AWS 백서

배포 모범 사례 WorkSpaces

배포 모범 사례 WorkSpaces: AWS 백서

Table of Contents

Amazon 배포를 위한 모범 사례 WorkSpaces

발행일: 2022년 6월 1일 () 문서 수정

요약

이 백서에서는 배포를 위한 일련의 모범 사례를 간략하게 설명합니다. WorkSpaces 백서는 네트워크 고려 사항, 디렉터리 서비스, 사용자 인증, 보안, 모니터링 및 로깅에 대해 다룹니다.

또한 이 백서를 통해 관련 정보에 빠르게 액세스할 수 있으며 네트워크 엔지니어, 디렉토리 엔지니어 또는 보안 엔지니어를 대상으로 합니다.

소개

WorkSpacesAmazon은 클라우드의 관리형 데스크톱 컴퓨팅 서비스입니다. Amazon은 하드웨어를 조달 또는 배포하거나 복잡한 소프트웨어를 설치하는 부담을 WorkSpaces 없애고 Amazon Web Services (AWS) 명령줄 인터페이스 (CLI) 를 사용하거나 애플리케이션 프로그래밍 인터페이스 (API) 를 사용하여 클릭 몇 번으로 데스크톱 환경을 제공합니다. AWS Management Console WorkSpacesAmazon을 사용하면 몇 분 안에 Microsoft Windows 또는 Amazon Linux 데스크톱을 시작할 수 있으며, 이를 통해 온프레미스 또는 외부 네트워크에서 데스크톱 소프트웨어에 안전하고 안정적이며 빠르게 연결하고 액세스할 수 있습니다. 다음을 할 수 있습니다.

- 디렉터리 서비스: 액티브 디렉터리 커넥터 (AD Connector) 를 사용하여 AWS 기존의 온-프레미스 Microsoft Active Directory (AD) 를 활용하십시오.
- 디렉터리를 AWS 클라우드로 확장하세요.
- AWS Directory Service Microsoft AD 또는 Simple AD를 사용하여 관리형 디렉터리를 구축하여 사용자를 관리하고 WorkSpaces
- AD Connector와 함께 온-프레미스 또는 클라우드 호스팅 RADIUS 서버를 활용하여 다단계 인증 (MFA) 을 제공합니다. WorkSpaces

CLI 또는 API를 사용하여 Amazon WorkSpaces 프로비저닝을 자동화할 수 있으며, 이를 통해 WorkSpaces Amazon을 기존 프로비저닝 워크플로에 통합할 수 있습니다.

보안을 위해 Amazon WorkSpaces 서비스가 제공하는 통합 네트워크 암호화 외에도 사용자 전용 암호화를 활성화할 수 있습니다 WorkSpaces. 이 문서의 암호화된 WorkSpaces 섹션을 참조하십시오.

Microsoft System Center WorkSpaces Configuration Manager (SCCM), Puppet Enterprise 또는 Ansible과 같은 기존 온-프레미스 도구를 사용하여 애플리케이션을 배포할 수 있습니다.

다음 섹션에서는 WorkSpaces Amazon에 대한 세부 정보를 제공하고, 서비스 작동 방식을 설명하고, 서비스를 시작하는 데 필요한 사항을 설명하고, 사용할 수 있는 옵션 및 기능을 설명합니다.

WorkSpaces 요구 사항

Amazon WorkSpaces 서비스를 성공적으로 배포하려면 세 가지 구성 요소가 필요합니다.

- WorkSpaces 클라이언트 애플리케이션 — Amazon에서 WorkSpaces 지원하는 클라이언트 디바이스. 사용자 계정 WorkSpace 시작하기를 참조하십시오.

  인터넷 프로토콜을 통한 개인용 컴퓨터 (PCoIP) 제로 클라이언트를 사용하여 연결할 수도 있습니다. WorkSpaces 사용 가능한 디바이스 목록은 Amazon용 PCoIP 제로 클라이언트를 참조하십시오. WorkSpaces
- 사용자를 인증하고 사용자에게 액세스를 제공하는 디렉터리 서비스 WorkSpace — Amazon은 WorkSpaces 현재 AWS 디렉터리 서비스 및 Microsoft AD와 협력하고 있습니다. AWS Directory Service와 함께 온프레미스 AD 서버를 사용하여 WorkSpaces Amazon의 기존 엔터프라이즈 사용자 자격 증명을 지원할 수 있습니다.
- Amazon을 실행할 Amazon Virtual Private Cloud (Amazon VPC) WorkSpaces — 각 AWS Directory Service 구조에는 다중 AZ 배포에서 두 개의 서브넷이 필요하기 때문에 Amazon WorkSpaces 배포에는 최소 두 개의 서브넷이 필요합니다.

네트워크 고려 사항

WorkSpace 각각은 이를 생성하는 데 사용한 특정 Amazon VPC 및 AWS 디렉터리 서비스 구조와 연결되어 있습니다. 모든 AWS 디렉터리 서비스 구조 (Simple AD, AD Connector 및 Microsoft AD) 를 사용하려면 각각 다른 가용 영역 (AZ) 에 있는 두 개의 서브넷이 필요합니다. 서브넷은 Directory Service 구조와 영구적으로 연결되며 생성된 후에는 수정할 수 없습니다. 따라서 디렉터리 서비스 구조를 만들기 전에 반드시 올바른 서브넷 크기를 결정해야 합니다. 서브넷을 만들기 전에 다음 사항을 주의 깊게 고려하십시오.

- 시간이 WorkSpaces 지나면 얼마나 필요할까요?
- 예상 성장률은 어느 정도인가요?
- 어떤 유형의 사용자를 수용해야 할까요?
- 연결할 AD 도메인은 몇 개입니까?
- 기업 계정은 어디에 있습니까?

Amazon은 계획 프로세스의 일부로 필요한 액세스 유형 및 사용자 인증을 기반으로 사용자 그룹 또는 페르소나를 정의할 것을 권장합니다. 이러한 질문에 대한 답변은 특정 애플리케이션 또는 리소스에 대한 액세스를 제한해야 할 때 유용합니다. 정의된 사용자 페르소나는 AWS Directory Service, 네트워크 액세스 제어 목록, 라우팅 테이블 및 VPC 보안 그룹을 사용하여 액세스를 세분화하고 제한하는 데 도움이 될 수 있습니다. 각 AWS Directory Service 구문은 두 개의 서브넷을 사용하며 WorkSpaces 해당 구조에서 시작하는 모든 서브넷에 동일한 설정을 적용합니다. 예를 들어 AD Connector에 WorkSpaces 연결된 모든 항목에 적용되는 보안 그룹을 사용하여 MFA가 필요한지 또는 최종 사용자가 MFA에 대한 로컬 관리자 액세스 권한을 가질 수 있는지 여부를 지정할 수 있습니다. WorkSpace

> **Note**
>
> 각 AD Connector는 기존 엔터프라이즈 Microsoft AD에 연결됩니다. 이 기능을 활용하고 OU (조직 구성 단위) 를 지정하려면 사용자 페르소나를 고려하여 Directory Service를 구성해야 합니다.

VPC 설계

이 섹션에서는 VPC 및 서브넷 크기 조정 모범 사례, 트래픽 흐름, 디렉터리 서비스 설계에 미치는 영향을 설명합니다.

확장, 보안 및 관리 용이성을 위한 WorkSpaces 환경을 구축할 수 WorkSpaces 있도록 Amazon의 VPC, 서브넷, 보안 그룹, 라우팅 정책 및 네트워크 액세스 제어 목록 (ACL) 을 설계할 때 고려해야 할 몇 가지 사항은 다음과 같습니다.

- VPC — 배포 전용으로 별도의 VPC를 사용하는 것이 좋습니다. WorkSpaces 별도의 VPC를 사용하면 트래픽을 WorkSpaces 분리하여 필요한 거버넌스 및 보안 가드레일을 지정할 수 있습니다.
- 디렉터리 서비스 — 각 AWS Directory Service 구성에는 AZ 간에 분할된 고가용성 디렉터리 서비스를 제공하는 한 쌍의 서브넷이 필요합니다.
- 서브넷 크기 - WorkSpaces 배포는 디렉터리 구조에 연결되며 선택한 AWS Directory Service 것과 동일한 VPC에 위치하지만 서로 다른 VPC 서브넷에 있을 수 있습니다. 몇 가지 고려 사항:
  - 서브넷 크기는 영구적이며 변경할 수 없습니다. 향후 성장을 위한 충분한 여지를 남겨 두어야 합니다.
  - 선택한 기본 보안 그룹을 지정할 수 있습니다 AWS Directory Service. 보안 그룹은 특정 AWS Directory Service 구성과 관련된 모든 WorkSpaces 항목에 적용됩니다.
  - 동일한 서브넷을 AWS Directory Service 사용하는 여러 인스턴스가 있을 수 있습니다.

VPC를 설계할 때 향후 계획을 고려하세요. 예를 들어 바이러스 백신 서버, 패치 관리 서버, AD 또는 RAD/RADIUS MFA 서버와 같은 관리 구성 요소를 추가할 수 있습니다. 이러한 요구 사항을 수용하려면 VPC 설계에 사용 가능한 추가 IP 주소를 계획하는 것이 좋습니다.

VPC 설계 및 서브넷 크기 조정에 대한 자세한 지침과 고려 사항은 re:Invent 프레젠테이션 Amazon.com이 Amazon으로 이전하는 방법을 참조하십시오. WorkSpaces

네트워크 인터페이스

각 WorkSpaces 인터페이스에는 두 개의 엘라스틱 네트워크 인터페이스 (ENI), 관리 네트워크 인터페이스 () 및 기본 네트워크 인터페이스 (`eth0`) 가 있습니다. `eth1` AWS 관리 네트워크 인터페이스를 사용하여 관리합니다. 관리 네트워크 인터페이스는 클라이언트 연결이 종료되는 인터페이스입니다. WorkSpace AWS 이 인터페이스에 사설 IP 주소 범위를 사용합니다. 네트워크 라우팅이 제대로 작동하려면 WorkSpaces VPC와 통신할 수 있는 네트워크에서 이 프라이빗 주소 공간을 사용해서는 안 됩니다.

지역별로 사용되는 사설 IP 범위 목록은 Amazon Details (Amazon WorkSpaces Details) 를 참조하십시오.

> **Note**
>
> Amazon WorkSpaces 및 관련 관리 네트워크 인터페이스는 VPC에 상주하지 않으므로 사용자는 사용자 VPC에 관리 네트워크 인터페이스 또는 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 ID를 AWS Management Console 볼 수 없습니다 (Figure 5, 및 참조). Figure 6 Figure 7 하지만 콘솔에서 기본 네트워크 인터페이스 (`eth1`) 의 보안 그룹 설정을 보고 수정할 수 있습니다. 각 WorkSpace 인터페이스의 기본 네트워크 인터페이스는 ENI Amazon EC2 리소스 할당량에 포함됩니다. WorkSpacesAmazon을 대량으로 배포하는 경우 ENI 할당량을 AWS Management Console 늘리려면 를 통해 지원 티켓을 열어야 합니다.

트래픽 흐름

Amazon WorkSpaces 트래픽을 두 가지 주요 구성 요소로 나눌 수 있습니다.

- 클라이언트 디바이스와 Amazon WorkSpaces 서비스 간의 트래픽.
- Amazon WorkSpaces 서비스와 고객 네트워크 트래픽 간의 트래픽.

다음 섹션에서는 이 두 구성 요소에 대해 설명합니다.

클라이언트 장치: WorkSpace

위치 (온프레미스 또는 원격) 에 관계없이 Amazon WorkSpaces 클라이언트를 실행하는 디바이스는 Amazon WorkSpaces 서비스에 연결하는 데 동일한 포트 2개를 사용합니다. 클라이언트는 모든 인증 및 세션 관련 정보에 포트 443 (HTTPS 포트) 을 사용하고, 지정된 네트워크 상태 확인으로의 픽셀 스트리밍을 위해 전송 제어 프로토콜 (TCP) 과 사용자 데이터그램 프로토콜 (UDP) 을 모두 사용하는 포트 4172 (PCoIP 포트) 를 사용합니다. WorkSpace 두 포트의 트래픽은 암호화됩니다. 포트 443 트래픽은 인증 및 세션 정보에 사용되며 TLS를 사용하여 트래픽을 암호화합니다. 픽셀 스트리밍 트래픽은 스트리밍 게이트웨이를 통한 클라이언트와 `eth0` 클라이언트 간 통신에 AES-256비트 암호화를 사용합니다. WorkSpace 자세한 내용은 이 문서의 보안 섹션에서 확인할 수 있습니다.

PCoIP 스트리밍 게이트웨이 및 네트워크 상태 점검 엔드포인트의 지역별 IP 범위를 게시합니다. 포트 4172에서 Amazon을 사용하는 특정 AWS 지역으로 향하는 아웃바운드 트래픽만 허용하여 기업 네트워크에서 AWS 스트리밍 게이트웨이 및 네트워크 상태 점검 엔드포인트로 향하는 포트 4172의 아

웃바운드 트래픽을 제한할 수 있습니다. WorkSpaces IP 범위 및 네트워크 상태 점검 엔드포인트는 Amazon WorkSpaces PCoIP 게이트웨이 IP 범위를 참조하십시오.

Amazon WorkSpaces 클라이언트에는 네트워크 상태 검사 기능이 내장되어 있습니다. 이 유틸리티는 애플리케이션 오른쪽 하단의 상태 표시기를 통해 네트워크가 연결을 지원할 수 있는지 여부를 사용자에게 보여줍니다. 다음 그림은 클라이언트의 오른쪽 상단에서 네트워크를 선택하여 액세스할 수 있는 네트워크 상태를 보다 자세히 보여줍니다.

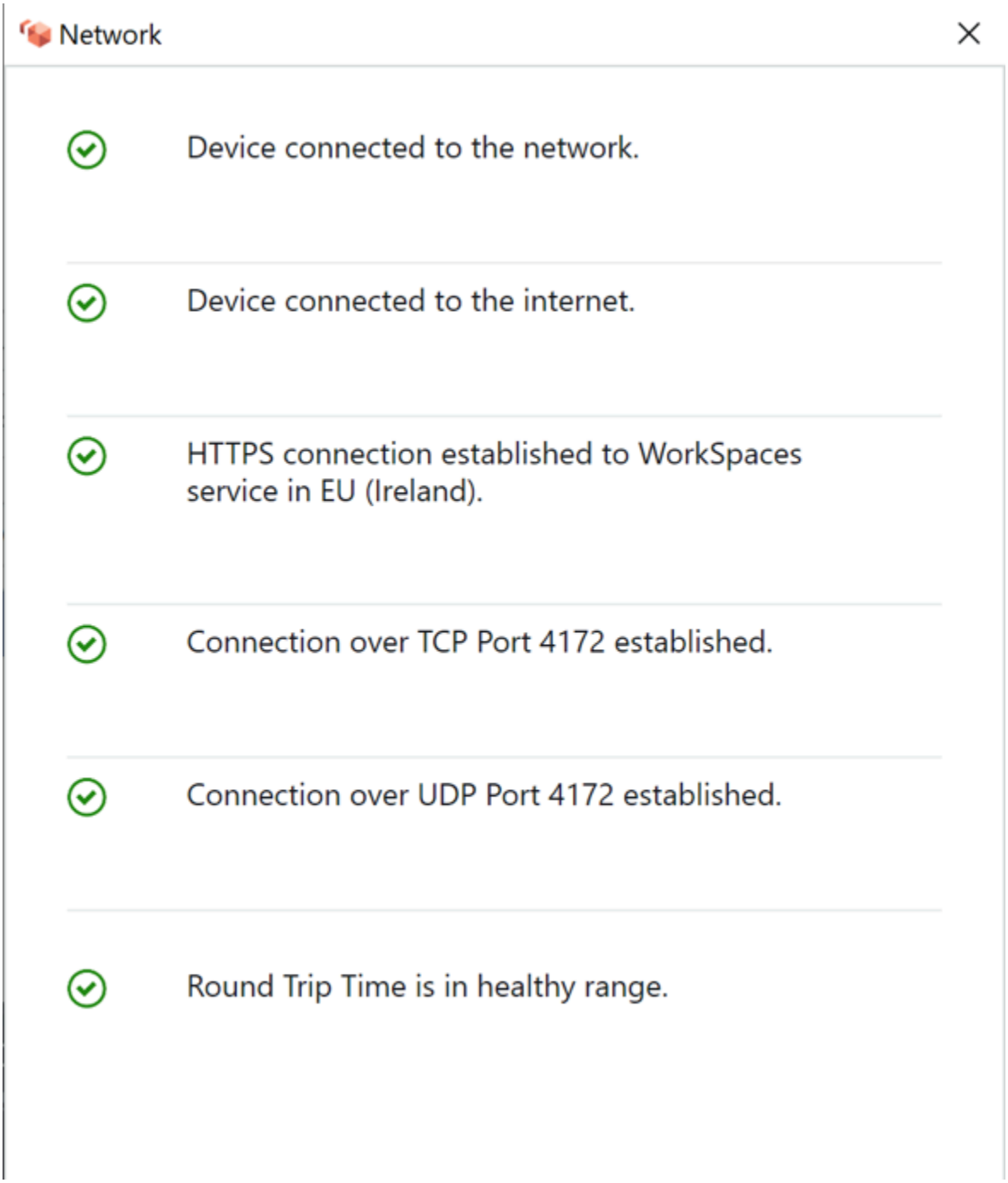

그림 1: WorkSpaces 클라이언트: 네트워크 검사

사용자는 Directory WorkSpaces Service 구조에서 사용하는 디렉토리 (일반적으로 회사 디렉토리) 에 대한 로그인 정보를 제공하여 클라이언트에서 Amazon 서비스로의 연결을 시작합니다. 로그인 정보는 HTTPS를 통해 해당 계정이 위치한 지역의 Amazon WorkSpaces 서비스 인증 게이트웨이로 전송됩니다. WorkSpace 그러면 Amazon WorkSpaces 서비스의 인증 게이트웨이가 트래픽을 WorkSpace 사용자와 관련된 특정 AWS Directory Service 구조로 전달합니다.

