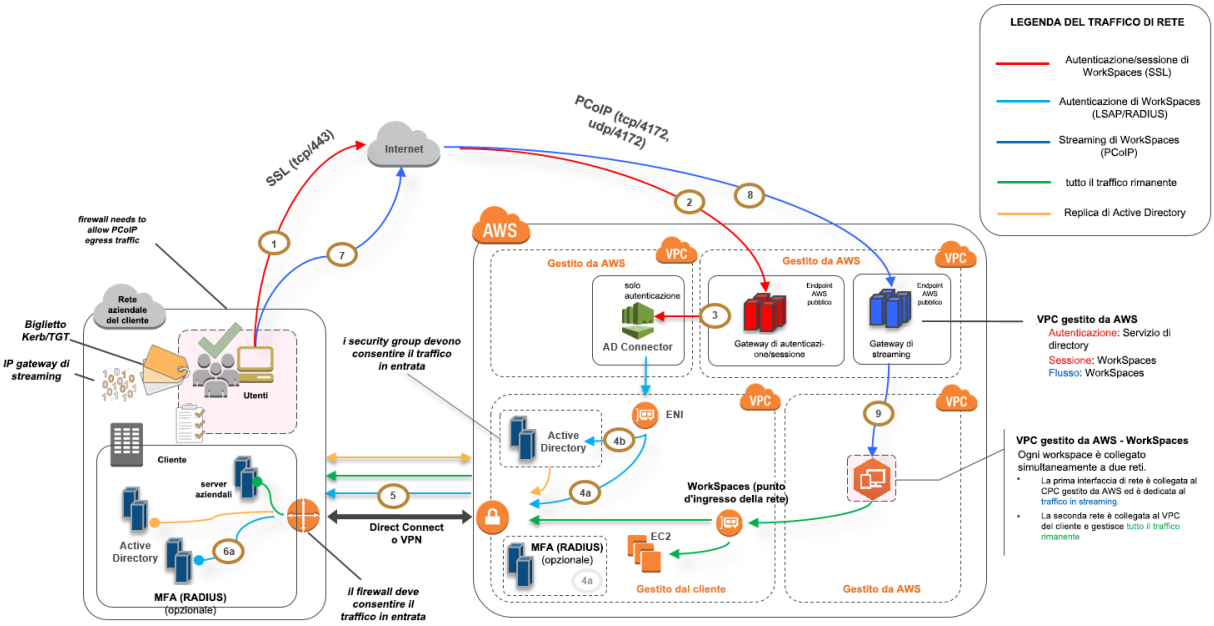

Figura 6: estendere il dominio Active Directory del cliente al cloud

Come avviene nello scenario 1, AD Connector viene usato per l'autenticazione MFA o di tutti gli utenti e, a sua volta, inviato come proxy alla sottorete AD DS del cliente (Figura 5). Nello scenario 2, la sottorete AD DS del cliente viene distribuita attraverso le zone di disponibilità su istanze Amazon EC2, promosse a controller di dominio della foresta Active Directory locale del cliente, eseguita in AWS Cloud. Ogni controller di dominio viene distribuito in sottoreti private VPC per rendere AD DS altamente disponibile in AWS Cloud. Per le best practice relative alla distribuzione di AD DS in AWS Cloud, vedere Considerazioni progettuali più avanti nel presente whitepaper.

Una volta distribuite le istanze dei workspace, questi ultimi avranno accesso ai controller dei domini basati su cloud per il DNS e i servizi di directory sicuri e a bassa latenza. La sicurezza di tutto il traffico della rete, inclusa la comunicazione AD DS, le richieste di autenticazione e la replica di Active Directory, viene garantita o con sottoreti private o attraverso il tunnel VPN o DX del cliente.

Questa architettura utilizza i seguenti componenti o la seguente configurazione.

Amazon Web Services:

- **Amazon VPC:** creazione di un Amazon VPC con almeno quattro sottoreti private in due zone di disponibilità (due per AD DS del cliente, due per AD Connector o WorkSpaces).
- **Set di opzioni DHCP:** creazione di un set di opzioni Amazon VPC DHCP. Questo consente di definire il nome del dominio specifico del cliente e i DNS (AD DS locale). Per maggiori informazioni consultare Set di opzioni DHCP.
- **Gateway privato virtuale Amazon:** consente la comunicazione con la propria rete su un tunnel IPsec VPN o una connessione AWS Direct Connect.
- **Amazon EC2:**

— controller del dominio AD DS aziendale del cliente distribuiti su istanze Amazon EC2 in sottoreti private VPC dedicate.

— Server RADIUS "opzionali" del cliente per MFA.

- **AWS Directory Services**: AD Connector viene distribuito su una coppia di sottoreti private Amazon VPC.
- **Amazon WorkSpaces:** i workspace vengono distribuiti nelle stesse sottoreti private di AD Connector (vedere Considerazioni di natura progettuale, AD Connector).

Cliente:

- **Connettività della rete:** Endpoint del VPN aziendale o di AWS Direct Connect.
- **AD DS:** AD DS aziendale (richiesto per la replica).
- **MFA "opzionale":** server aziendale RADIUS.

Dispositivi degli utenti finali: i dispositivi degli utenti finali BYOL o aziendali (come Windows, Mac, iPad o tablet Android, zero client e Chromebook) usati per accedere al servizio Amazon WorkSpaces (vedere Dispositivi e piattaforme supportati).

A differenza dello scenario 1, questa soluzione non presenta gli stessi punti di debolezza. Pertanto, WorkSpaces e AWS Directory Service non hanno attiva l'opzione di garanzia di affidabilità della connettività.

- **Garanzia di affidabilità della connettività:** se si perde la connettività al data center del cliente, gli utenti finali possono continuare a lavorare perché l'autenticazione e l'MFA "opzionale" sono elaborati in locale.
- **Latenza:** tutte le autenticazioni sono locali e a bassa latenza, ad eccezione del traffico di replica (vedere *Considerazioni di* natura progettuale*:* siti e servizi AD DS).
- **Costi relativi al traffico:** in questo scenario, l'autenticazione è in locale e solo la replica AD DS deve attraversare il link VPN o DX, con conseguente riduzione del trasferimento di dati.