예를 들어 AD Connector를 사용하는 경우 AD Connector는 온프레미스 또는 AWS VPC에 있는 AD 서비스에 인증 요청을 직접 전달합니다. 자세한 내용은 이 문서의 AD DS 배포 시나리오 섹션을 참조하십시오. AD Connector는 인증 정보를 저장하지 않으며 상태 비저장 프록시 역할을 합니다. 따라서 AD Connector는 반드시 AD 서버에 연결되어 있어야 합니다. AD 커넥터는 AD 커넥터를 만들 때 정의한 DNS 서버를 사용하여 연결할 AD 서버를 결정합니다.

AD Connector를 사용 중이고 디렉터리에 MFA를 활성화한 경우 디렉터리 서비스 인증 전에 MFA 토큰을 확인합니다. MFA 검증이 실패할 경우 사용자의 로그인 정보는 Directory AWS Service로 전달되지 않습니다.

사용자가 인증되면 포트 4172 (PCoIP 포트) 를 사용하여 스트리밍 게이트웨이를 통해 로 향하는 스트리밍 트래픽이 시작됩니다. AWS WorkSpace 세션 관련 정보는 세션 내내 HTTPS를 통해 계속 교환됩니다. 스트리밍 트래픽은 VPC에 연결되지 않은 WorkSpace (`eth0`on WorkSpace) 의 첫 번째 ENI를 사용합니다. 스트리밍 게이트웨이에서 ENI로의 네트워크 연결은 에서 관리합니다. AWS 스트리밍 게이트웨이에서 WorkSpaces 스트리밍 ENI로의 연결에 장애가 발생하는 경우 CloudWatch 이벤트가 생성됩니다. 자세한 내용은 이 문서의 Amazon을 사용한 모니터링 또는 로깅 CloudWatch 섹션을 참조하십시오.

Amazon WorkSpaces 서비스와 클라이언트 간에 전송되는 데이터의 양은 픽셀 활동 수준에 따라 달라집니다. 최적의 사용자 경험을 보장하기 위해 WorkSpaces 클라이언트와 사용자가 위치한 AWS 지역 간의 왕복 시간 (RTT) 을 100밀리초 (ms) 미만으로 설정하는 WorkSpaces 것이 좋습니다. 일반적으로 이는 WorkSpaces 클라이언트가 호스팅되는 지역에서 2,000마일 미만의 거리에 있다는 것을 의미합니다. WorkSpace Connection Health Check 웹 페이지는 Amazon WorkSpaces 서비스에 연결하기에 가장 적합한 AWS 지역을 결정하는 데 도움이 될 수 있습니다.

WorkSpaces VPC에 대한 아마존 서비스

클라이언트에서 A로의 연결이 WorkSpace 인증되고 스트리밍 트래픽이 시작되면 WorkSpaces 클라이언트에는 가상 사설 클라우드 (VPC WorkSpace) 에 연결된 Windows 또는 Linux 데스크톱 (Amazon) 이 표시되고 네트워크에는 해당 연결이 설정된 것으로 표시됩니다. 로 `eth1` 식별되는 기본 엘라스틱 네트워크 인터페이스 (ENI) 에는 VPC에서 제공하는 동적 호스트 구성 프로토콜 (DHCP) 서비스 (일반

적으로 Directory Service) 와 동일한 서브넷에서 제공되는 IP 주소가 할당됩니다. WorkSpace AWS IP 주소는 수명 기간 WorkSpace 동안 와 함께 유지됩니다. WorkSpace VPC의 ENI는 VPC의 모든 리소스와 사용자가 VPC에 연결된 모든 네트워크 (VPC 피어링, 연결 또는 VPN 연결을 통해) 에 액세스할 수 있습니다. AWS Direct Connect

네트워크 리소스에 대한 ENI 액세스는 AWS Directory Service가 WorkSpace 각각에 대해 구성하는 기본 보안 그룹 및 서브넷의 라우팅 테이블과 ENI에 할당한 추가 보안 그룹에 따라 결정됩니다. 또는 를 사용하여 AWS Management Console 언제든지 VPC와 연결된 ENI에 보안 그룹을 추가할 수 있습니다. AWS CLI (보안 그룹에 대한 자세한 내용은 사용자를 위한 보안 WorkSpaces 그룹을 참조하십시오.) 보안 그룹 외에도 특정 그룹에서 선호하는 호스트 기반 방화벽을 사용하여 VPC 내 리소스에 대한 네트워크 WorkSpace 액세스를 제한할 수 있습니다.

사용자 환경에 맞는 Active Directory에 권한을 부여하는 DNS 서버 IP와 정규화된 도메인 이름을 사용하여 DHCP 옵션 세트를 생성한 다음, 사용자 지정으로 생성한 DHCP 옵션 세트를 Amazon에서 사용하는 Amazon VPC에 할당하는 것이 좋습니다. WorkSpaces 기본적으로 Amazon VPC (가상 사설 클라우드) 는 디렉터리 서비스 AWS DNS 대신 DNS를 사용합니다. DHCP 옵션 세트를 사용하면 본인뿐 아니라 배포를 위해 계획한 지원 워크로드 또는 인스턴스에 대해 내부 DNS 이름 서버를 적절히 확인하고 일관되게 구성할 수 있습니다. WorkSpaces

DHCP 옵션을 적용할 경우 기존 EC2 인스턴스에 적용하는 WorkSpaces 방식과 비교하여 적용 방식에는 두 가지 중요한 차이점이 있습니다.

- 첫 번째 차이점은 DHCP 옵션 DNS 접미사가 적용되는 방식입니다. WorkSpace 각 DNS 접미사 옵션의 기본 및 연결별 DNS 접미사 추가 및 상위 접미사 추가 옵션이 활성화된 상태로 네트워크 어댑터용으로 구성된 DNS 설정이 있습니다. 구성은 기본적으로 등록 및 연결된 AWS Directory Service 내에 구성된 DNS 접미사로 업데이트됩니다. WorkSpace 또한 사용된 DHCP 옵션 세트 내에 구성된 DNS 접미사가 다른 경우 해당 접미사가 추가되어 모든 관련 항목에 적용됩니다. WorkSpaces
- 두 번째 차이점은 Amazon WorkSpaces 서비스가 구성된 디렉터리의 도메인 컨트롤러 IP 주소를 우선시하기 WorkSpace 때문에 구성된 DHCP 옵션 DNS IP가 에 적용되지 않는다는 것입니다.

또는 하이브리드 또는 분할 DNS 환경을 지원하도록 Route 53 프라이빗 호스팅 영역을 구성하고 Amazon WorkSpaces 환경에 적합한 DNS 확인을 확보할 수 있습니다. 자세한 내용은 VPC용 하이브리드 클라우드 DNS 옵션 및 Active Directory를 사용하는 AWS 하이브리드 DNS를 참조하십시오.

> **Note**
>
> VPC에 새 DHCP 옵션 세트 또는 다른 DHCP 옵션 세트를 적용할 때 각각 IP 테이블을 새로 WorkSpace 고쳐야 합니다. 업데이트된 DHCP 옵션 세트로 구성된 VPC에서 ipconfig /renew

를 실행하거나 WorkSpace 재부팅하면 새로 고칠 수 있습니다. AD Connector를 사용하고 연결된 IP 주소/도메인 컨트롤러의 IP 주소를 업데이트하는 경우, 해당 IP 주소/도메인 컨트롤러의 Skylight `DomainJoinDNS` 레지스트리 키를 업데이트해야 합니다. WorkSpaces GPO를 통해 이 작업을 수행하는 것이 좋습니다. 이 레지스트리 키의 경로는 입니다`HKLM:\SOFTWARE\Amazon\Skylight`. AD 커넥터의 DNS 설정을 수정해도 이 `REG_SZ` 값은 업데이트되지 않으며 VPC DHCP 옵션 세트도 이 키를 업데이트하지 않습니다.

이 백서의 AD DS 배포 시나리오 섹션에 있는 그림은 설명된 트래픽 흐름을 보여줍니다.

앞서 설명한 것처럼 Amazon WorkSpaces 서비스는 DNS 확인을 위해 구성된 디렉터리의 도메인 컨트롤러 IP 주소의 우선 순위를 지정하고 DHCP 옵션 세트에 구성된 DNS 서버는 무시합니다. Amazon의 DNS 서버 설정을 보다 세밀하게 제어해야 하는 경우 Amazon WorkSpaces WorkSpaces 관리 가이드의 Amazon용 DNS 서버 업데이트 WorkSpaces 가이드에 WorkSpaces 있는 지침을 사용하여 Amazon용 DNS 서버를 업데이트할 수 있습니다.

에서 AWS 다른 서비스를 WorkSpaces 확인해야 하고 VPC에 설정된 기본 DHCP 옵션을 사용하는 경우 이 VPC의 도메인 컨트롤러 DNS 서비스는 VPC CIDR의 기본 IP 주소에 2를 더한 Amazon DNS 서버를 가리키는 DNS 전달을 사용하도록 구성해야 합니다. 즉, VPC CIDR이 10.0.0.0/24인 경우 DNS를 구성합니다. 10.0.0.2에서 표준 Route 53 DNS 리졸버를 사용하도록 포워딩합니다.

온프레미스 네트워크 리소스의 DNS 확인이 WorkSpaces 필요한 경우 Route 53 Resolver 아웃바운드 엔드포인트를 사용하고, Route 53 전달 규칙을 생성하고, 이 규칙을 이 DNS 확인이 필요한 VPC와 연결할 수 있습니다. 이전 단락에서 설명한 대로 도메인 컨트롤러 DNS 서비스를 VPC의 기본 Route 53 DNS 해석기로 전달하도록 구성한 경우, Amazon Route 53 개발자 안내서의 VPC 간 DNS 쿼리 해결 및 네트워크 가이드에서 DNS 확인 프로세스를 찾을 수 있습니다.

기본 DHCP 옵션 세트를 사용하고 Active Directory 도메인에 속하지 않은 VPC의 다른 호스트가 Active Directory 네임스페이스의 호스트 이름을 확인할 수 있도록 하려면 이 Route 53 리졸버 아웃바운드 엔드포인트를 사용하고 Active Directory 도메인에 대한 DNS 쿼리를 Active Directory DNS 서버로 전달하는 또 다른 Route 53 전달 규칙을 추가할 수 있습니다. 이 Route 53 전달 규칙은 Active Directory DNS 서비스에 연결할 수 있는 Route 53 리졸버 아웃바운드 엔드포인트 및 Active Directory 도메인에서 DNS 레코드를 확인할 수 있도록 설정하려는 모든 VPC와 연결되어야 합니다. WorkSpaces

마찬가지로, Route 53 리졸버 인바운드 엔드포인트를 사용하여 온프레미스 네트워크에서 Active Directory 도메인의 DNS 레코드를 DNS 방식으로 확인할 수 있습니다 WorkSpaces.

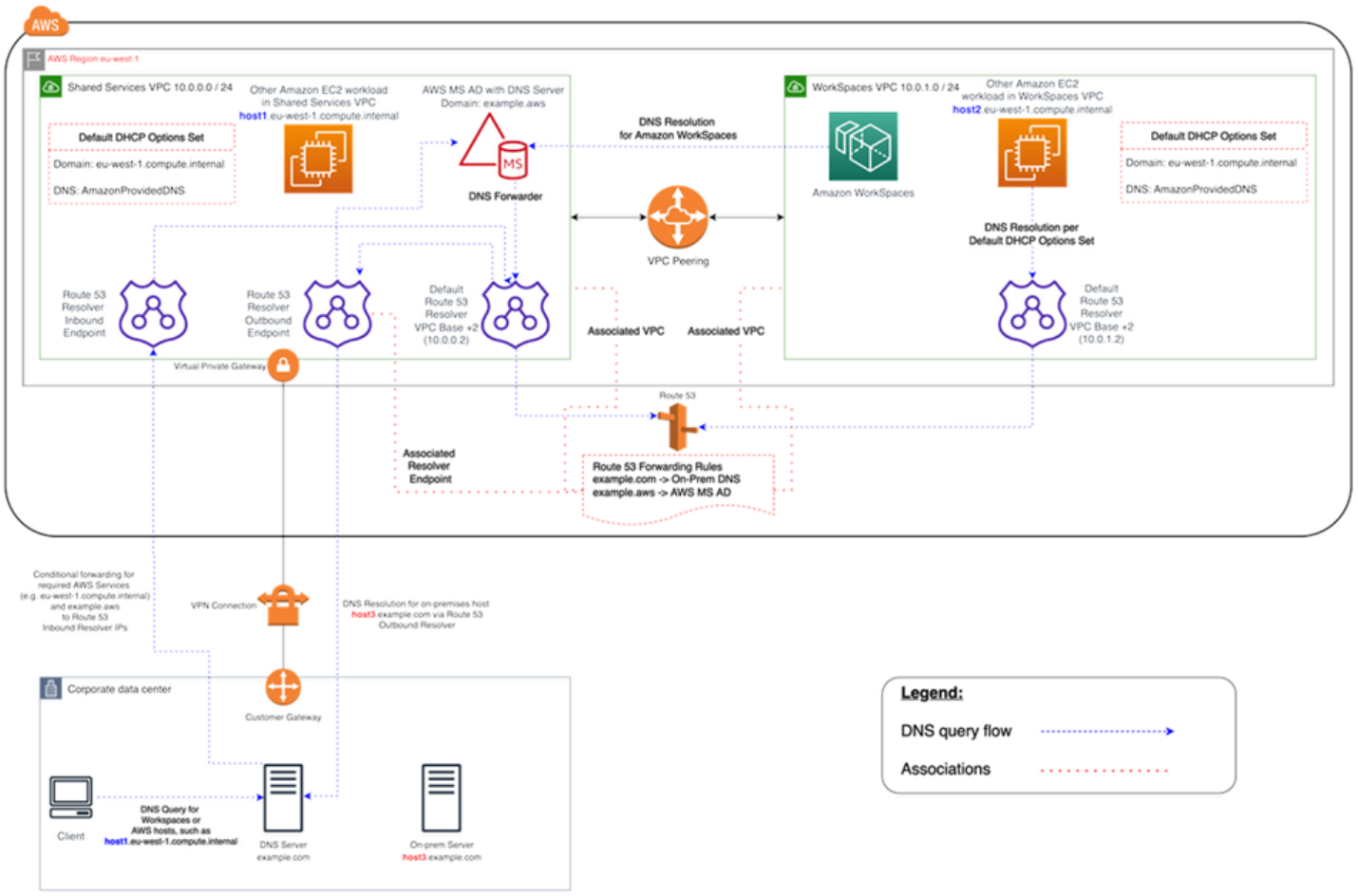

그림 2: Route 53 엔드포인트를 사용한 WorkSpaces DNS 해상도 예제

- WorkSpaces Amazon은 DNS 확인을 위해 AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) DNS 서비스를 사용합니다. AWS Managed Microsoft AD DNS 서비스는 `example.aws` 도메인을 확인하고 다른 모든 DNS 쿼리를 VPC CIDR 기본 IP 주소 +2에 있는 기본 Route 53 DNS 해석기로 전달하여 DNS 확인을 활성화합니다.

  공유 서비스 VPC에는 두 개의 Route 53 전달 규칙과 연결된 Route 53 아웃바운드 리졸버 엔드포인트가 포함되어 있습니다. 이 규칙 중 하나는 `example.com` 도메인에 대한 DNS 쿼리를 온프레미스 DNS 서버로 전달합니다. 두 번째 규칙은 AWS Managed Microsoft AD 도메인에 대한 DNS 쿼리를 공유 서비스 `example.aws` VPC의 Active Directory DNS 서비스에 전달합니다.

  이 아키텍처를 통해 WorkSpaces Amazon은 다음에 대한 DNS 쿼리를 해결할 수 있습니다.