In generale, l'esperienza di WorkSpaces è migliore e non dipende in gran misura dall'elemento 5 come mostrato in Figura 6. Questo aspetto diventa ancora più evidente quando si desidera distribuire WorkSpaces a migliaia di desktop, soprattutto in relazione alle query di catalogo globale di AD DS, dal momento che questo traffico rimane in locale.

Scenario 3: distribuzione standalone isolata con AWS Directory Service in AWS Cloud.

Questo scenario, mostrato in Figura 7, presenta una sottorete AD DS distribuita in AWS Cloud in un ambiente isolato e standalone. AWS Directory Service viene usato esclusivamente in questo scenario. Invece di gestire totalmente AD DS in autonomia, è possibile avvalersi di AWS Directory Service per attività come la definizione di una topologia di directory altamente disponibili, il monitoraggio dei controller di dominio e la configurazione di backup e snapshot.

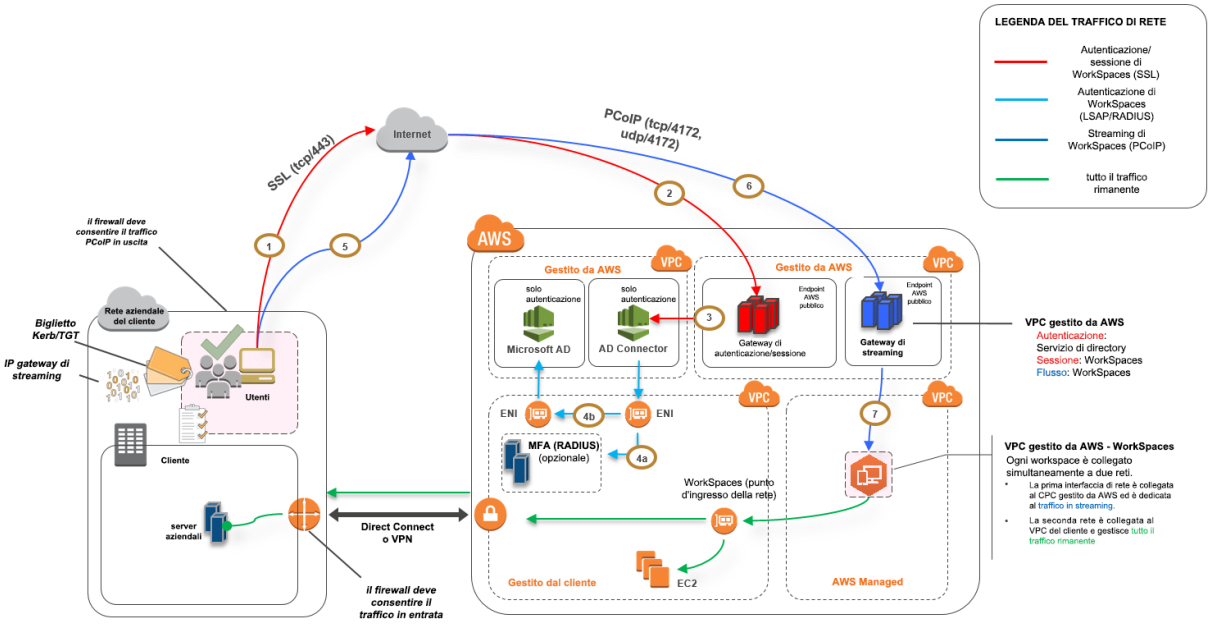

Figura 7: solo cloud - AWS Directory Services (Microsoft AD)

Come nello scenario 2, AD DS (Microsoft AD) viene distribuito in sottoreti dedicate che coprono due zone di disponibilità, rendendo così AD DS altamente disponibile in AWS Cloud. Oltre a Microsoft AD, AD Connector (in tutti e tre gli scenari) viene usato per l'autenticazione di WorkSpaces o per MFA. Questo garantisce una separazione di ruoli o funzioni in Amazon VPC, una best practice standard (vedere la sezione *Considerazioni di* natura progettuale: Rete partizionata).

Lo scenario 3 illustra una configurazione standard completa ideale per i clienti che desiderano che AWS gestisca la distribuzione, l'applicazione di patch, l'alta disponibilità e il monitoraggio di AWS Directory Service. A causa del suo isolamento, oltre alla produzione, lo scenario funziona bene anche per proof of concept e ambienti lab.

Oltre al posizionamento di AWS Directory Service, la Figura 7 mostra il flusso di traffico da un utente a un workspace e l'interazione tra il workspace e il server AD o il server MFA.

Questa architettura utilizza i seguenti componenti o la seguente configurazione.

Amazon Web Services:

- **Amazon VPC:** creazione di un Amazon VPC con almeno quattro sottoreti private in due zone di disponibilità (due per AD DS *Microsoft AD*, due per AD Connector o WorkSpaces). "*Separazione dei ruoli*".
- **Set di opzioni DHCP:** creazione di un set di opzioni Amazon VPC DHCP. Questo consente di definire il nome del dominio specifico per il cliente e i DNS (Microsoft AD). Per maggiori informazioni consultare Set di opzioni DHCP.
- **Opzionale: Gateway privato virtuale Amazon:** consente la comunicazione con la propria rete su un tunnel IPsec VPN (VPN) o una connessione AWS Direct Connect. Da usare per l'accesso ai sistemi di back-end locali.
- **AWS Directory Service:** Microsoft AD viene distribuito su una coppia di sottoreti VPC dedicate (AD DS Managed Service).
- **Amazon EC2:** server RADIUS "opzionali" del cliente per MFA.
- **AWS Directory Services**: AD Connector viene distribuito su una coppia di sottoreti private Amazon VPC.
- **Amazon WorkSpaces:** i workspace vengono distribuiti nelle stesse sottoreti private di AD Connector (vedere Considerazioni di natura progettuale, AD Connector).

Cliente:

- **Opzionale: connettività della rete:** VPN aziendale o endpoint AWS Direct Connect.
- **Dispositivi degli utenti finali:** i dispositivi degli utenti finali BYOL o aziendali (come Windows, Mac, iPad o tablet Android, zero client e Chromebook) usati per accedere al servizio Amazon WorkSpaces (vedere Dispositivi e piattaforme supportati).