  - 귀하의 AWS Managed Microsoft AD 도메인`example.aws`.
  - 기본 DHCP 옵션 세트 (예:`host1.eu-west-1.compute.internal`) 와 기타 AWS 서비스 또는 엔드포인트로 구성된 도메인의 EC2 인스턴스

  - 온프레미스 도메인의 호스트 및 서비스 (예: `host3.example.com`
- • Route 53 전달 규칙이 두 VPC에 모두 연결되어 있는 한 WorkSpaces, 공유 서비스 WorkSpaces VPC (`host2.eu-west-1.compute.internal`) 및 VPC () 의 다른 EC2 워크로드는 사용자와 동일한 DNS 확인을 수행할 수 있습니다. `host1.eu-west-1.compute.internal` 이 경우 `example.aws` 도메인에 대한 DNS 확인은 VPC CIDR 기본 IP 주소 +2에 있는 기본 Route 53 DNS 확인자를 통해 이루어지며, 구성되고 연결된 Route 53 전달 규칙에 따라 Route 53 확인자 아웃바운드 엔드포인트를 통해 Active Directory DNS 서비스로 전달됩니다. WorkSpaces
- • 마지막으로, 온프레미스 DNS 서버가 `example.aws` 및 `eu-west-1.compute.internal` 도메인에 대한 조건부 전달자로 구성되어 이러한 도메인에 대한 DNS 쿼리를 Route 53 Resolver 인바운드 엔드포인트 IP 주소로 전달하므로 온프레미스 클라이언트도 동일한 DNS 확인을 수행할 수 있습니다.

일반적인 구성의 예

두 가지 유형의 사용자가 있고 AWS Directory Service에서 사용자 인증에 중앙 집중식 AD를 사용하는 시나리오를 가정해 보겠습니다.

- 어디서나 완전한 액세스가 필요한 작업자 (예: 정규직 직원) — 이러한 사용자는 인터넷 및 내부 네트워크에 대한 전체 액세스 권한을 갖게 되며 VPC에서 온프레미스 네트워크로 방화벽을 통과합니다.
- 회사 네트워크 내부에서만 액세스를 제한해야 하는 작업자 (예: 계약업체 및 컨설턴트) — 이러한 사용자는 프록시 서버를 통해 VPC의 특정 웹 사이트에 대한 인터넷 액세스를 제한하고 VPC와 온프레미스 네트워크에 대한 네트워크 액세스가 제한됩니다.

정규직 직원에게 로컬 관리자 액세스 권한을 부여하여 소프트웨어를 설치할 수 있게 WorkSpace 하고, MFA를 통해 2단계 인증을 적용하고 싶습니다. 또한 정규직 직원이 제한 없이 인터넷에 액세스할 수 있도록 허용해야 합니다. WorkSpace

계약업체의 경우 사전 설치된 특정 애플리케이션만 사용할 수 있도록 로컬 관리자 액세스를 차단해야 합니다. 이에 대한 보안 그룹을 사용하여 제한적인 네트워크 액세스 제어를 적용하려고 합니다. WorkSpaces 포트 80과 443을 특정 내부 웹 사이트에만 열고 해당 웹 사이트의 인터넷 액세스를 완전히 차단해야 합니다.

이 시나리오에는 네트워크 및 데스크톱 액세스에 대한 요구 사항이 서로 다른 완전히 다른 두 가지 유형의 사용자 페르소나가 있습니다. 이들을 WorkSpaces 다르게 관리하고 구성하는 것이 가장 좋습니다. 각 사용자 페르소나마다 하나씩, 두 개의 AD 커넥터를 만들어야 합니다. 각 AD Connector에는 WorkSpaces 사용량 증가 예상치를 충족하기에 충분한 IP 주소가 있는 두 개의 서브넷이 필요합니다.

> **Note**
>
> 각 AWS VPC 서브넷은 관리 목적으로 5개의 IP 주소 (처음 4개와 마지막 IP 주소) 를 사용하며, 각 AD Connector는 유지되는 각 서브넷에서 하나의 IP 주소를 사용합니다.

이 시나리오에 대한 추가 고려 사항은 다음과 같습니다.

- AWS VPC 서브넷은 사설 서브넷이어야 합니다. 그래야 인터넷 액세스와 같은 트래픽이 네트워크 주소 변환 (NAT) 게이트웨이, 클라우드의 프록시 NAT 서버를 통해 제어되거나 온프레미스 트래픽 관리 시스템을 통해 다시 라우팅될 수 있습니다.
- 온프레미스 네트워크로 향하는 모든 VPC 트래픽에는 방화벽이 있습니다.
- Microsoft AD 서버와 MFA RADIUS 서버는 온프레미스 (이 문서의 시나리오 1: AD Connector를 사용하여 온-프레미스 AD DS에 대한 프록시 인증 참조) 이거나 AWS 클라우드 구현의 일부 (이 문서의 시나리오 2 및 시나리오 3, AD DS 배포 시나리오 참조) 입니다.

모든 사용자에게 일정한 형태의 인터넷 액세스가 WorkSpaces 허용되고 프라이빗 서브넷에서 호스팅된다는 점을 고려하면 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있는 퍼블릭 서브넷도 만들어야 합니다. 정규직 직원이 인터넷에 액세스할 수 있도록 허용하는 NAT 게이트웨이와 컨설턴트와 계약자가 특정 내부 웹 사이트에 대한 액세스를 제한할 수 있는 프록시 NAT 서버가 필요합니다. 장애에 대비하고, 고가용성을 고려하여 설계하고, AZ 간 트래픽 요금을 제한하려면 다중 AZ 배포에서 두 개의 서로 다른 서브넷에 두 개의 NAT 게이트웨이와 NAT 또는 프록시 서버가 있어야 합니다. 영역이 두 개 이상인 지역에서 퍼블릭 서브넷으로 선택한 두 AZ는 WorkSpaces 서브넷에 사용하는 두 AZ와 일치합니다. 각 WorkSpaces AZ의 모든 트래픽을 해당 퍼블릭 서브넷으로 라우팅하여 AZ 간 트래픽 요금을 제한하고 관리를 더 쉽게 할 수 있습니다. 다음 그림은 VPC 구성을 보여줍니다.

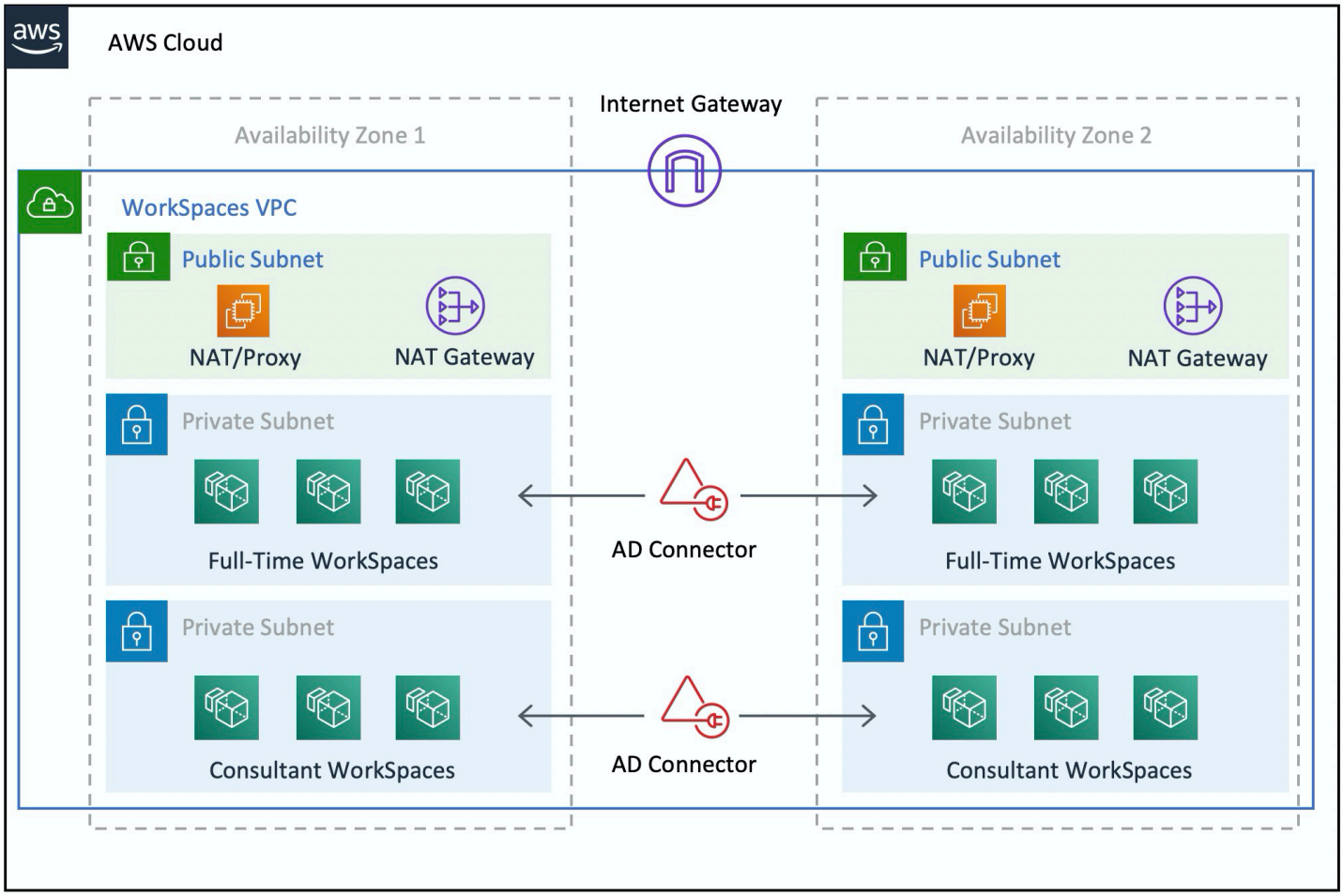

그림 3: 높은 수준의 VPC 설계

다음 정보는 두 가지 WorkSpaces 유형을 구성하는 방법을 설명합니다.

정규직 WorkSpaces 직원을 구성하려면:

1. Amazon WorkSpaces 관리 콘솔의 메뉴 표시줄에서 디렉터리 옵션을 선택합니다.
2. 정규직 직원을 호스팅하는 디렉터리를 선택하십시오.
3. 로컬 관리자 설정을 선택합니다.

이 옵션을 활성화하면 새로 만든 모든 사용자가 로컬 관리자 권한을 WorkSpace 갖게 됩니다. 인터넷 액세스를 허용하려면 VPC에서 아웃바운드 인터넷에 액세스할 수 있도록 NAT를 구성하십시오. MFA를 활성화하려면 RADIUS 서버, 서버 IP, 포트 및 사전 공유 키를 지정해야 합니다.

정규직 직원의 WorkSpaces 경우 AD Connector 설정을 통해 기본 보안 그룹을 적용하여 Helpdesk 서브넷의 RDP (원격 데스크톱 프로토콜) 로 인바운드 트래픽을 제한할 WorkSpace 수 있습니다.

계약자 및 컨설턴트를 위해 WorkSpaces 구성하려면:

1. Amazon WorkSpaces 관리 콘솔에서 인터넷 액세스 및 로컬 관리자 설정을 비활성화합니다.
2. 보안 그룹 설정 섹션 아래에 보안 그룹을 추가하여 해당 디렉터리에 새로 WorkSpaces 생성된 모든 보안 그룹에 보안 그룹을 적용합니다.

컨설턴트의 WorkSpaces 경우 AD Connector 설정을 통한 기본 보안 그룹을 AD Connector와 연결된 모든 WorkSpaces 그룹에 WorkSpaces 적용하여 아웃바운드 및 인바운드 트래픽을 로 제한하십시오. 보안 그룹은 HTTP 및 HTTPS 트래픽 이외의 다른 WorkSpaces 트래픽으로의 아웃바운드 액세스와 온프레미스 네트워크의 헬프데스크 서브넷에서 RDP로의 인바운드 트래픽을 차단합니다.

> **Note**
>
> 보안 그룹은 VPC `eth1` (on WorkSpace) 에 있는 ENI에만 적용되며, 보안 그룹의 결과로 클라이언트에서의 액세스는 제한되지 않습니다. WorkSpace WorkSpaces 다음 그림은 최종 WorkSpaces VPC 설계를 보여줍니다.

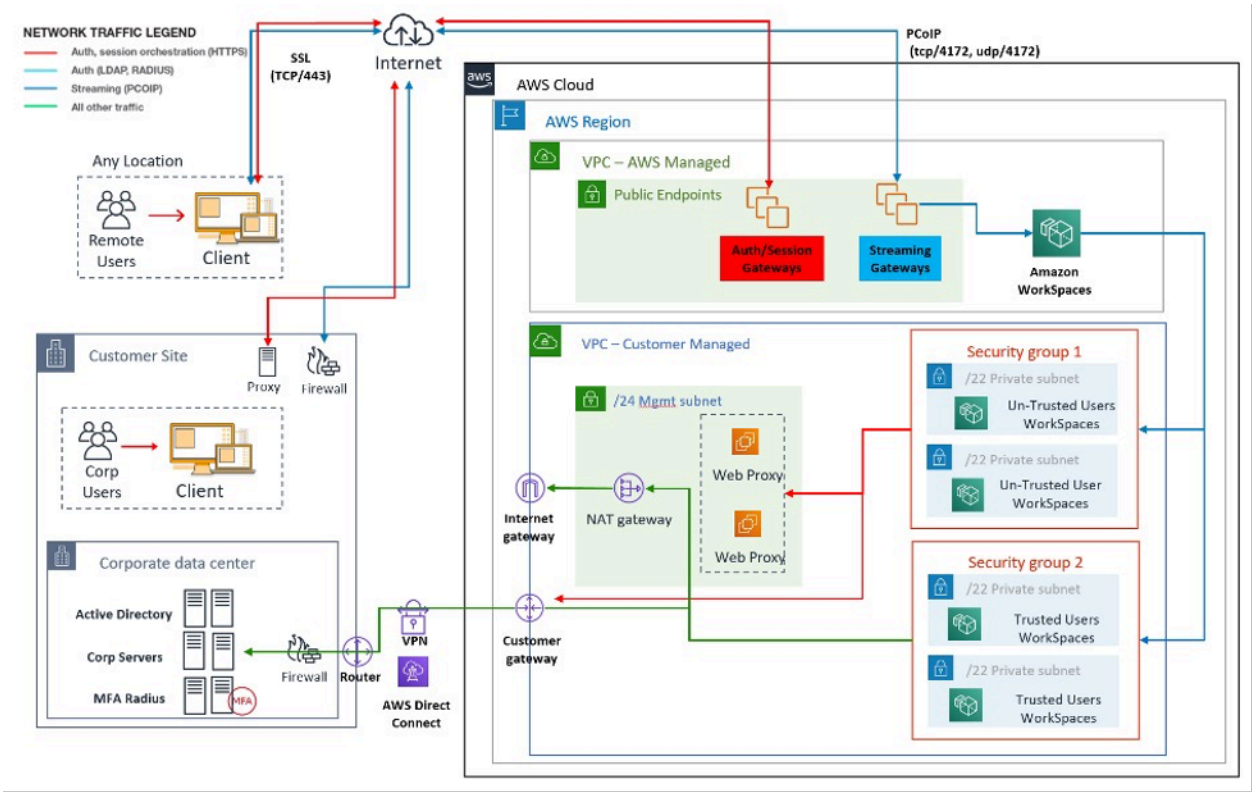

그림 4: 사용자 페르소나를 활용한 WorkSpaces 디자인

AWS Directory 서비스

서론에서 언급했듯이 AWS Directory Service는 Amazon의 핵심 구성 요소입니다 WorkSpaces. AWS Directory Service를 사용하면 WorkSpaces Amazon에서 세 가지 유형의 디렉터리를 생성할 수 있습니다.

- AWS 매니지드 마이크로소프트 AD는 윈도우 서버 2012 R2로 구동되는 매니지드 마이크로소프트 AD입니다. AWS 관리형 Microsoft AD는 스탠다드 또는 엔터프라이즈 에디션으로 제공됩니다.
- Simple AD는 Samba 4를 기반으로 하는 Microsoft AD와 호환되는 독립 실행형 관리형 디렉터리 서비스입니다.
- AD Connector는 인증 요청 및 사용자 또는 그룹 조회를 기존 온-프레미스 Microsoft AD로 리디렉션하기 위한 디렉터리 프록시입니다.

다음 섹션에서는 Amazon WorkSpaces 중개 서비스와 디렉터리 서비스 간의 인증을 위한 통신 흐름, AWS Directory Service를 WorkSpaces 사용한 AWS 구현 모범 사례, 고급 개념 (예: MFA) 에 대해 설명합니다. 또한 대규모 Amazon의 인프라 아키텍처 개념, Amazon WorkSpaces VPC의 요구 사항, 온프레미스 Microsoft AD 도메인 서비스 (AD DS) 와의 통합을 비롯한 디렉터리 서비스에 대해서도 설명합니다. AWS

AD DS 배포 시나리오

Amazon의 지원은 AWS 디렉터리 WorkSpaces 서비스이며, 디렉터리 서비스를 적절하게 설계하고 배포하는 것이 매우 중요합니다. 다음 6가지 시나리오는 AWS 퀵 스타트 가이드의 Active Directory 도메인 서비스를 기반으로 하며 Amazon과 함께 사용할 때 AD DS의 배포 옵션에 대한 모범 사례를 설명합니다 WorkSpaces. 이 문서의 설계 고려 사항 섹션에서는 전체 WorkSpaces 설계 개념의 필수적인 부분인 AD Connector를 사용하기 위한 WorkSpaces 특정 요구 사항과 모범 사례를 자세히 설명합니다.

- 시나리오 1: AD Connector를 사용하여 온-프레미스 AD DS에 대한 프록시 인증 - 이 시나리오에서는 고객에게 네트워크 연결 (VPN/Direct Connect) 이 제공되며, 모든 인증은 Directory Service (AD Connector) AWS 를 통해 고객 온-프레미스 AD DS로 프록시됩니다.
- 시나리오 2: 온-프레미스 AD DS를 AWS (복제본) 으로 확장 - 이 시나리오는 시나리오 1과 비슷하지만, 여기서는 고객 AD DS의 복제본이 AD Connector와 함께 배포되므로 AD DS 및 AD DS 글로벌 카탈로그에 대한 AWS 인증/쿼리 요청 지연 시간이 줄어듭니다.
- 시나리오 3: AWS 클라우드의 AWS Directory Service를 사용하는 독립형 격리 배포 — 이는 격리된 시나리오이며 인증을 위한 고객과의 연결은 포함되지 않습니다. 이 접근 방식에서는 AWS 디렉터리 서비스 (Microsoft AD) 와 AD 커넥터를 사용합니다. 이 시나리오에서는 인증을 위해 고객과의 연결을 사용하지 않지만 필요한 경우 VPN 또는 Direct Connect를 통해 애플리케이션 트래픽을 프로비저닝합니다.
- 시나리오 4: AWS Microsoft AD 및 온-프레미스로의 양방향 전이적 신뢰 — 이 시나리오에는 온-프레미스 AWS Microsoft AD 포리스트에 대한 양방향 전이적 트러스트를 사용하는 관리형 Microsoft AD 서비스 (MAD) 가 포함됩니다.
- 시나리오 5: 공유 서비스 VPC를 사용하는 AWS Microsoft AD - 이 시나리오에서는 공유 서비스 VPC의 관리형 AWS Microsoft AD를 사용하여 여러 서비스 (AWS Amazon EC2 WorkSpaces, Amazon 등) 의 자격 증명 도메인으로 사용하고 AD Connector를 사용하여 경량 디렉터리 액세스 프로토콜 (LDAP) 사용자 인증 요청을 AD 도메인 컨트롤러에 프록시합니다.
- 시나리오 6: AWS Microsoft AD, Shared Services VPC 및 온-프레미스 AD에 대한 단방향 신뢰 — 이 시나리오는 시나리오 5와 비슷하지만 온-프레미스에 대한 단방향 트러스트를 사용하는 서로 다른 ID 및 리소스 도메인을 포함합니다.

Active Directory 도메인 서비스 (ADDS) 배포 시나리오를 선택할 때는 몇 가지 사항을 고려해야 합니다. 이 섹션에서는 WorkSpaces Amazon에서 AD Connector의 역할을 설명하고 ADDS 배포 시나리오를 선택할 때 고려해야 할 몇 가지 중요한 사항을 다룹니다. ADDS의 설계 및 계획에 대한 AWS 자세한 지침은 Active Directory 도메인 서비스 AWS 설계 및 계획 가이드를 참조하십시오.

아마존에서 AWS AD 커넥터의 역할 WorkSpaces

AWS AD AWS Connector는 Active Directory의 프록시 서비스 역할을 하는 디렉터리 서비스입니다. 사용자 자격 증명을 저장하거나 캐시하지는 않지만 인증 또는 조회 요청을 Active Directory (온프레미스 또는 온프레미스) 에 전달합니다. AWS 를 사용하지 않는 한 Amazon WorkSpaces () 에서 사용하기 AWS Managed Microsoft AD 위해 Active Directory (온프레미스 또는 확장 AWS) 를 등록할 수 있는 유일한 방법이기도 합니다. WorkSpaces

AD 커넥터는 온프레미스 Active Directory, 확장된 Active Directory AWS (Amazon EC2의 AD 도메인 컨트롤러) 또는 를 가리킬 수 있습니다. AWS Managed Microsoft AD

AD Connector는 다음 섹션에서 다루는 대부분의 배포 시나리오에서 중요한 역할을 합니다. AD Connector와 함께 WorkSpaces 사용하면 다음과 같은 여러 가지 이점이 있습니다.

- 회사 Active Directory를 가리키면 사용자는 기존 회사 자격 증명을 사용하여 WorkSpaces Amazon 과 같은 다른 서비스에 로그온할 수 WorkDocs 있습니다.
- 사용자가 온프레미스 인프라 또는 기타 인프라의 리소스에 액세스하는지 여부에 관계없이 기존 보안 정책 (암호 만료, 계정 잠금 등) 을 일관되게 적용할 수 있습니다. AWS 클라우드 WorkSpaces
- AD Connector를 사용하면 기존 RADIUS 기반 MFA 인프라와 간단하게 통합하여 추가 보안 계층을 제공할 수 있습니다.
- 이를 통해 사용자를 분리할 수 있습니다. 예를 들어 사용자 인증을 위해 여러 AD 커넥터가 Active Directory의 동일한 도메인 컨트롤러 (DNS 서버) 를 가리킬 수 있으므로 사업부 또는 개인 사용자별로 다양한 WorkSpaces 옵션을 구성할 수 있습니다.
  - Active Directory GPO (그룹 정책 개체) 의 대상 적용을 위한 대상 도메인 또는 조직 구성 단위
  - 들어오고 나가는 트래픽 흐름을 제어하는 다양한 보안 그룹 WorkSpaces
  - 다양한 액세스 제어 옵션 (허용된 클라이언트 장치) 및 IP 액세스 제어 그룹 (IP 범위에 대한 액세스 제한)
  - 로컬 관리자 권한의 선택적 활성화
  - 다양한 셀프 서비스 권한
  - 다중 요소 인증 (MFA) 의 선택적 적용
  - 격리를 위해 WorkSpaces 엘라스틱 네트워크 인터페이스 (ENI) 를 여러 VPC 또는 서브넷에 배치

또한 소형 또는 대형 AD 커넥터 하나의 성능 한계에 도달하는 경우 여러 AD 커넥터를 사용하면 더 많은 사용자를 지원할 수 있습니다. 자세한 내용은 크기 조정 AWS Managed Microsoft AD 섹션을 참조하십시오.

소형 AD 커넥터에는 활성 사용자가 한 명 이상 있고 대형 AD 커넥터에는 활성 WorkSpaces 사용자가 100명 이상이면 AD 커넥터를 무료로 사용할 수 있습니다. WorkSpaces WorkSpaces 자세한 내용은 AWS 디렉터리 서비스 요금 페이지를 참조하십시오.

온-프레미스 Active Directory를 AWS 사용한 네트워크 링크의 중요성

WorkSpaces 액티브 디렉터리와의 연결에 의존합니다. 따라서 Active Directory에 대한 네트워크 링크의 가용성이 가장 중요합니다. 예를 들어 시나리오 1의 네트워크 링크가 다운되면 사용자는 인증을 받을 수 없게 되고 결과적으로 네트워크 링크를 사용할 수 없게 됩니다. WorkSpaces

온-프레미스 Active Directory를 시나리오의 일부로 사용하려면 네트워크 연결의 복원력, 지연 시간 및 트래픽 비용을 고려해야 합니다. AWS 다중 지역 WorkSpaces 배포의 경우 여기에는 서로 다른 AWS 지역에 있는 여러 네트워크 링크가 포함되거나, 온프레미스 AD에 연결된 상태에서 AD 트래픽을 VPC로 라우팅하기 위해 두 지역 간에 피어링이 설정된 여러 AWS Transit Gateway 개의 네트워크 링크가 포함될 수 있습니다. 이러한 네트워크 링크 고려 사항은 다음 섹션에 설명된 대부분의 시나리오에 적용되지만, AD 커넥터의 AD 트래픽이 온프레미스 Active Directory에 도달하기 위해 네트워크 링크를 WorkSpaces 통과해야 하는 시나리오에 특히 중요합니다. 시나리오 1에서는 몇 가지 주의 사항을 중점적으로 설명합니다.

다단계 인증 사용: WorkSpaces

MFA (Multi-Factor Authentication) WorkSpaces 를 사용하려는 경우 AD AWS Connector 또는 AWS Managed Microsoft AD an을 사용해야 합니다. 이러한 서비스에서만 RADIUS에서 사용할 WorkSpaces 디렉터리를 등록하고 RADIUS를 구성할 수 있기 때문입니다. RADIUS 서버를 배치할 때는 온-프레미스 Active Directory를 AWS 사용한 네트워크 링크의 중요성 섹션에서 다룬 네트워크 연결 고려 사항이 적용됩니다.

계정과 리소스 도메인 분리

보안상의 이유나 관리 용이성을 위해 계정 도메인과 리소스 도메인을 분리하는 것이 좋을 수 있습니다. 예를 들어, WorkSpaces 컴퓨터 개체는 별도의 리소스 도메인에 배치하고 사용자는 계정 도메인에 속해 있습니다. 이와 같은 구현을 사용하면 파트너 조직이 계정 도메인에 대한 제어권을 포기하거나 액세스 권한을 부여하지 않으면서 리소스 도메인의 AD 그룹 정책 WorkSpaces 사용을 관리할 수 있습니다. Active Directory 트러스트가 구성된 두 개의 액티브 디렉터리를 사용하면 이 작업을 수행할 수 있습니다. 다음 섹션에서는 이에 대해 더 자세히 다룹니다.

- 시나리오 4: AWS Microsoft AD 및 온-프레미스로의 양방향 전이적 신뢰
- 시나리오 6: AWS Microsoft AD, 공유 서비스 VPC, 온프레미스로의 단방향 트러스트

대규모 액티브 디렉터리 배포

Active Directory 사이트 및 서비스가 적절하게 구성되어 있는지 확인해야 합니다. 이는 Active Directory가 서로 다른 지리적 위치에 있는 많은 수의 도메인 컨트롤러로 구성된 경우 특히 중요합니다. Windows는 표준 Microsoft 메커니즘을 WorkSpaces 사용하여 할당된 Active Directory 사이트에 대한 도메인 컨트롤러를 검색합니다. 이 DC 로케이터 프로세스는 DNS를 사용하며 DC 로케이터 프로세스의 초기 단계에서 우선 순위와 가중치가 지정되지 않은 긴 도메인 컨트롤러 목록이 반환되는 경우 상당히 오래 걸릴 수 있습니다. 더 중요한 것은 최적이 아닌 도메인 컨트롤러에 "고정"되면 광역 네트워크 링크를 통과할 때 이 도메인 컨트롤러와의 모든 후속 통신에 네트워크 지연 시간이 증가하고 대역폭이 감소할 수 있다는 점입니다. WorkSpaces 이렇게 하면 잠재적으로 많은 수의 그룹 정책 개체 (GPO) 처리 및 도메인 컨트롤러로부터의 파일 전송을 포함하여 도메인 컨트롤러와의 모든 통신 속도가 느려집니다. 네트워크 토폴로지에 따라 도메인 컨트롤러 간에 WorkSpaces 교환되는 데이터가 비용이 많이 드는 네트워크 경로를 불필요하게 통과할 수 있기 때문에 네트워킹 비용이 증가할 수도 있습니다. VPC 설계의 VPC 설계 DHCP 및 DNS, Active Directory 사이트 및 서비스에 대한 지침은 및 설계 고려 사항 섹션을 참조하십시오.

다음과 함께 Microsoft Azure 액티브 디렉터리 또는 액티브 디렉터리 도메인 서비스 사용 WorkSpaces

Microsoft Azure Active Directory를 와 함께 WorkSpaces 사용하려는 경우 Azure AD Connect를 사용하여 자격 증명을 온-프레미스 Active Directory나 AWS (Amazon EC2의 도메인 컨트롤러) 의 액티브 디렉터리와 동기화할 수 있습니다. AWS Managed Microsoft AD 하지만 이렇게 하면 Azure Active Directory에 WorkSpaces 가입할 수 없습니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft 하이브리드 ID 설명서를 참조하십시오.

Azure 액티브 디렉터리에 WorkSpaces 가입하려면 Microsoft Azure Active Directory 도메인 서비스 (Azure AD DS) 를 AWS 배포하고, Azure 간에 연결을 설정하고, Azure AD DS 도메인 컨트롤러를 가리키는 AWS AD 커넥터를 사용해야 합니다. 이를 설정하는 방법에 대한 자세한 내용은 Azure Active Directory 도메인 서비스를 사용하여 Azure AD에 WorkSpaces 추가하기 블로그 게시물을 참조하십시오.

AWS Directory Services와 함께 WorkSpaces 사용할 때는 WorkSpaces 배포 크기와 예상 성장률을 고려하여 적절한 크기를 조정해야 합니다. AWS Directory Service 이 섹션에서는 에서 사용할 크기 조정에 AWS Directory Service 대한 지침을 제공합니다. WorkSpaces 또한 AWS Directory Service 관리 가이드의 섹션에서 AD Connector의 모범 사례와 모범 사례 AWS Managed Microsoft AD 섹션을 검토하는 것이 좋습니다.

AD 커넥터 크기 조정 (포함) WorkSpaces

Active Directory 커넥터 (AD 커넥터) 는 소형과 대형의 두 가지 크기로 제공됩니다. 사용자 또는 연결 제한이 적용되지는 않지만, WorkSpaces 권한이 있는 사용자 최대 500명까지는 소형 AD Connector를 사용하고, 최대 WorkSpaces 5000명의 자격 있는 사용자에게는 대형 AD Connector를 사용하는 것이 좋습니다. 애플리케이션 부하를 여러 AD Connector에 분산하여 성능 요구 사항에 맞게 확장할 수 있습니다. 예를 들어 WorkSpaces 1500명의 사용자를 지원해야 하는 경우 각각 500명의 사용자를 지원하는 3개의 소형 AD Connector에 WorkSpaces 균등하게 분산할 수 있습니다. 모든 사용자가 같은 도메인에 있는 경우 AD 커넥터는 모두 Active Directory 도메인을 확인하는 동일한 DNS 서버 집합을 가리킬 수 있습니다.

참고, 처음에는 AD Connector가 작게 시작했고 시간이 지나면서 WorkSpaces 배포 규모가 커지면 사용 WorkSpaces 권한이 있는 많은 사용자를 처리하기 위해 AD Connector의 크기를 소형에서 대형으로 변경하도록 지원 티켓을 제출할 수 있습니다.

크기 조정 AWS Managed Microsoft AD

AWS Managed Microsoft ADMicrosoft Active Directory를 관리 서비스로 실행할 수 있습니다. 서비스를 시작할 때 스탠다드 에디션과 엔터프라이즈 에디션 중에서 선택할 수 있습니다. Standard Edition은 최대 5,000명의 사용자가 있는 중소기업에 권장되며 사용자, 그룹, 컴퓨터 등 약 30,000개의 디렉터리 객체를 지원합니다. Enterprise Edition은 최대 500,000개의 디렉터리 개체를 지원하도록 설계되었으며 다중 지역 복제와 같은 추가 기능도 제공합니다.

500,000개 이상의 디렉터리 객체를 지원해야 하는 경우 Amazon EC2에 Microsoft Active Directory 도메인 컨트롤러를 배포하는 것을 고려해 보십시오. 이러한 도메인 컨트롤러의 크기 조정에 대한 내용은 Microsoft의 Active Directory 도메인 서비스 용량 계획 문서를 참조하십시오.

시나리오 1: AD 커넥터를 사용하여 온-프레미스 Active Directory 서비스에 대한 프록시 인증

이 시나리오는 온-프레미스 AD 서비스를 확장하고 싶지 않거나 AD DS를 새로 배포할 AWS 수 없는 고객을 위한 것입니다. 다음 그림은 각 구성 요소와 사용자 인증 흐름을 개괄적으로 보여줍니다.