Come nello scenario 2, questa soluzione non presenta problematiche relative alla garanzia di affidabilità della connettività al data center locale del cliente, alla latenza o ai costi legati al trasferimento dei dati in uscita (ad eccezione del caso in cui l'accesso a Internet sia abilitato per i workspace all'interno del VPC), poiché è stata appositamente progettata come scenario isolato o solo cloud.

Considerazioni di natura progettuale

Una distribuzione AD DS funzionale in AWS Cloud richiede una buona conoscenza dei concetti Active Directory e dei servizi AWS specifici. In questa sezione faremo alcune considerazioni di natura progettuale importanti per la distribuzione AD DS per WorkSpaces, parleremo di best practice VPC per AWS Directory Service, di requisiti DHCP e DNS, di specifiche riguardanti AD Connector e di siti e servizi Active Directory.

Progettazione VPC

Come accennato nella sezione Considerazioni sulla rete di questo documento e illustrato in precedenza negli scenari 2 e 3, AD DS deve essere distribuito in AWS Cloud con una coppia dedicata di sottoreti private, attraverso due zone di disponibilità, e separato da AD Connector o dalle sottoreti di WorkSpaces. Questa configurazione offre un accesso altamente disponibile e a bassa latenza ai servizi AD DS per WorkSpaces, osservando, al tempo stesso, le best practice standard di separazione di ruoli o funzioni all'interno di Amazon VPC.

La Figura 8 mostra la separazione di AD DS e AD Connector in sottoreti private dedicate (scenario 3). In questo esempio tutti i servizi risiedono nello stesso Amazon VPC.

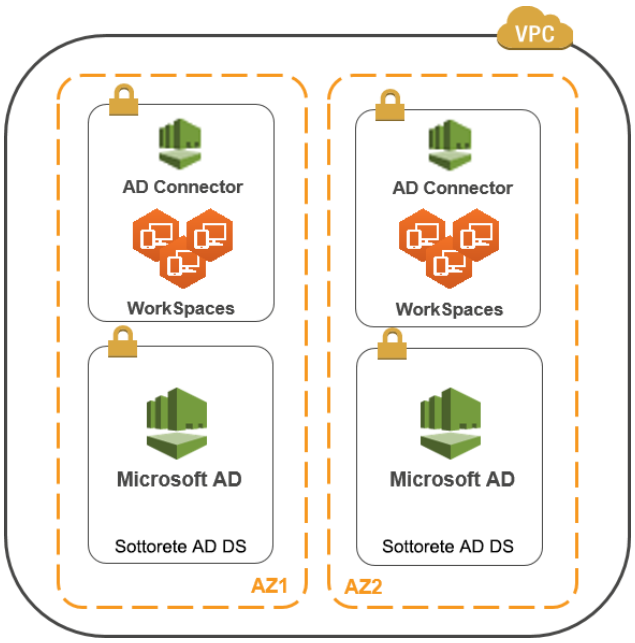

Figura 8: segregazione della rete AD DS

La figura 9 mostra un progetto simile allo scenario 1; tuttavia, in questo scenario la porzione locale risiede in un Amazon VPC dedicato.

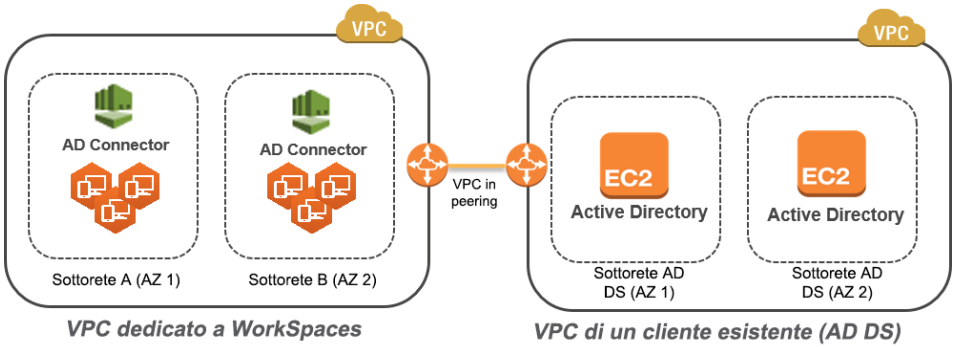

Figura 9: VPC di workspace dedicati

> **Nota** Ai clienti che hanno una distribuzione AWS già attiva con AD DS, consigliamo di posizionare WorkSpaces in un VPC dedicato e di usare VPC in peering per le comunicazioni AD DS.

Oltre alla creazione di sottoreti private dedicate per AD DS, i controller dei domini e i server dei membri richiedono l'applicazione di diverse regole di security group per consentire il traffico legato ai servizi, come la replica AD DS, l'autenticazione degli utenti, i servizi Windows Time e il Distributed File System (DFS).

> **Nota** secondo le best practice è necessario limitare le regole del security group alle sottoreti private di WorkSpaces e, nel caso dello scenario 2, consentire comunicazioni AD DS bidirezionali in locale verso/da AWS Cloud, come mostrato nella tabella che segue.

Protocollo	Porta	Uso	Destinazione
tcp	53, 88, 135, 139, 389, 445, 464, 636	Autenticazione (primaria)	Active Directory (data center privato o EC2)*
tcp	49152 – 65535	RPC High Port	Active Directory (data center privato o EC2)**
tcp	3268-3269	Trust	Active Directory (data center privato o EC2)*
tcp	9389	Remote Microsoft Windows PowerShell (opzionale)	Active Directory (data center privato o EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	Autenticazione (primaria)	Active Directory (data center privato o EC2)*
udp	1812	Autenticazione (MFA) (opzionale)	RADIUS (data center privato o EC2)*

* Vedere Requisiti in termini di porte per Active Directory e Active Directory Domain Services

**Vedere Panoramica del servizio e requisiti in termini di porte di rete per Windows

Per una guida dettagliata sulle regole di implementazione vedere Aggiungere regole a un security group nella *Guida per l'utente su Amazon Elastic Compute Cloud*.