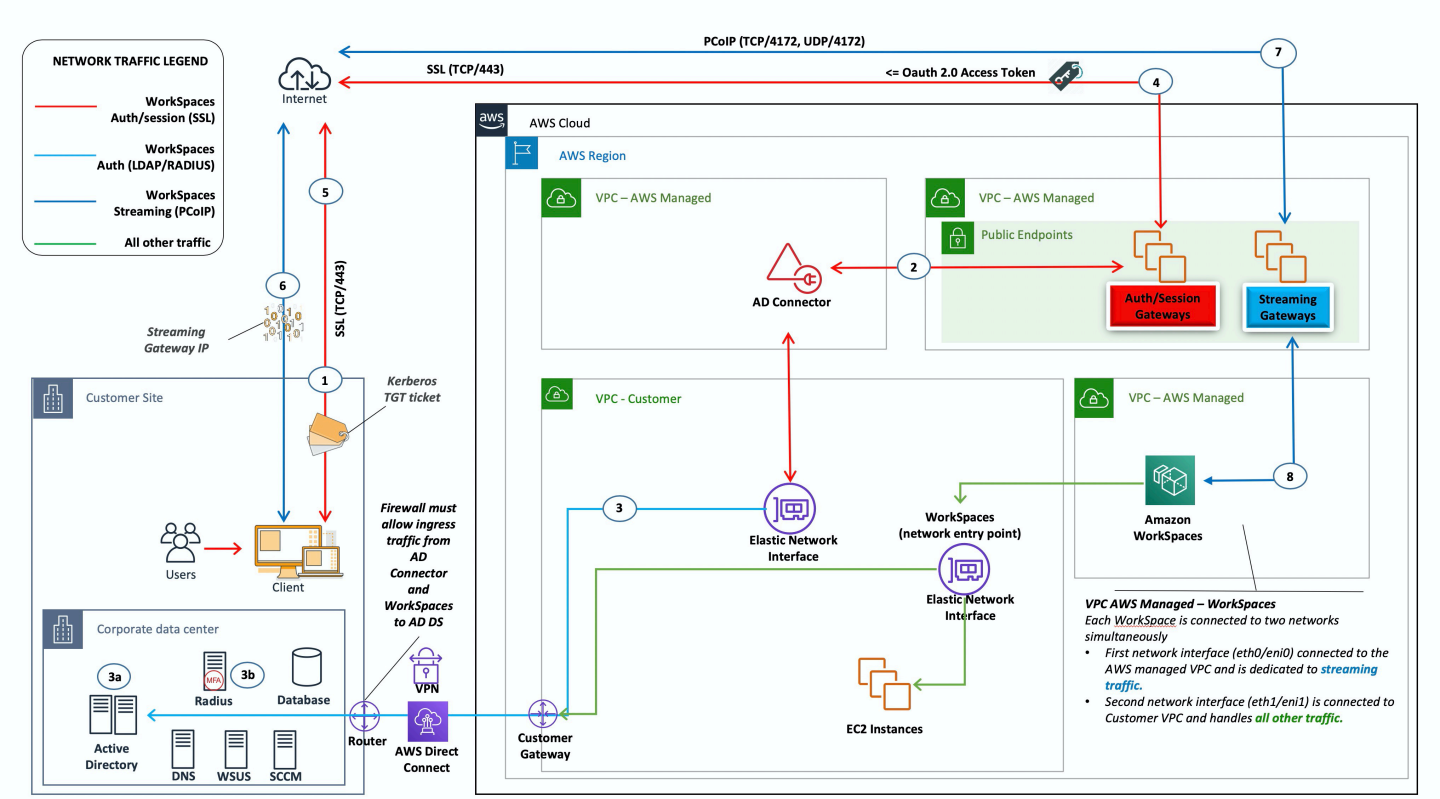

그림 5: 온-프레미스 액티브 디렉터리에 대한 AD 커넥터

이 시나리오에서는 AD Connector를 통해 고객 온-프레미스 AD DS로 프록시되는 모든 사용자 또는 MFA 인증에 AWS 디렉터리 서비스 (AD 커넥터) 가 사용됩니다 (다음 그림 참조). 인증 프로세스에 사용되는 프로토콜 또는 암호화에 대한 자세한 내용은 이 문서의 보안 섹션을 참조하십시오.

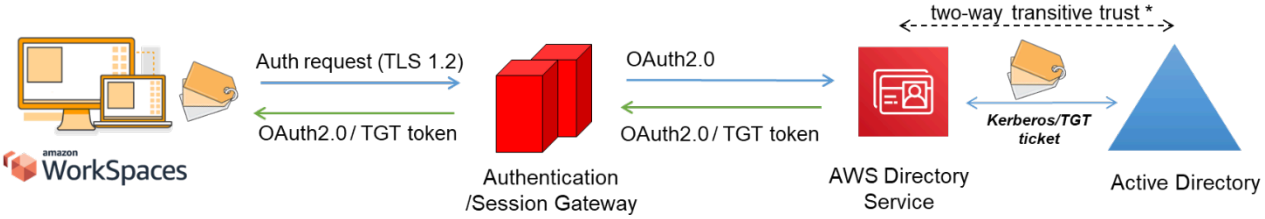

그림 6: 인증 게이트웨이를 통한 사용자 인증

시나리오 1은 고객이 이미 리소스를 보유하고 있을 수 있는 하이브리드 아키텍처와 WorkSpaces Amazon을 통해 액세스할 수 있는 온 프레미스 데이터 센터의 리소스를 보여줍니다. AWS 고객은 기존 온프레미스 AD DS 및 RADIUS 서버를 사용자 및 MFA 인증에 활용할 수 있습니다.

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 AZ에 걸쳐 최소 두 개의 프라이빗 서브넷이 있는 Amazon VPC를 생성합니다.
- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객이 지정한 도메인 이름 및 DNS (도메인 이름 서버) (온프레미스 서비스) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- Amazon 가상 사설 게이트웨이 — IPsec VPN 터널 또는 AWS Direct Connect 연결을 통해 자체 네트워크와 통신할 수 있습니다.
- AWS 디렉터리 서비스 — AD Connector는 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 네트워크 연결 — 기업 VPN 또는 Direct Connect 엔드포인트.
- AD DS — 기업 AD DS.
- MFA (선택 사항) — 기업 RADIUS 서버.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL (BYOL) 최종 사용자 디바이스 (예: Windows, Mac, iPad, Android 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저는 이 클라이언트 애플리케이션 목록을 참조하십시오.

이 솔루션은 AD DS를 클라우드에 배포하지 않으려는 고객에게 유용하지만 몇 가지 주의 사항이 있습니다.

- 연결 의존 — 데이터 센터에 대한 연결이 끊어지면 사용자는 해당 WorkSpaces 데이터 센터에 로그인할 수 없으며 기존 연결은 Kerberos/Ticket-Granting Ticket (TGT) 수명 기간 동안 활성 상태로 유지됩니다.

- 지연 시간 — 연결을 통해 대기 시간이 발생하는 경우 (Direct Connect보다 VPN의 경우 더 많음), WorkSpaces 인증 및 모든 ADDS 관련 활동 (예: 그룹 정책 (GPO) 적용에 더 많은 시간이 소요됩니다.
- 트래픽 비용 — 모든 인증은 VPN 또는 Direct Connect 링크를 통과해야 하므로 연결 유형에 따라 달라집니다. 이는 Amazon EC2에서 인터넷으로의 데이터 전송 또는 데이터 송신 (직접 연결) 입니다.

> **Note**
>
> AD 커넥터는 프록시 서비스입니다. 사용자 자격 증명을 저장하거나 캐시하지 않습니다. 대신 모든 인증, 조회 및 관리 요청은 AD에서 처리합니다. 디렉터리 서비스에는 모든 사용자 정보를 읽고 컴퓨터를 도메인에 가입시킬 수 있는 권한이 있는 위임 권한이 있는 계정이 필요합니다.

일반적으로 WorkSpaces 경험은 이전 그림에 표시된 Active Directory 인증 프로세스에 따라 크게 달라집니다. 이 시나리오에서 WorkSpaces 인증 환경은 고객 AD와 WorkSpaces VPC 간의 네트워크 링크에 크게 의존합니다. 고객은 링크의 가용성이 높은지 확인해야 합니다.

시나리오 2: 온-프레미스 AD DS를 AWS (복제본) 으로 확장

이 시나리오는 시나리오 1과 비슷합니다. 하지만 이 시나리오에서는 고객 AD DS의 복제본이 AD Connector와 함께 배포됩니다. AWS 이렇게 하면 Amazon Elastic Compute Cloud (Amazon EC2) 에서 실행되는 AD DS에 대한 인증 또는 쿼리 요청의 지연 시간이 줄어듭니다. 다음 그림은 각 구성 요소와 사용자 인증 흐름을 개괄적으로 보여줍니다.

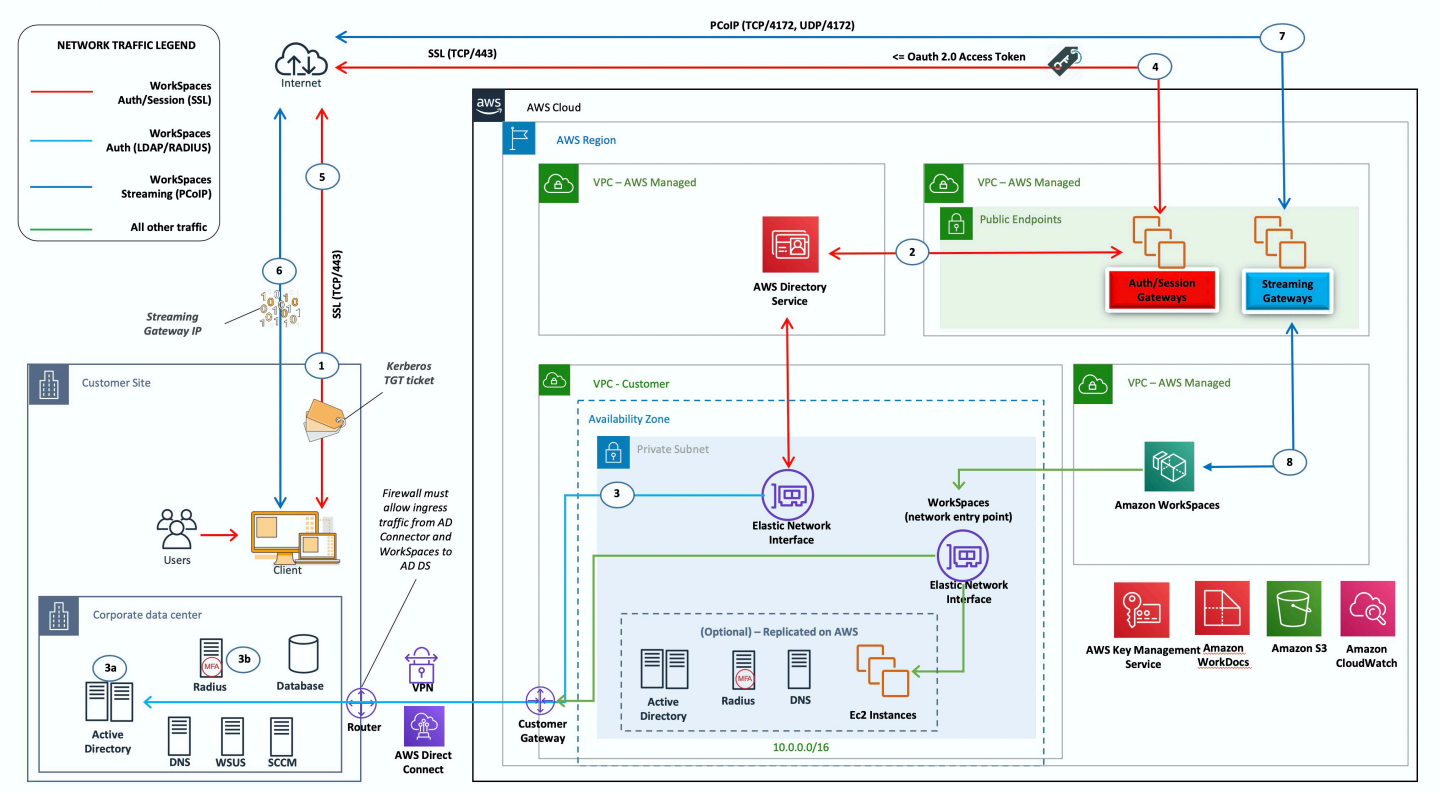

그림 7: 고객 Active Directory 도메인을 클라우드로 확장

시나리오 1에서와 같이 AD Connector는 모든 사용자 또는 MFA 인증에 사용되며, 이 인증은 고객 AD DS로 프록시됩니다 (이전 그림 참조). 이 시나리오에서 고객 AD DS는 클라우드에서 실행되는 고객의 온프레미스 AD 포리스트에 있는 도메인 컨트롤러로 승격되는 Amazon EC2 인스턴스의 AZ에 배포됩니다. AWS 각 도메인 컨트롤러는 VPC 프라이빗 서브넷에 배포되어 클라우드에서 AD DS의 가용성을 높일 수 있습니다. AWS AD DS를 배포하기 위한 모범 사례는 이 문서의 설계 고려 사항 섹션을 참조하십시오. AWS

WorkSpaces 인스턴스를 배포한 후에는 클라우드 기반 도메인 컨트롤러에 액세스하여 안전하고 지연 시간이 짧은 디렉터리 서비스와 DNS를 사용할 수 있습니다. AD DS 통신, 인증 요청, AD 복제를 비롯한 모든 네트워크 트래픽은 프라이빗 서브넷 내에서 또는 고객 VPN 터널 또는 Direct Connect를 통해 보호됩니다.

이 아키텍처는 다음과 같은 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 개의 AZ에 걸쳐 최소 네 개의 프라이빗 서브넷을 포함하는 Amazon VPC 생성 (고객 AD DS용 2개, AD Connector 또는 Amazon용 2개) WorkSpaces
- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객은 지정된 도메인 이름과 DNS (AD DS 로컬) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- Amazon 가상 사설 게이트웨이 — IPsec VPN 터널 또는 연결을 통해 고객 소유 네트워크와 통신할 수 있습니다. AWS Direct Connect
- Amazon EC2
  - 전용 프라이빗 VPC 서브넷의 Amazon EC2 인스턴스에 배포된 고객 기업 AD DS 도메인 컨트롤러
  - 전용 프라이빗 VPC 서브넷에 있는 Amazon EC2 인스턴스의 MFA용 고객 (선택 사항) RADIUS 서버.
- AWS 디렉터리 서비스 — AD Connector는 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 네트워크 연결 — 기업 VPN 또는 AWS Direct Connect 엔드포인트.

- AD DS - 기업 AD DS (복제에 필요).

- MFA (선택 사항) — 기업 RADIUS 서버.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL 최종 사용자 디바이스 (예: 윈도우, 맥, 아이패드, 안드로이드 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저에 대한 클라이언트 애플리케이션 목록을 참조하십시오. 이 솔루션에는 시나리오 1과 같은 주의 사항이 없습니다. WorkSpaces Amazon과 AWS Directory Service는 현재의 연결성에 의존하지 않습니다.
- 연결에 대한 의존 — 고객 데이터 센터와의 연결이 끊어져도 인증 및 선택적 MFA가 로컬에서 처리되므로 최종 사용자는 계속 작업할 수 있습니다.
- 지연 시간 — 복제 트래픽을 제외한 모든 인증은 로컬에서 수행되며 지연 시간이 짧습니다. 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.
- 트래픽 비용 - 이 시나리오에서는 인증이 로컬에서 이루어지므로 AD DS 복제만 VPN 또는 Direct Connect 링크를 통과하면 되므로 데이터 전송이 줄어듭니다.

일반적으로 이전 그림에서 볼 수 있듯이 WorkSpaces 환경은 향상되며 온-프레미스 도메인 컨트롤러에 대한 연결에 크게 의존하지 않습니다. 고객이 특히 AD DS 글로벌 카탈로그 쿼리와 관련하여 수천 대의 데스크톱으로 WorkSpaces 확장하려는 경우에도 마찬가지입니다. 이 트래픽은 환경에 국한되기 때문입니다. WorkSpaces

시나리오 3: 클라우드의 AWS Directory Service를 사용한 독립형 격리 배포 AWS

다음 그림에 표시된 이 시나리오에서는 AD DS가 독립형 격리된 AWS 환경의 클라우드에 배포되었습니다. AWS Directory Service는 이 시나리오에서만 사용됩니다. 고객은 AD DS를 완벽하게 관리하는 대신 AWS Directory Service를 사용하여 고가용성 디렉터리 토폴로지 구축, 도메인 컨트롤러 모니터링, 백업 및 스냅샷 구성과 같은 작업을 수행할 수 있습니다.

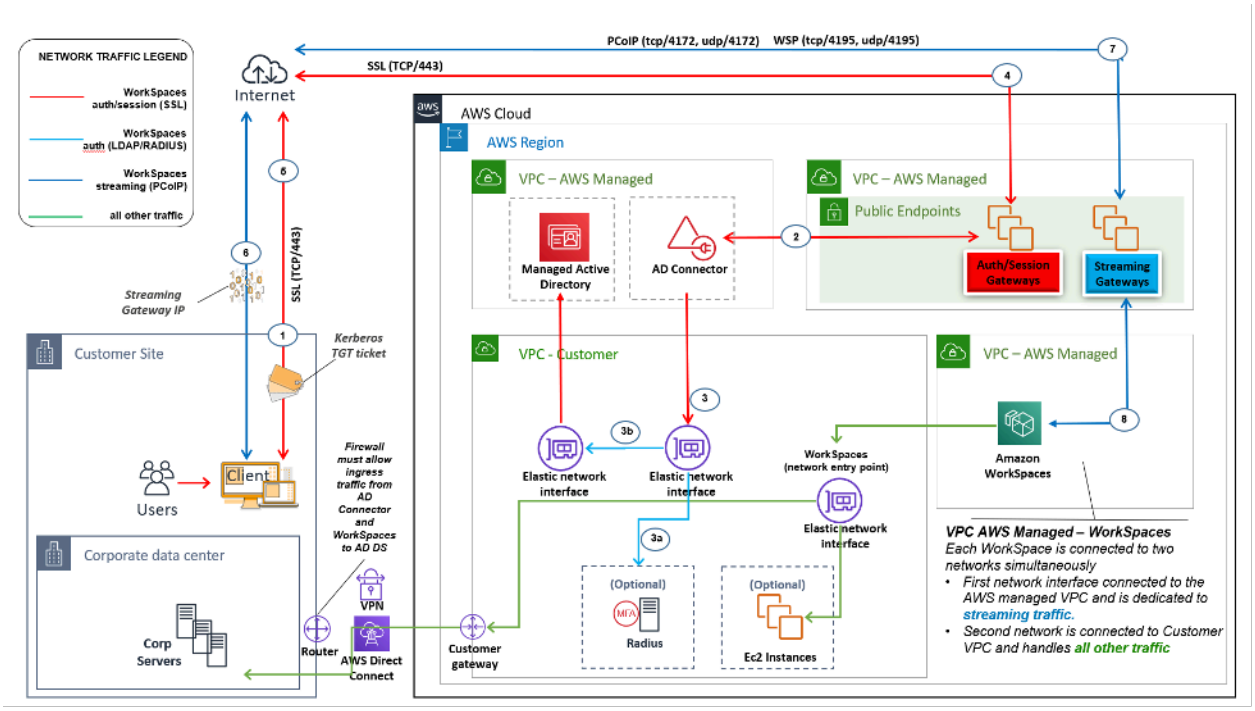

그림 8: 클라우드 전용: AWS 디렉터리 서비스 (Microsoft AD)

시나리오 2에서와 같이 AD DS (Microsoft AD) 는 두 AZ에 걸쳐 있는 전용 서브넷에 배포되므로 클라우드에서 AD DS의 가용성이 높아집니다. AWS Microsoft AD 외에도 AD Connector (세 가지 시나리오 모두) 가 WorkSpaces 인증 또는 MFA를 위해 배포됩니다. 이를 통해 Amazon VPC 내에서 역할 또는 기능을 분리할 수 있으며, 이는 표준 모범 사례입니다. 자세한 내용은 이 문서의 설계 고려 사항 섹션을 참조하십시오.

시나리오 3은 AWS Directory Service의 배포, 패치, 고가용성 및 모니터링을 AWS 관리하려는 고객에게 적합한 표준 통합 구성입니다. 이 시나리오는 격리 모드이기 때문에 개념 증명, 랩 및 프로덕션 환경에도 적합합니다.

AWS Directory Service의 배치 외에도 이 그림은 사용자로부터 작업 공간으로의 트래픽 흐름과 작업 영역이 AD 서버 및 MFA 서버와 상호 작용하는 방식을 보여줍니다.

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 개의 AZ에 걸쳐 최소 네 개의 프라이빗 서브넷을 포함하는 Amazon VPC 생성 (AD DS, Microsoft AD의 경우 2개, AD Connector용 2개, AD Connector 또는. WorkSpaces
- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객은 지정된 도메인 이름과 DNS (Microsoft AD) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.

- 선택 사항: Amazon 가상 프라이빗 게이트웨이 — IPsec VPN 터널 (VPN) 또는 연결을 통해 고객 소유 네트워크와 통신할 수 있습니다. AWS Direct Connect 온프레미스 백엔드 시스템에 액세스하는 데 사용합니다.
- AWS 디렉터리 서비스 — Microsoft AD는 VPC 서브넷의 전용 쌍에 배포되었습니다 (AD DS 관리 서비스).
- Amazon EC2 — MFA용 고객 "옵션" RADIUS 서버.
- AWS 디렉터리 서비스 — AD Connector는 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 선택 사항: 네트워크 연결 — 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL 최종 사용자 디바이스 (예: 윈도우, 맥, 아이패드, 안드로이드 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저는 이 클라이언트 애플리케이션 목록을 참조하십시오.

시나리오 2와 마찬가지로 이 시나리오는 고객 온프레미스 데이터 센터에 대한 연결, 지연 시간 또는 데이터 송신 전송 비용 (VPC WorkSpaces 내에서 인터넷 액세스가 지원되는 경우 제외) 에 대한 의존도와 관련된 문제가 없습니다. 이는 설계상 격리되거나 클라우드 전용 시나리오이기 때문입니다.

시나리오 4: AWS Microsoft AD 및 온-프레미스로의 양방향 전이적 신뢰

다음 그림에 표시된 이 시나리오는 고객 온-프레미스 AD에 대한 양방향 전이적 신뢰를 갖는 AWS 클라우드에 AWS 관리형 AD를 배포했습니다. 사용자는 관리형 AD에서 WorkSpaces 생성되며, AD 트러스트를 통해 온-프레미스 환경에서 리소스에 액세스할 수 있습니다.

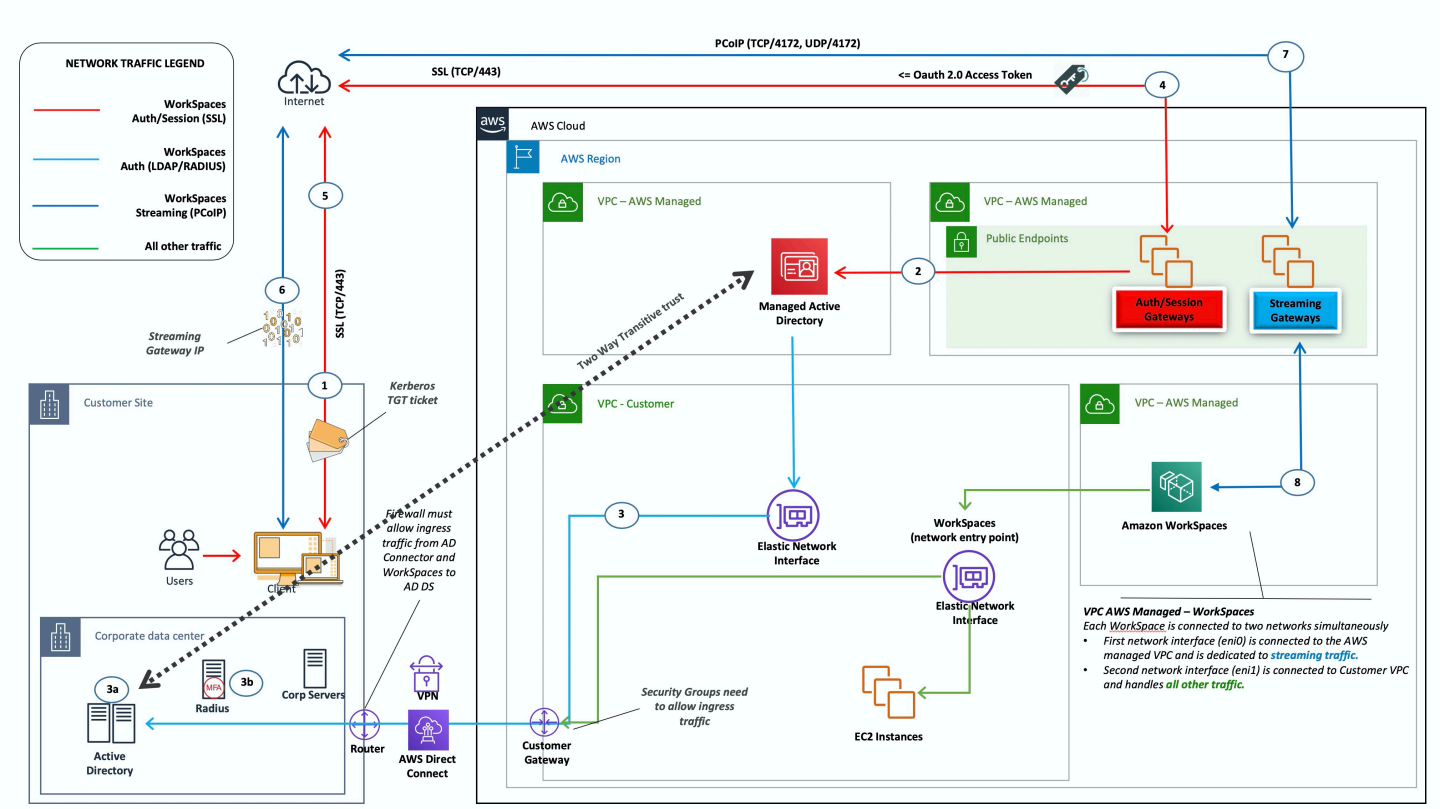

그림 9: AWS Microsoft AD와 온프레미스로의 양방향 전이적 신뢰

시나리오 3에서와 같이 AD DS (Microsoft AD) 는 두 AZ에 걸쳐 있는 전용 서브넷에 배포되므로 클라우드에서 AD DS의 가용성이 높아집니다. AWS

이 시나리오는 AWS 클라우드의 배포, 패치, 고가용성, 모니터링을 포함하여 완전히 관리되는 AWS Directory Service를 사용하려는 고객에게 적합합니다. 또한 이 시나리오를 통해 WorkSpaces 사용자는 기존 네트워크에서 AD에 가입된 리소스에 액세스할 수 있습니다. 이 시나리오를 수행하려면 도메인 트러스트가 있어야 합니다. 보안 그룹과 방화벽 규칙은 두 활성 디렉터리 간의 통신을 허용해야 합니다.

AWS Directory Service의 배치 외에도 이전 그림에서는 사용자로부터 작업 공간으로의 트래픽 흐름과 작업 공간이 AD 서버 및 MFA 서버와 상호 작용하는 방식을 설명합니다.

이 아키텍처는 다음과 같은 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 개의 AZ에 걸쳐 최소 네 개의 프라이빗 서브넷을 포함하는 Amazon VPC 생성 (AD DS, Microsoft AD의 경우 2개, AD Connector용 2개, AD Connector 또는. WorkSpaces

- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객은 지정된 도메인 이름과 DNS (Microsoft AD) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- 선택 사항: Amazon 가상 프라이빗 게이트웨이 — IPsec VPN 터널 (VPN) 또는 연결을 통해 고객 소유 네트워크와 통신할 수 있습니다. AWS Direct Connect 온프레미스 백엔드 시스템에 액세스하는 데 사용합니다.
- AWS 디렉터리 서비스 — Microsoft AD는 VPC 서브넷의 전용 쌍에 배포되었습니다 (AD DS 관리 서비스).

- Amazon EC2 — 고객이 선택할 수 있는 MFA용 RADIUS 서버.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 네트워크 연결 — 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL 최종 사용자 디바이스 (예: 윈도우, 맥, 아이패드, 안드로이드 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저에 대한 클라이언트 애플리케이션 목록을 참조하십시오.

이 솔루션을 사용하려면 고객 온-프레미스 데이터 센터에 연결해야 신뢰 프로세스가 작동할 수 있습니다. WorkSpaces사용자가 온프레미스 네트워크의 리소스를 사용하는 경우 지연 시간 및 아웃바운드 데이터 전송 비용을 고려해야 합니다.

시나리오 5: 공유 서비스 가상 사설 클라우드 (VPC) 를 사용하는 AWS Microsoft AD

다음 그림에 표시된 이 시나리오에서는 AWS 관리형 AD가 AWS 클라우드에 배포되어 이미 호스팅되어 AWS 있거나 더 광범위한 마이그레이션의 일환으로 제공될 예정인 워크로드에 대한 인증 서비스를 제공합니다. 모범 사례 권장 사항은 Amazon을 전용 VPC에 WorkSpaces 두는 것입니다. 또한 고객은 특정 AD OU를 만들어 WorkSpaces 컴퓨터 객체를 구성해야 합니다.

관리형 AD를 호스팅하는 공유 서비스 VPC를 사용하여 WorkSpaces 배포하려면 관리형 AD에서 만든 ADC 서비스 계정을 사용하여 AD 커넥터 (ADC) 를 배포하십시오. 서비스 계정에는 공유 서비스 관리형 AD의 WorkSpaces 지정된 OU에 컴퓨터 개체를 만들 수 있는 권한이 필요합니다.

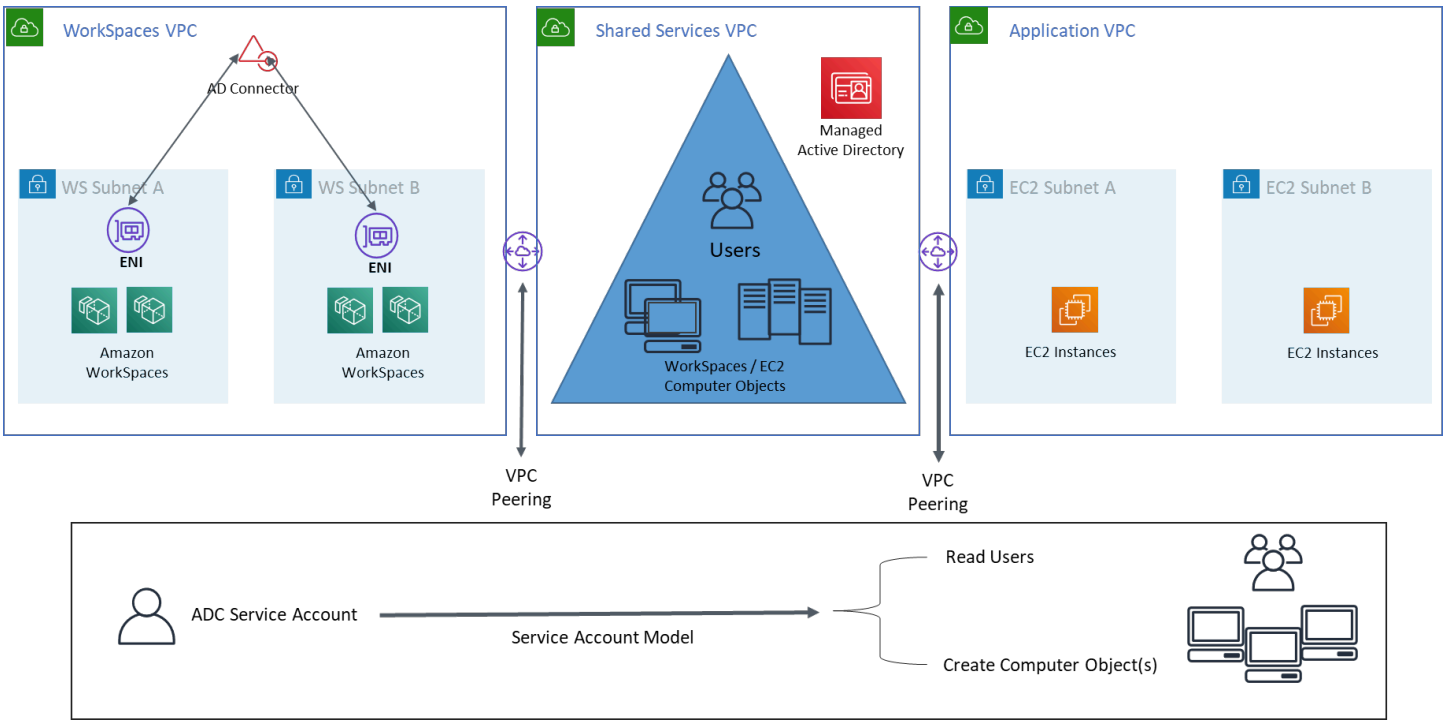

그림 10: 공유 서비스 VPC를 사용하는 AWS Microsoft AD

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 개의 AZ에 걸쳐 최소 두 개의 프라이빗 서브넷이 있는 Amazon VPC 생성 (AD Connector의 경우 2개, AD Connector의 경우 2개) WorkSpaces
- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객은 지정된 도메인 이름과 DNS (Microsoft AD) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- 선택 사항: Amazon 가상 프라이빗 게이트웨이 — IPsec VPN 터널 (VPN) 또는 연결을 통해 고객 소유 네트워크와 통신할 수 있습니다. AWS Direct Connect 온프레미스 백엔드 시스템에 액세스하는 데 사용합니다.
- AWS 디렉터리 서비스 — 전용 VPC 서브넷 쌍 (AD DS 관리 서비스), AD Connector에 배포된 Microsoft AD
- AWS 트랜짓 게이트웨이/VPC 피어링 — 워크스페이스 VPC와 공유 서비스 VPC 간 연결 지원
- Amazon EC2 — 고객이 선택할 수 있는 MFA용 RADIUS 서버.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 네트워크 연결 — 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL 최종 사용자 디바이스 (예: 윈도우, 맥, 아이패드, 안드로이드 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저에 대한 클라이언트 애플리케이션 목록을 참조하십시오.