Progettazione VPC: DHCP e DNS

Con un Amazon VPC, i servizi DHCP vengono forniti per le istanze per impostazione predefinita. Per impostazione predefinita, ogni VPC offre un server DNS interno accessibile tramite Classless Inter-Domain Routing (CIDR) +2 spazi indirizzi e viene assegnato a tutte le istanze attraverso un set di opzioni DHCP predefinito.

I set di opzioni DHCP vengono usati in Amazon VPC per definire le opzioni relative agli ambiti di applicazione, come il nome del dominio o i server dei nomi che devono essere trasmessi alle istanze tramite DHCP. Il corretto funzionamento dei servizi Windows all'interno del VPC dipende da questa opzione relativa all'ambito di applicazione DHCP e deve pertanto essere impostata correttamente. In ognuno degli scenari definiti in precedenza, è necessario creare e assegnare il proprio ambito di applicazione per definire il nome dei domini e i server dei nomi. In questo modo le istanze Windows aggiunte al dominio o WorkSpaces vengono configurate per usare Active Directory DNS. La tabella che segue è un esempio di un set personalizzato di opzioni DHCP relative agli ambiti di applicazione necessario per il corretto funzionamento di WorkSpaces e AWS Directory Services.

Parametro	Valore
Tag del nome	Crea un tag con chiave = **nome** e **valore** per una stringa specifica Esempio: exampleco.com
Nome del dominio	exampleco.com
Server dei nomi dei domini	Indirizzo DNS del server, separato da virgole Esempio: 10.0.0.10, 10.0.1.10
Server NTP	Lasciare questo campo vuoto
Server dei nomi NetBIOS	Inserire gli stessi IP separati da virgola dei server dei nomi dei domini Esempio: 10.0.0.10, 10.0.1.10
Tipo di nodo NetBIOS	2

Per maggiori dettagli su come creare un set di opzioni DHCP personalizzato e associarlo ad Amazon VPC, vedere Lavorare con i set di opzioni DHCP in *Guida per l'utente su Amazon Virtual Private Cloud*.

Nello scenario 1 l'ambito di applicazione DHCP è relativo al DNS o AD DS locali. Negli scenari 2 o 3, invece, si tratterebbe di un servizio di directory distribuito localmente (AD DS su Amazon EC2 o AWS Directory Services: Microsoft AD). Consigliamo di trasformare ogni controller di dominio che risiede in AWS Cloud in un server di catalogo globale e in un server Directory Integrated DNS.

Active Directory: siti e servizi

Per lo scenario 2, siti e servizi sono componenti strategici per il corretto funzionamento di AD DS. La topologia del sito controlla la replica Active Directory tra i controller dei domini all'interno dello stesso sito e tra i confini dei siti. Nello scenario 2 sono presenti almeno due siti, uno in locale e AWS WorkSpaces nel cloud. Definire la corretta topologia del sito significa garantire l'affinità dei client e quindi i client (in questo caso WorkSpaces) useranno il controller di dominio locale preferito.

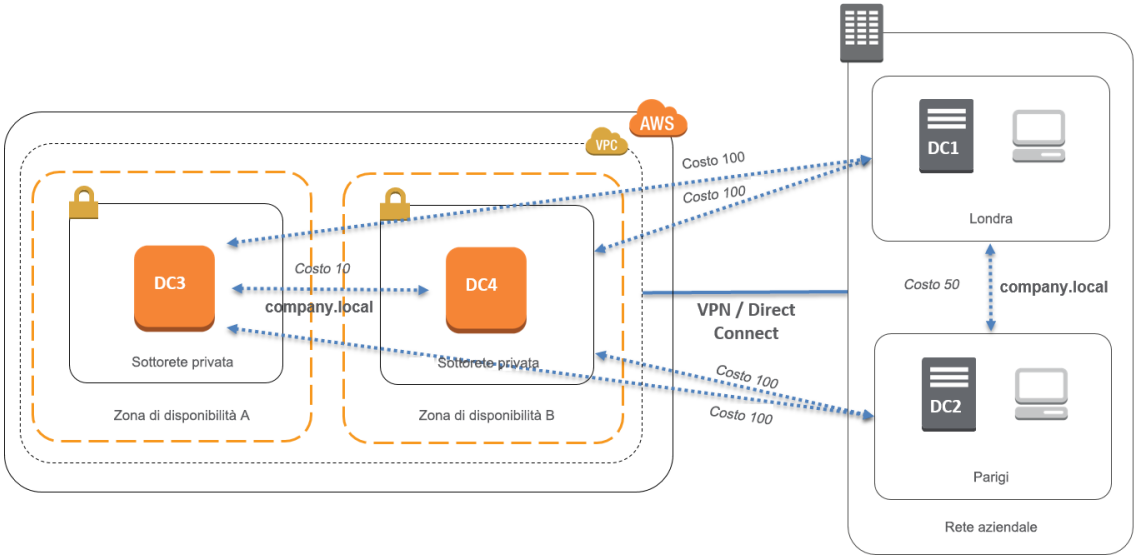

Figura 10: siti e servizi Active Directory: affinità dei client

> **Best practice** Definire i costi elevati per i collegamenti dei siti tra AD DS locale e AWS Cloud. La Figura 10 è un esempio dei costi da assegnare ai collegamenti dei siti (costo 100) per garantire affinità tra client indipendentemente dai siti.

Con queste associazioni si è sicuri che il traffico (come nel caso della replica AD DS o dell'autenticazione del client) utilizzi il percorso migliore per raggiungere il controller dei domini. Nel caso degli scenari 2 e 3, questo aspetto aiuta a diminuire la latenza e il traffico legato ai collegamenti.

Multi-Factor Authentication (MFA)

Per implementare MFA l'infrastruttura di WorkSpaces deve usare AD Connector come AWS Directory Service e avere un server RADIUS. Sebbene nel presente documento non venga illustrata la distribuzione di un server RADIUS, la sezione precedente, Scenari di distribuzione di AD DS spiega nel dettaglio il posizionamento di un server RADIUS in ogni scenario.

MFA – Autenticazione a due fattori

Amazon WorkSpaces supporta MFA attraverso AWS Directory Service: AD Connector e un server RADIUS *di proprietà del cliente*. Una volta abilitati, gli utenti devono fornire **Nome utente**, **Password** e **Codice MFA** del client WorkSpaces per l'autenticazione ai rispettivi desktop di WorkSpaces.

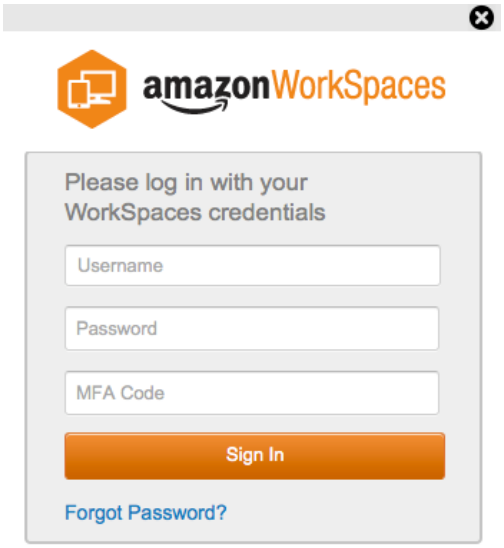

Figura 11: client di WorkSpaces con MFA abilitato

> **Regola importante** l'implementazione dell'autenticazione MFA richiede l'uso di AD Connector. AD Connector non supporta l'autenticazione MFA selettiva "per utente", dal momento che si tratta di un'impostazione globale per AD Connector. Se si richiede l'autenticazione MFA selettiva "per utente", allora gli utenti devono essere separati tramite AD Connector.

MFA per WorkSpaces richiede uno o più server RADIUS. In genere, si tratta di soluzioni esistenti, ad esempio RSA, o i server possono essere distribuiti all'interno del VPC (vedere Scenari di distribuzione di AD DS). Se si distribuisce una nuova soluzione RADIUS, oggi esistono diverse tipologie di implementazioni, come FreeRADIUS e servizi cloud come Duo Security.

Per un elenco dei prerequisiti per implementare MFA con Amazon WorkSpaces, vedere la *Guida per l'amministrazione di Amazon WorkSpaces*, Preparare la rete per una directory AD Connector. Il processo di configurazione di AD Connector per MFA viene descritto in Gestire una directory AD Connector: autenticazione a più fattori, in *Guida per l'amministrazione di Amazon WorkSpaces*.

Sicurezza

Questa sezione spiega come garantire la sicurezza dei dati attraverso la crittografia quando si utilizzano i servizi Amazon WorkSpaces. Parliamo di crittografia dei dati in transito e memorizzati e dell'uso di security group per proteggere l'accesso dalla rete a WorkSpaces. È possibile trovare informazioni aggiuntive sull'autenticazione (incluso il supporto a MFA) nella sezione AWS Directory Service.

Crittografia in transito

Amazon WorkSpaces usa la crittografia per garantire la riservatezza in diverse fasi della comunicazione (in transito) e per proteggere tutti i dati inattivi (workspace crittografati). Nelle sezioni che seguono vengono descritti i processi di ogni fase della crittografia usata da Amazon WorkSpaces per i dati in transito. Per informazioni sulla crittografia dei dati inattivi, vedere la sezione Workspace crittografati più avanti in questo whitepaper.

Registrazione e aggiornamenti

L'applicazione client del desktop comunica con Amazon per aggiornamenti e registrazione tramite https.

Fase di autenticazione

Il client desktop avvia la procedura di autenticazione inviando le credenziali al gateway di autenticazione. La comunicazione tra il client desktop e il gateway di autenticazione avviene tramite https. Alla fine di questa fase, se l'autenticazione è andata a buon fine, il gateway risponde al client desktop con un token OAuth 2.0, usando sempre la connessione https.

> **Nota** L'applicazione client del desktop supporta l'uso di un server proxy per il traffico della porta 443 (HTTPS), per gli aggiornamenti, la registrazione e l'autenticazione.

Dopo aver ricevuto le credenziali dal client, il gateway di autenticazione invia una richiesta di autenticazione a AWS Directory Service. La comunicazione dal gateway di autenticazione a AWS Directory Service avviene tramite HTTPS, per cui nessuna credenziale viene trasmessa con testi in chiaro.

Autenticazione - AD Connector

AD Connector usa Kerberos per stabilire una comunicazione autenticata con AD in locale, così può vincolarsi a LDAP ed eseguire le successive query LDAP. Al momento, AWS Directory Service non supporta LDAP con TLS (LDAP). Tuttavia, le credenziali utente non vengono mai trasmesse come testo in chiaro. Per maggiore sicurezza è possibile collegare il VPC di WorkSpaces con la rete locale (dove risiede AD) tramite una connessione VPN. Quando si usa una connessione hardware VPN AWS, è possibile configurare la crittografia in transito usando il metodo IPSEC standard (IKE e IPSEC SA) con le chiavi di crittografia simmetrica AES-128 o AES-256, la funzione crittografica di hash SHA-1 o SHA-256 per garantire l'integrità e i gruppi DH (2,14-18, 22, 23 e 24 per la fase 1; 1,2,5, 14-18, 22, 23 e 24 per la fase 2) con PFS.

Fase broker

Dopo aver ricevuto il token OAuth 2.0 (dal gateway di autenticazione, se l'autenticazione è andata a buon fine), il client desktop eseguirà una query ai servizi Amazon WorkSpaces (Broker Connection Manager) tramite HTTPS. Il client desktop si autenticherà inviando il token OAuth 2.0 e riceverà l'informazione relativa all'endpoint del gateway di streaming di WorkSpaces.

Fase di streaming

Il client desktop richiede l'apertura di una sessione PCoIP con il gateway di streaming (usando il token OAuth 2.0). Questa sessione è crittografata con aes256 e usa la porta PCoIP per il controllo della comunicazione (4712/tcp).

Tramite il token OAuth2.0, il gateway di streaming richiede le informazioni di WorkSpaces specifiche dell'utente al servizio WorkSpaces tramite https.

Il gateway di streaming riceve il TGT dal client (crittografato usando la password dell'utente del client) e, grazie al pass-through di Kerberos TGT, il gateway avvia un login di Windows al workspace, utilizzando il Kerberos TGT dell'utente così recuperato.