시나리오 6: AWS Microsoft AD, 공유 서비스 VPC, 온프레미스로의 단방향 트러스트

다음 그림에 표시된 것처럼 이 시나리오에서는 사용자용 기존 온-프레미스 Active Directory를 사용하고 AWS 클라우드에 별도의 관리형 Active Directory를 도입하여 이와 관련된 컴퓨터 개체를 호스팅합니다. WorkSpaces 이 시나리오를 사용하면 컴퓨터 개체 및 Active Directory 그룹 정책을 회사 Active Directory와 독립적으로 관리할 수 있습니다.

이 시나리오는 타사에서 고객을 대신하여 Windows를 관리하려는 경우 유용합니다. 타사에서 고객 WorkSpaces AD에 대한 액세스 권한을 부여할 필요 없이 타사에서 고객과 관련된 정책 WorkSpaces 및 정책을 정의하고 제어할 수 있기 때문입니다. 이 시나리오에서는 공유 서비스 AD의 WorkSpaces 컴퓨터 개체를 구성하기 위해 특정 Active Directory OU (조직 구성 단위) 가 만들어집니다.

> **Note**
>
> Amazon Linux를 생성하려면 양방향 트러스트가 WorkSpaces 필요합니다.

고객 ID 도메인의 사용자를 사용하여 관리형 Active Directory를 호스팅하는 공유 서비스 VPC에서 만든 컴퓨터 개체와 WorkSpaces 함께 Windows를 배포하려면 회사 AD를 참조하는 Active Directory 커넥터 (ADC) 를 배포하십시오. Shared Services 관리 AD에서 Windows용으로 구성되고 회사 Active Directory (ID 도메인) 에 대한 읽기 권한이 있는 OU (조직 구성 단위) WorkSpaces 에서 컴퓨터 개체를 만들 수 있는 권한을 위임받은 회사 AD (ID 도메인) 에서 만든 ADC 서비스 계정을 사용하십시오.

도메인 로케이터 기능으로 자격 증명 도메인에 대해 원하는 AD 사이트의 WorkSpaces 사용자를 인증할 수 있도록 하려면 Microsoft 설명서에 따라 두 도메인의 Amazon WorkSpaces 서브넷용 AD 사이트 이름을 동일하게 지정하십시오. Amazon과 같은 AWS 지역에 자격 증명 도메인과 공유 서비스 도메인 AD 도메인 컨트롤러를 둘 다 두는 것이 가장 좋습니다 WorkSpaces.

이 시나리오를 구성하는 방법에 대한 자세한 지침은 AWS 디렉터리 서비스를 WorkSpaces 통한 Amazon에 대한 단방향 트러스트를 설정하는 구현 안내서를 검토하십시오.

이 시나리오에서는 공유 서비스 VPC와 온-프레미스 AD 간에 단방향 전이적 트러스트를 설정합니다. AWS Managed Microsoft AD 그림 11은 신뢰와 액세스의 방향과 AD Connector가 AWS AD Connector 서비스 계정을 사용하여 리소스 도메인에서 컴퓨터 개체를 만드는 방법을 보여줍니다.

Microsoft 권장 사항에 따라 포리스트 트러스트는 가능할 때마다 Kerberos 인증을 사용하도록 하는 데 사용됩니다. 의 리소스 도메인으로부터 GPO (그룹 정책 개체) 를 WorkSpaces 수신합니다. AWS Managed Microsoft AD 또한 ID 도메인을 WorkSpaces 사용하여 Kerberos 인증을 수행합니다. 이 기능이 안정적으로 작동하려면 ID 도메인을 위에서 설명한 AWS 대로 확장하는 것이 가장 좋습니다. 자세한 내용은 AWS Directory Service 구현 가이드가 포함된 단방향 신뢰 리소스 도메인을 WorkSpaces 사용하여 Amazon 배포를 검토하는 것이 좋습니다.

AD Connector와 사용자 WorkSpaces 모두 ID 도메인 및 리소스 도메인의 도메인 컨트롤러와 통신할 수 있어야 합니다. 자세한 내용은 Amazon WorkSpaces 관리 안내서의 IP 주소 및 포트 요구 사항을 참조하십시오. WorkSpaces

여러 AD 커넥터를 사용하는 경우 각 AD 커넥터가 고유한 AD 커넥터 서비스 계정을 사용하는 것이 가장 좋습니다.

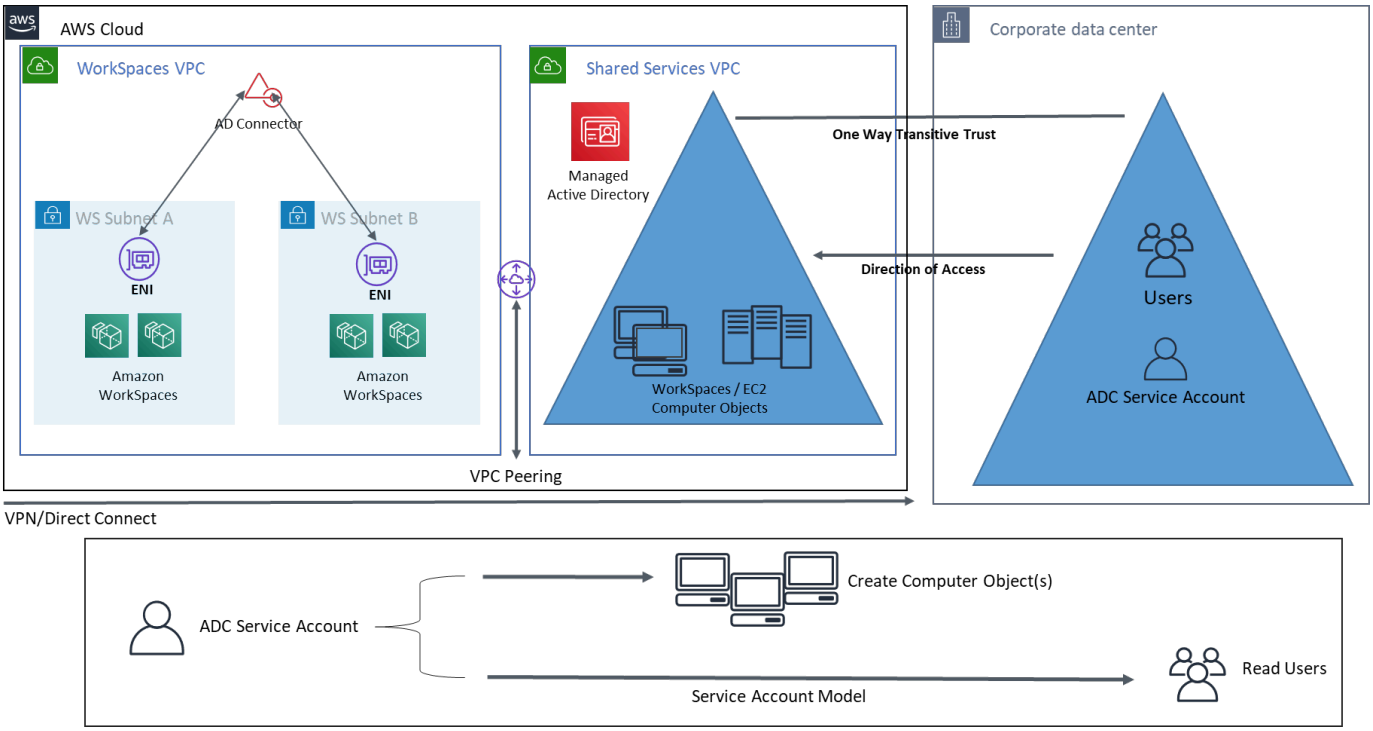

그림 11: AWS Microsoft, 공유 서비스 VPC, AD 온프레미스에 대한 단방향 트러스트

이 아키텍처는 다음과 같은 구성 요소 또는 구조를 사용합니다.

AWS

- Amazon VPC — 두 개의 AZ에 걸쳐 최소 두 개의 프라이빗 서브넷이 있는 Amazon VPC 생성 (AD Connector용 2개, AD Connector용 2개) WorkSpaces
- DHCP 옵션 세트 — Amazon VPC DHCP 옵션 세트 생성. 이를 통해 고객은 지정된 도메인 이름과 DNS (Microsoft AD) 를 정의할 수 있습니다. 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- 선택 사항: Amazon 가상 프라이빗 게이트웨이 — IPsec VPN 터널 (VPN) 또는 연결을 통해 고객 소유 네트워크와 통신할 수 있습니다. AWS Direct Connect 온프레미스 백엔드 시스템에 액세스하는 데 사용합니다.
- AWS 디렉터리 서비스 — Microsoft AD는 전용 VPC 서브넷 쌍 (AD DS 관리 서비스), AD Connector에 배포되었습니다.
- 트랜짓 게이트웨이/VPC 피어링 — 워크스페이스 VPC와 공유 서비스 VPC 간의 연결을 활성화합니다.
- Amazon EC2 — MFA용 고객 "옵션" RADIUS 서버.
- Amazon WorkSpaces — AD Connector와 동일한 프라이빗 서브넷에 WorkSpaces 배포됩니다. 자세한 내용은 이 문서의 Active Directory: 사이트 및 서비스 섹션을 참조하십시오.

고객

- 네트워크 연결 — 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- 최종 사용자 디바이스 — Amazon 서비스에 액세스하는 데 사용되는 기업용 또는 BYOL 최종 사용자 디바이스 (예: 윈도우, 맥, 아이패드, 안드로이드 태블릿, 제로 클라이언트, 크롬북). WorkSpaces 지원되는 장치 및 웹 브라우저는 이 클라이언트 애플리케이션 목록을 참조하십시오.

Amazon에서 다중 지역 AWS 관리형 액티브 디렉터리 사용 WorkSpaces

AWS 마이크로소프트 액티브 디렉터리용 디렉터리 서비스 (MAD) 는 WorkSpaces 아마존과 페어링할 수 있는 완전 관리형 마이크로소프트 액티브 디렉터리 (AD) 입니다. 고객이 AWS 관리형 Microsoft AD를 선택하는 이유는 고가용성, 모니터링 및 백업 기능이 내장되어 있기 때문입니다. AWS 관리형 Microsoft AD Enterprise 에디션에는 다중 지역 복제를 구성하는 기능이 추가되었습니다. 이 기능은 지역 간 네트워킹 연결을 자동으로 구성하고, 도메인 컨트롤러를 배포하고, 모든 Active Directory 데이터를 여러 지역에 복제하여 해당 지역에 있는 Windows 및 Linux 워크로드가 낮은 지연 시간과 높은 성능으로 MAD에 연결하여 사용할 AWS 수 있도록 합니다. 복제된 MAD 영역은 직접 등록할 수 없지만 복

제된 도메인 컨트롤러를 가리키도록 AD Connector (ADC) 를 WorkSpaces 구성하여 복제된 MAD 디렉터리를 등록할 수 있습니다. WorkSpaces

MAD를 사용하여 AD 커넥터를 배포할 때 가장 좋은 방법은 WorkSpaces 환경 내의 각 사업부에 대해 AD 커넥터를 만드는 것입니다. 이렇게 하면 각 사업부를 Active Directory 내의 특정 조직 구성 단위에 맞출 수 있습니다. 그런 다음 해당 사업부에 직접 맞는 조직 단위 수준에서 AD 그룹 정책 개체를 할당할 수 있습니다.

아키텍처

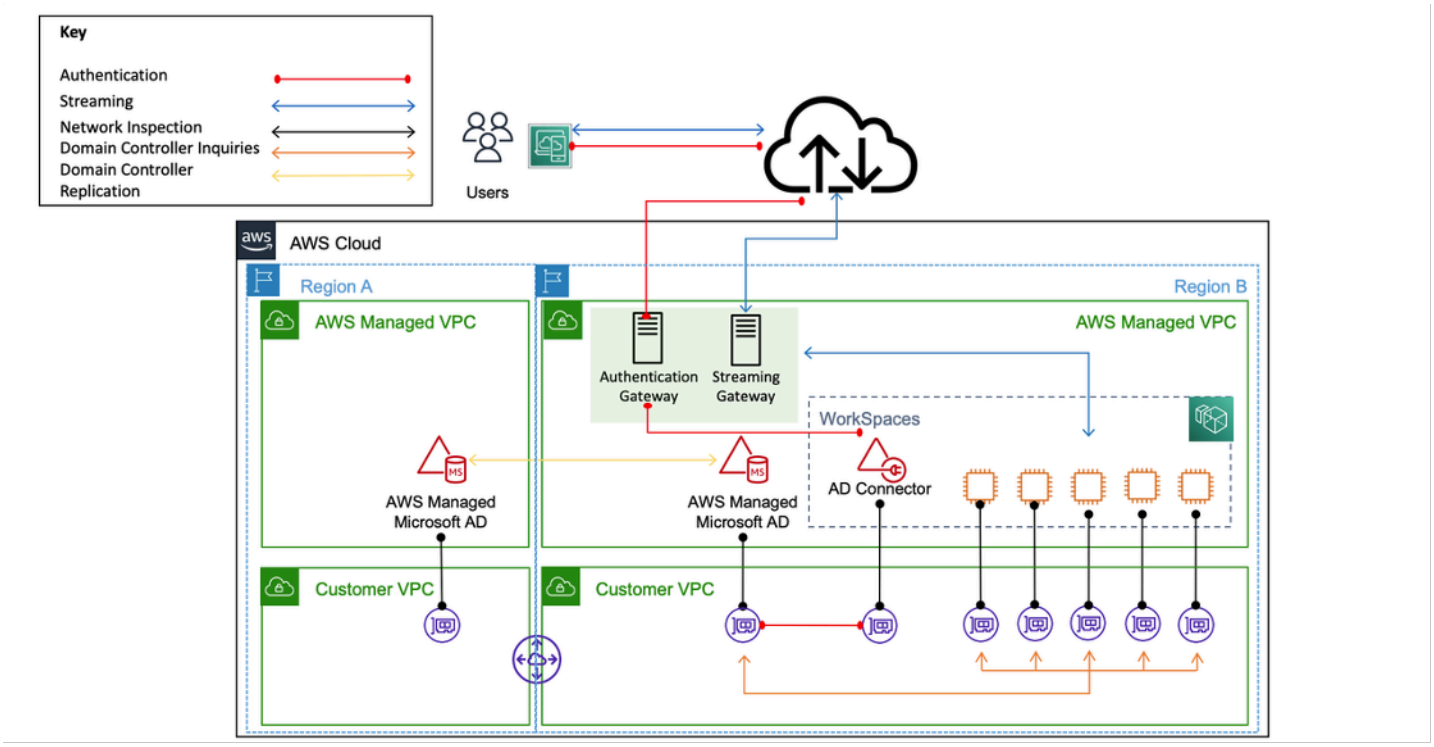

그림 12: 복제된 MAD 영역을 도메인에 등록하기 위한 샘플 아키텍처 WorkSpace

구현

복제된 MAD 영역을 등록하려면 MAD 도메인 컨트롤러 IP를 가리키는 AD 커넥터를 만들어야 합니다. WorkSpaces AWS Directory Service 콘솔 탐색 창으로 이동하여 디렉터리를 선택한 다음 올바른 디렉터리 ID를 선택하면 MAD 도메인 컨트롤러 IP 주소를 찾을 수 있습니다. 이러한 AD 커넥터를 만들려면 이 가이드를 따르십시오. 만든 후에는 등록할 수 있습니다 WorkSpaces. 새 WorkSpaces 지역에 배포하기 전에 VPC의 DHCP 옵션 세트를 업데이트했는지 확인하세요.

설계 고려 사항

AWS 클라우드에서 AD DS를 제대로 배포하려면 Active Directory 개념과 특정 서비스를 모두 잘 이해해야 합니다. AWS 이 섹션에서는 Amazon용 AD DS를 배포할 때의 주요 설계 고려 사항, AWS Directory Service에 대한 WorkSpaces VPC 모범 사례, DHCP 및 DNS 요구 사항, AD Connector 세부 사항, AD 사이트 및 서비스에 대해 설명합니다.

VPC 설계

이 문서의 네트워크 고려 사항 섹션에서 앞서 설명하고 시나리오 2와 3에 대해 앞서 설명했듯이 고객은 AWS 클라우드의 AD DS를 두 AZ에 걸쳐 AD Connector 또는 서브넷과 분리된 전용 프라이빗 서브넷 쌍에 배포해야 합니다. WorkSpaces 이 구조는 Amazon VPC 내에서 역할 또는 기능을 분리하는 표준 모범 사례를 유지하면서 AD DS 서비스에 대한 WorkSpaces 가용성이 높고 지연 시간이 짧은 액세스를 제공합니다.