Il workspace avvia a questo punto una richiesta di autenticazione all'AWS Directory Service configurato, tramite l'autenticazione Kerberos standard.

Una volta effettuato con successo l'accesso al workspace, comincia lo streaming PCoIP. La connessione viene inizializzata dal client sulla porta tcp 4172 con il traffico di ritorno sulla porta udp 4172. Inoltre, la connessione iniziale tra il gateway di streaming e il desktop di WorkSpaces attraverso l'interfaccia di gestione avviene tramite UDP 55002 (vedere la documentazione su Amazon Workspaces, Maggiori dettagli su Amazon WorkSpaces; la porta UDP iniziale in uscita è 55002). La connessione dello streaming, che usa le porte 4172 (tcp e udp), è crittografata tramite la cifratura AES 128- e 256-bit ma, per impostazione predefinita, è su 128-bit. È possibile cambiarla a 256-bit tramite l'Active Directory GPO specifico per PCoIP (pcoip.adm).

Interfacce di rete

Ogni Amazon WorkSpaces ha due interfacce di rete, chiamate interfaccia di rete primaria e interfaccia di gestione della rete.

L'interfaccia di rete primaria offre la connettività alle risorse presenti all'interno del VPC, come l'accesso a AWS Directory Service, a Internet e alla rete aziendale. È possibile collegare i security group a questa interfaccia di rete primaria (come si farebbe con qualsiasi ENI). Concettualmente è necessario distinguere i security group collegati a questa ENI in base all'ambito di applicazione della distribuzione: il security group di WorkSpaces e i security group ENI.

Interfaccia di gestione della rete

Non è possibile controllare l'interfaccia di gestione della rete tramite i security group; tuttavia, è possibile usare un host-based firewall sul workspace per bloccare le porte o controllare gli accessi. È sconsigliato applicare limitazioni sull'interfaccia di gestione della rete. Se si decide di aggiungere le regole di un host-based firewall per gestire questa interfaccia, è necessario tenere alcune porte aperte in modo che il servizio WorkSpaces possa gestire l'integrità e l'accessibilità al workspace come descritto nella Guida per l'amministrazione di Amazon WorkSpaces.

Security Group di WorkSpaces

Per AWS Directory Service viene creato un security group predefinito che viene automaticamente collegato a tutti i workspace che appartengono a quella directory specifica.

Come con qualsiasi altro security group, è possibile modificare le regole di un security group di WorkSpaces. I risultati vengono applicati subito dopo aver effettuato le modifiche.

È anche possibile modificare il security group predefinito di WorkSpaces collegato a un AWS Directory Service modificando l'associazione del security group di WorkSpaces http://docs.aws.amazon.com/de_de/workspaces/latest/adminguide/admin_details.html - member_security_group.

> **Nota** un security group associato di recente sarà collegato solo ai workspace creati o ricreati dopo la modifica.

Security Group ENI

Considerato che l'interfaccia di rete primaria è un'interfaccia ENI standard, è possibile gestirne la configurazione attraverso diversi strumenti di gestione AWS (vedere Elastic Network Interfaces (ENI)). In particolare, è necessario individuare l'IP del workspace (nella pagina di WorkSpaces all'interno della console Amazon WorkSpaces) e poi usare quell'indirizzo IP come filtro per trovare l'ENI corrispondente (nella sezione Interfacce di rete della console Amazon EC2).

Una volta individuata l'ENI, è possibile gestire i security group direttamente da lì. Quando si assegnano manualmente i security group all'interfaccia di rete primaria, è necessario considerare i requisiti relativi alle porte di Amazon WorkSpaces, come spiegato in Maggiori dettagli su Amazon WorkSpaces.

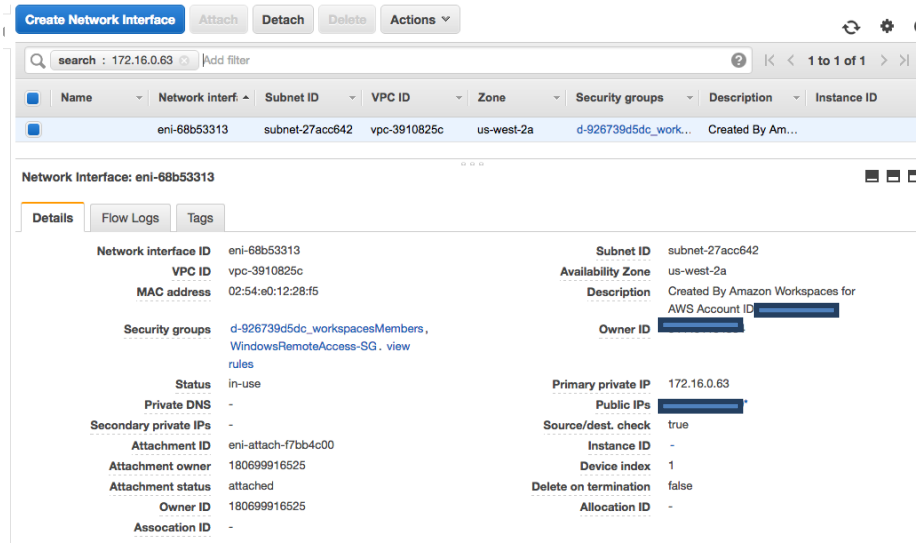

Figura 12: gestire le associazioni di security group

Workspace crittografati

Ogni Amazon WorkSpaces dispone di un volume radice (disco C:) e di un volume utente (disco D:). La funzione Workspace crittografati consente di crittografare uno dei due volumi o entrambi.

Cosa viene crittografato?

I dati inattivi, I/O su disco per i volumi e gli snapshot creati dai volumi crittografati sono tutti codificati.

Quando avviene la crittografia?

La crittografia di un workspace deve essere specificata al momento del lancio (della creazione) del workspace. I volumi dei workspace possono essere crittografati solo al momento del loro lancio: dopo questo momento non è possibile modificare lo stato di crittografia di un volume. La Figura 13 mostra la pagina della console Amazon WorkSpaces in cui selezionare la crittografia nella fase di lancio di un workspace.

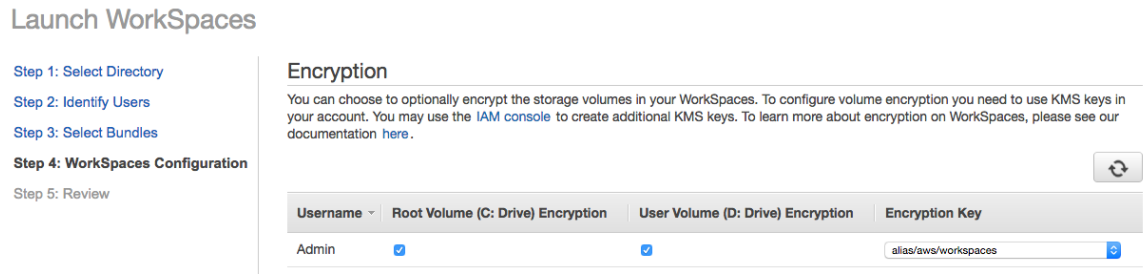

Figura 13: crittografia dei volumi dei workspace

Come viene crittografato un nuovo workspace?

È possibile selezionare l'opzione Workspace crittografati dalla console Amazon WorkSpaces o da AWS CLI, oppure è possibile usare le API di Amazon WorkSpaces al momento del lancio di un nuovo workspace.

Per crittografare i volumi, Amazon WorkSpaces usa una chiave master del cliente (CMK) di AWS Key Management Service (KMS). Quando un workspace viene lanciato per la prima volta in una regione (le CMK hanno un ambito di applicazione regionale) viene creata una CMK AWS KMS predefinita. È possibile anche creare una CMK gestita dal cliente da usare con i workspace crittografati. La CMK viene usata per crittografare le chiavi di dati usate dal servizio Amazon WorkSpaces per codificare i volumi (più precisamente, sarà il servizio Amazon Elastic Block Store (Amazon EBS) a codificare i volumi). Ogni CMK può essere usata per crittografare le chiavi di massimo 30 workspace.

> **Nota** Al momento non è possibile creare immagini personalizzate da un workspace crittografato. Inoltre, la visualizzazione dei workspace lanciati con la crittografia del volume radice abilitata può richiedere fino a un'ora.

Per una descrizione dettagliata del processo di crittografia dei workspace vedere Panoramica sulla crittografia di Amazon WorkSpaces tramite AWS KMS. Per ulteriori informazioni sulle chiavi master dei clienti e sulle chiavi di dati AWS KMS vedere Concetti di AWS Key Management Service.

Monitoraggio o accesso tramite Amazon CloudWatch

Il monitoraggio è parte integrante di qualsiasi infrastruttura, sia essa relativa a reti, server o log. I clienti che distribuiscono Amazon WorkSpaces devono monitorare le proprie attività e, soprattutto, l'integrità generale e lo stato della connessione di ogni singolo workspace.

Parametri Amazon CloudWatch per WorkSpaces

I parametri CloudWatch per WorkSpaces sono stati progettati per offrire agli amministratori una visione più completa dell'integrità generale e dello stato della connessione di ogni singolo workspace. I parametri sono disponibili per singolo workspace oppure vengono aggregati per tutti i workspace di un'organizzazione presenti all'interno di una directory specifica (*AD Connector, vedere Identità*).

Tali parametri, come tutte i parametri CloudWatch, possono essere visualizzati nella console di gestione AWS (Figura 13), sono accessibili tramite le API di CloudWatch e vengono monitorati tramite gli allarmi di CloudWatch e strumenti di terze parti.

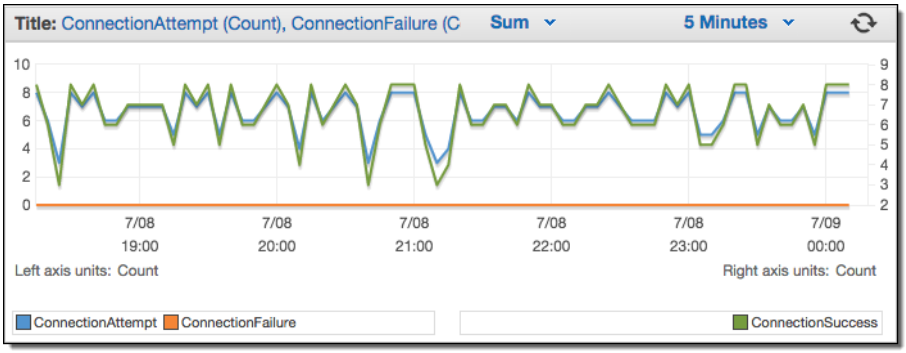

Figura 14: parametri CloudWatch – ConnectionAttempt/ConnectionFailure

Per impostazione predefinita sono abilitati i parametri che seguono senza alcun costo aggiuntivo:

- **Disponibile**: i workspace che rispondono a una verifica di stato rientrano in questo parametro.
- **Non integro**: i workspace che non rispondono alla stessa verifica di stato rientrano in questo parametro.
- **ConnectionAttempt**: il numero di tentativi di connessione a un workspace.
- **ConnectionSuccess**: il numero di tentativi di connessione con esito positivo.
- **ConnectionSuccess**: il numero di tentativi di connessione con esito negativo.
- **SessionLaunchTime**: la quantità di tempo richiesta per inizializzare una sessione, secondo la misurazione effettuata dal client di Amazon WorkSpaces.
- **InSessionLatency**: il round-trip time (RTT) tra il client di Amazon WorkSpaces e Amazon WorkSpaces, secondo la misurazione effettuata e comunicata dal client.
- **SessionDisconnect**: il numero di sessioni inizializzate dall'utente e automaticamente chiuse.

È possibile inoltre creare degli allarmi, come mostra la figura 15.

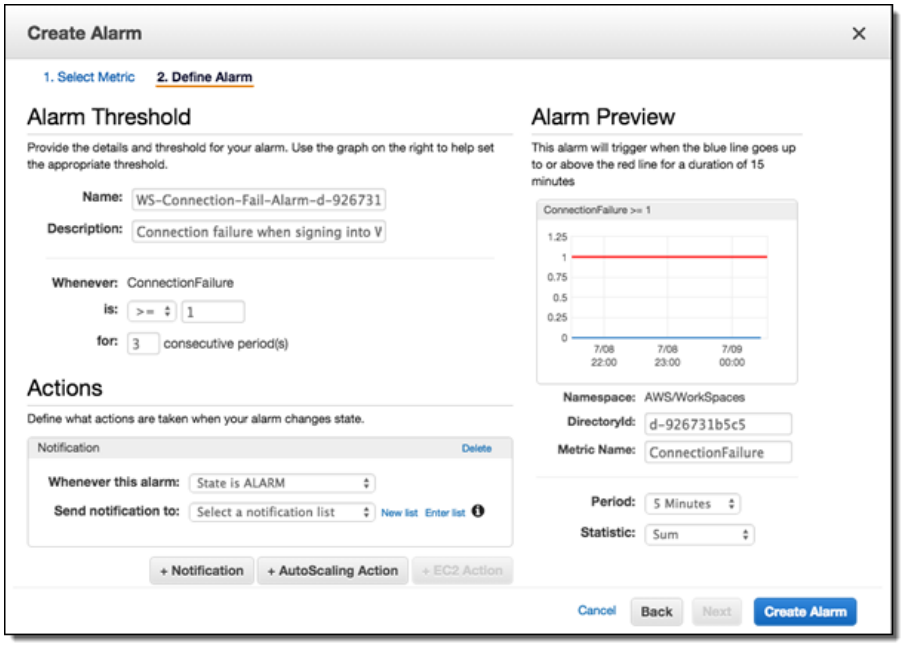

Figura 15: creare un allarme CloudWatch per gli errori di connessione di WorkSpaces

Risoluzione di problemi

Problemi comuni di amministrazione e relativi al client, come "Visualizzo il seguente messaggio di errore: "Il dispositivo non è in grado di collegarsi al servizio di registrazione di WorkSpaces" o "Impossibile collegarsi al workspace con un banner di accesso interattivo" possono essere consultati nelle pagine relative alla risoluzione di problemi del Client e di Admin nella *Guida sull'amministrazione di Amazon WorkSpaces*.

AD Connector non riesce a collegarsi ad Active Directory

Per consentire ad AD Connector di collegarsi alla directory locale, il firewall della rete locale deve avere alcune porte specifiche aperte per i CIDR di entrambi le sottoreti presenti nel VPC (vedere AD Connector). Per verificare se tali requisiti sono soddisfatti, eseguire le operazioni che seguono.

Per verificare la connessione

1. Lanciare un'istanza di Windows nel VPC e collegarla tramite RDP. Le fasi rimanenti vengono eseguite sull'istanza VPC.
2. Scaricare e decomprimere l'applicazione per i test DirectoryServicePortTest. Il codice sorgente e i file Visual Studio di progetto sono inclusi per cui è possibile modificare l'applicazione per i test, se necessario.
3. Da un prompt dei comandi di Windows eseguire l'applicazione per i test DirectoryServicePortTest con le seguenti opzioni:

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
"53,88,135,139,389,445,464,636,49152" -udp "53,88,123,137,138,389,445,464"
<domain_name>
```

<*domain_name*>

Il nome completo del dominio qualificato, usato per testare i livelli funzionali a livello di foresta e di dominio. Se si esclude il nome del dominio non sarà effettuato alcun test sui livelli funzionali.

<*server_IP_address*>

L'indirizzo IP di un controller di dominio nel dominio locale. Le porte saranno testate usando questo indirizzo IP. Se si esclude l'indirizzo IP non sarà effettuato alcun test sulle porte.

Questa operazione stabilirà se le porte necessarie sono aperte dal VPC verso il dominio. L'app di test verifica anche i livelli funzionali minimi a livello di foresta e di dominio.

Come verificare la latenza verso la Regione AWS più vicina

A ottobre 2015, Amazon WorkSpaces ha rilasciato il sito Web Controllo dello stato della connessione. Il sito Web verifica rapidamente se è possibile accedere a tutti i servizi richiesti per usare WorkSpaces. Effettua anche una verifica delle performance per ogni Regione AWS in cui vengono eseguiti i workspace, consentendo così agli utenti di individuare quello più veloce.

Conclusioni

Al momento ci troviamo di fronte a una migrazione strategica verso l'end-user computing, legata alla volontà delle aziende di essere più agili, di proteggere meglio i propri dati e di aiutare i propri dipendenti a essere più produttivi. Molti dei vantaggi ottenuti attraverso il cloud computing possono essere replicati nell'end-user computing. Trasferendo i propri desktop in AWS Cloud con Amazon WorkSpaces, le organizzazioni possono offrire soluzioni scalabili in tempi rapidi al sopraggiungere di nuovi dipendenti, migliorare il proprio livello di sicurezza tenendo i dati lontani dai dispositivi e offrire al proprio personale un desktop a cui è possibile accedere ovunque usando un dispositivo a scelta.

Amazon WorkSpaces è stato progettato per essere integrato in processi e sistemi IT già esistenti e in questo whitepaper vengono descritte le best practice per eseguire tale integrazione. Il risultato delle linee guida presenti in questo whitepaper è una distribuzione nel cloud dei desktop, efficiente da un punto di vista dei costi e in grado di adeguarsi alla crescita del business attraverso l'infrastruttura globale AWS.

Collaboratori

Le persone indicate di seguito hanno collaborato alla stesura di questo documento:

- Justin Bradley, Solutions Architect, Amazon Web Services
- Mahdi Sajjadpour, Senior Consultant, AWS Professional Services
- Mauricio Munoz, Solutions Architect, Amazon Web Services

Letture ulteriori

Per ulteriori informazioni, consultare le seguenti fonti:

- Risoluzione di problematiche di amministrazione di AWS Directory Service
- Risoluzione di problematiche di amministrazione di Amazon WorkSpaces
- Risoluzione di problematiche del client di Amazon WorkSpaces
- Guida per l'amministrazione di Amazon WorkSpaces
- Guida per sviluppatori di Amazon WorkSpaces
- Piattaforme e dispositivi supportati
- In che modo Amazon WorkSpaces usa AWS KMS
- Riferimento ai comandi AWS CLI – workspace
- Monitorare i parametri di Amazon WorkSpaces