다음 그림은 AD DS와 AD Connector를 전용 사설 서브넷으로 분리한 것을 보여줍니다 (시나리오 3). 이 예시에서는 모든 서비스가 동일한 Amazon VPC에 있습니다.

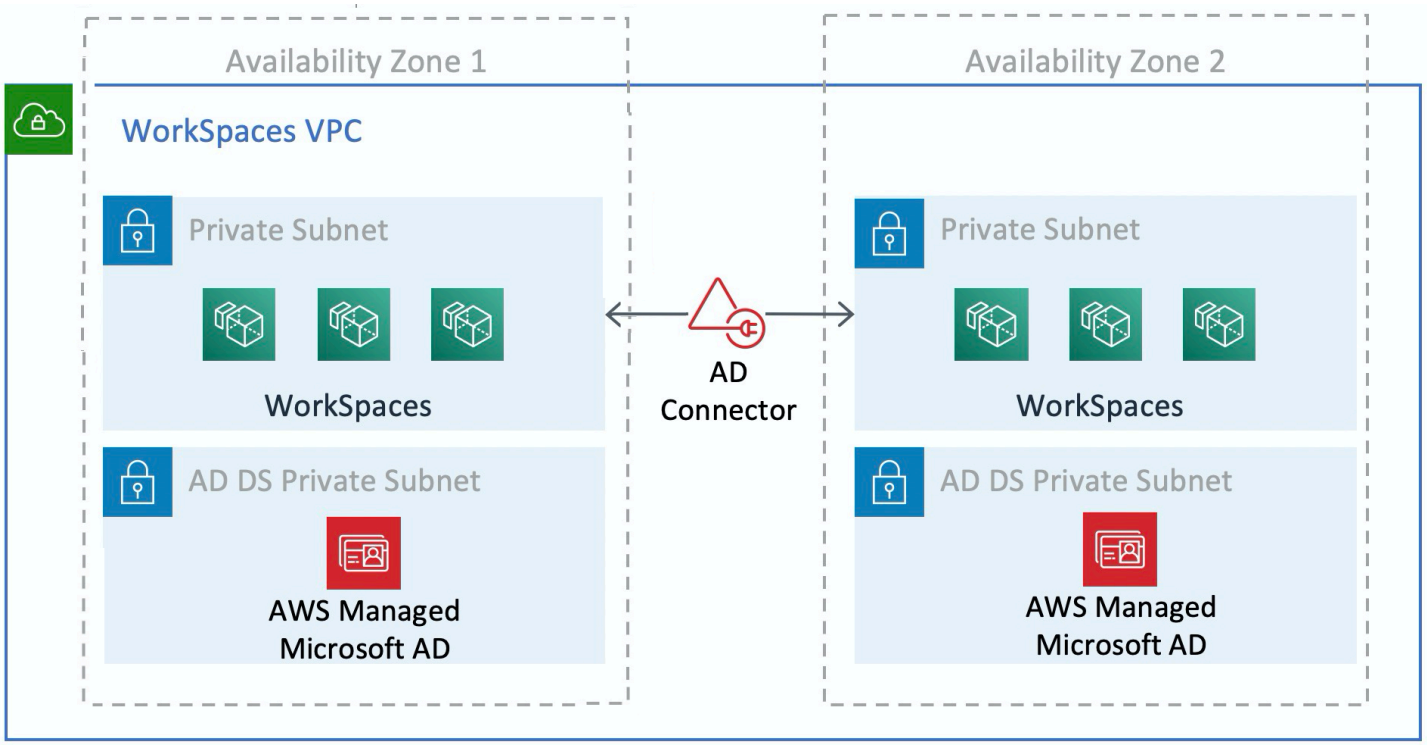

그림 13: AD DS 네트워크 분리

다음 그림은 시나리오 1과 비슷한 설계를 보여줍니다. 그러나 이 시나리오에서는 온프레미스 부분이 전용 Amazon VPC에 있습니다.

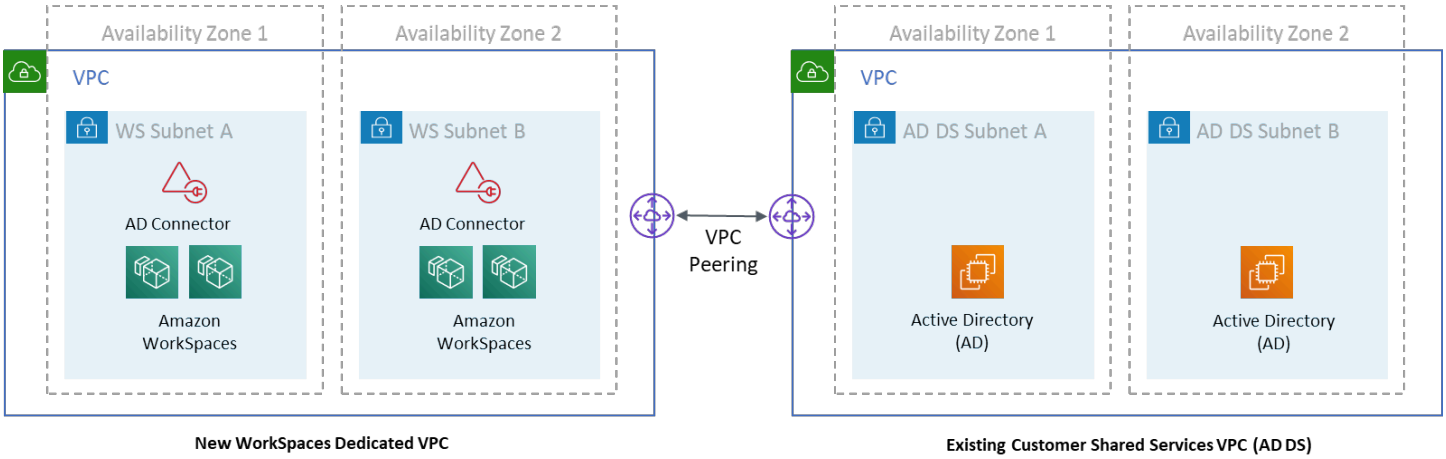

그림 14: 전용 WorkSpaces VPC

> **Note**
>
> AD DS를 사용하는 기존 AWS 배포가 있는 고객의 경우 전용 VPC에 배치하고 AD DS 통신을 위해 VPC 피어링을 사용하는 것이 좋습니다. WorkSpaces

AD DS용 전용 사설 서브넷을 만드는 것 외에도 도메인 컨트롤러와 구성원 서버에는 AD DS 복제, 사용자 인증, Windows Time 서비스 및 DFS (분산 파일 시스템) 와 같은 서비스에 대한 트래픽을 허용하는 몇 가지 보안 그룹 규칙이 필요합니다.

> **Note**
>
> 가장 좋은 방법은 필수 보안 그룹 규칙을 WorkSpaces 사설 서브넷으로 제한하고, 시나리오 2의 경우 다음 표와 같이 온-프레미스에서 AWS 클라우드와 주고받는 양방향 AD DS 통신을 허용하는 것입니다.

표 1 — 클라우드와 주고받는 양방향 AD DS 통신 AWS

프로토콜	Port	사용	대상
TCP	53, 88, 135, 139, 389, 445, 464, 636	인증 (기본)	액티브 디렉터리 (프라이빗 데이터 센터 또는 Amazon EC2) *
TCP	49152 — 65535	RPC 하이 포트	액티브 디렉터리 (프라이빗 데이터 센터 또는 Amazon EC2) **
TCP	3268-3269	트러스트	액티브 디렉터리 (프라이빗 데이터 센터 또는 Amazon EC2) *
TCP	9389	원격 마이크로소프트 윈도우 PowerShell (선택 사항)	액티브 디렉터리 (프라이빗 데이터 센터 또는 Amazon EC2) *
UDP	53, 88, 123, 137, 138, 389, 445, 464	인증 (기본)	액티브 디렉터리 (프라이빗 데이터 센터 또는 Amazon EC2) *
UDP	1812	인증 (MFA) (선택 사항)	RADIUS (프라이빗 데이터 센터 또는 아마존 EC2) *

자세한 내용은 Active Directory 및 Active Directory 도메인 서비스 포트 요구 사항 및 서비스 개요 및 Windows의 네트워크 포트 요구 사항을 참조하십시오.

규칙 구현에 대한 step-by-step 지침은 Amazon Elastic Compute 클라우드 사용 설명서의 보안 그룹에 규칙 추가를 참조하십시오.

VPC 설계: DHCP 및 DNS

Amazon VPC에서는 인스턴스에 동적 호스트 구성 프로토콜 (DHCP) 서비스가 기본적으로 제공됩니다. 기본적으로 모든 VPC는 CIDR (클래스 없는 도메인 간 라우팅) +2 주소 공간을 통해 액세스할 수 있는 내부 DNS (도메인 이름 시스템) 서버를 제공하며 기본 DHCP 옵션 세트를 통해 모든 인스턴스에 할당됩니다.

DHCP 옵션 세트는 Amazon VPC 내에서 범위 옵션 (예: DHCP를 통해 고객 인스턴스에 전달해야 하는 도메인 이름 또는 네임 서버) 을 정의하는 데 사용됩니다. 고객 VPC 내에서 Windows 서비스가 올바르게 기능하는지는 이 DHCP 범위 옵션에 따라 달라집니다. 앞서 정의한 각 시나리오에서 고객은 도메인 이름 및 이름 서버를 정의하는 자체 범위를 만들고 할당합니다. 이렇게 하면 도메인에 가입된 Windows 인스턴스 또는 AD WorkSpaces DNS를 사용하도록 구성됩니다.

다음 표는 Amazon WorkSpaces 및 AWS 디렉터리 서비스가 제대로 작동하기 위해 생성해야 하는 사용자 지정 DHCP 범위 옵션 세트의 예입니다.

표 2 — 사용자 지정 DHCP 범위 옵션 세트

파라미터	값
[Name tag]	key = name, 값을 특정 문자열로 설정하여 태그를 생성합니다. 예: example.com
도메인 이름	example.com
도메인 이름 서버	DNS 서버 주소, 쉼표로 구분됨 예: 192.0.2.10, 192.0.2.21
NTP 서버	이 필드는 비워 둡니다.
NetBIOS 이름 서버	도메인 이름 서버별로 동일한 IP를 쉼표로 구분하여 입력합니다. 예: 192.0.2.10, 192.0.2.21
NetBIOS 노드 유형	2

사용자 지정 DHCP 옵션 세트를 생성하고 이를 Amazon VPC와 연결하는 방법에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 DHCP 옵션 세트 사용을 참조하십시오.

시나리오 1에서 DHCP 범위는 온프레미스 DNS 또는 AD DS입니다. 하지만 시나리오 2 또는 3에서는 로컬로 배포된 디렉터리 서비스 (Amazon EC2의 AD DS 또는 AWS 디렉터리 서비스: Microsoft AD) 가 이에 해당합니다. AWS 클라우드에 상주하는 각 도메인 컨트롤러는 글로벌 카탈로그 및 디렉터리 통합 DNS 서버인 것이 좋습니다.

액티브 디렉터리: 사이트 및 서비스

시나리오 2의 경우 사이트 및 서비스는 AD DS의 올바른 기능을 위한 중요한 구성 요소입니다. 사이트 토폴로지는 동일한 사이트 내 도메인 컨트롤러 간 및 사이트 경계 전반의 AD 복제를 제어합니다. 시나리오 2에는 최소한 두 개의 사이트, 즉 온프레미스와 WorkSpaces 클라우드의 Amazon 사이트가 있습니다.

올바른 사이트 토폴로지를 정의하면 클라이언트 친화도가 보장되므로 클라이언트 (이 경우 WorkSpaces) 가 선호하는 로컬 도메인 컨트롤러를 사용합니다.

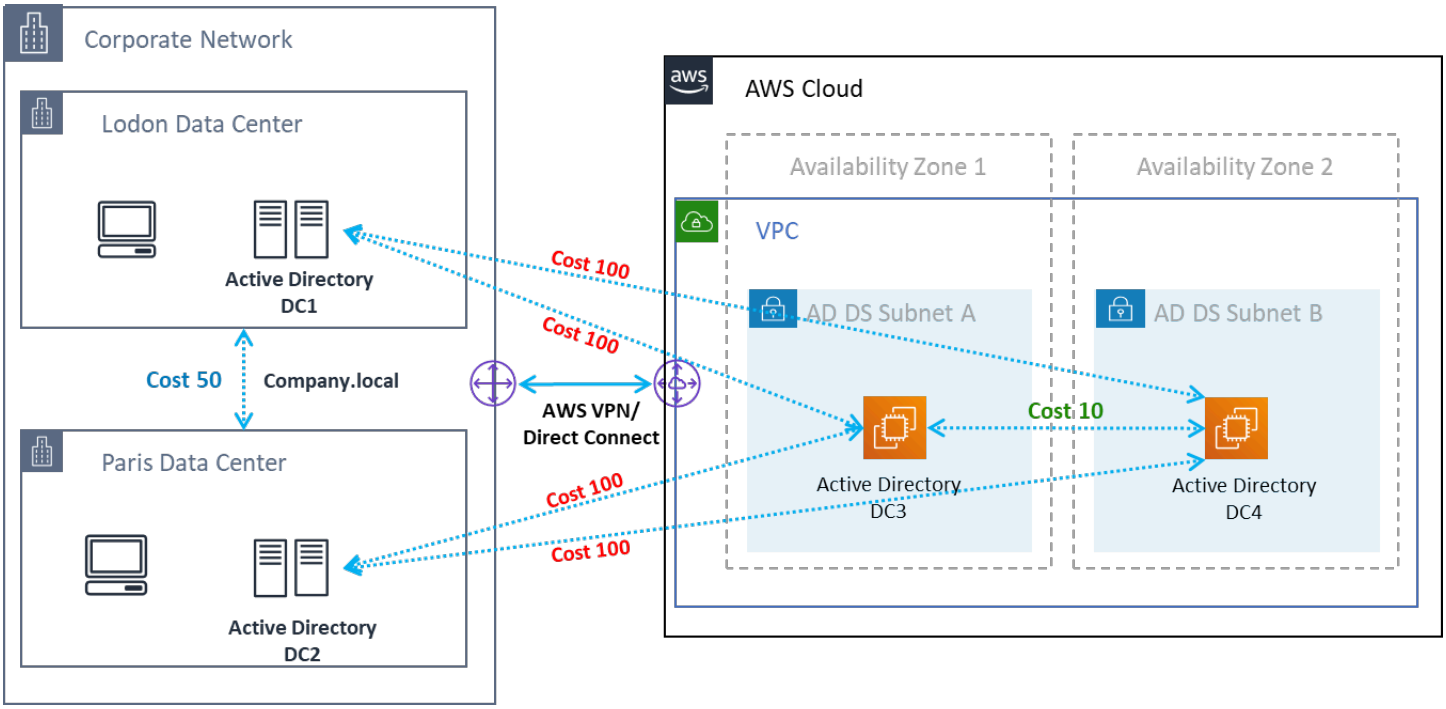

그림 15: 액티브 디렉터리 사이트 및 서비스: 클라이언트 선호도

모범 사례: 온-프레미스 AD DS와 클라우드 간의 사이트 링크에 대한 높은 비용을 정의하십시오 AWS . 다음 그림은 사이트 독립적 클라이언트 선호도를 보장하기 위해 사이트 링크에 할당하는 비용 (비용 100) 의 예입니다.

이러한 연결은 AD DS 복제 및 클라이언트 인증과 같은 트래픽이 도메인 컨트롤러에 대한 가장 효율적인 경로를 사용하도록 하는 데 도움이 됩니다. 시나리오 2와 3의 경우 이렇게 하면 지연 시간을 줄이고 교차 연결 트래픽을 보장하는 데 도움이 됩니다.

프로토콜

Amazon WorkSpaces Streaming Protocol (WSP) 은 전 세계 거리와 불안정한 네트워크에서 일관된 사용자 경험을 지원하는 클라우드 네이티브 스트리밍 프로토콜입니다. WSP는 메트릭 분석, 인코딩, 코덱 사용 및 선택을 WorkSpaces 오프로드하여 프로토콜과 프로토콜을 분리합니다. WSP는 포트 TCP/UDP 4195를 사용합니다. WSP 프로토콜 사용 여부를 결정할 때는 배포 전에 답변해야 하는 몇 가지 주요 질문이 있습니다. 아래 의사결정 매트릭스를 참조하십시오.

질문	WSP	PCoIP
식별된 WorkSpaces 사용자에게 양방향 오디오/비디오가 필요할까요?	•	
제로 클라이언트를 원격 엔드포인트 (로컬 장치) 로 사용할 예정입니까?		•
원격 엔드포인트로 Windows 또는 macOS를 사용할 예정입니까?	•	•
우분투 18.04를 원격 엔드포인트로 사용할 예정인가요?		•
사용자가 웹 액세스를 WorkSpaces 통해 Amazon에 액세스할 수 있습니까?		•
세션 전 또는 세션 중 스마트카드 지원 (PIC/CAC) 이 필요한가요?	•	
중국 (닝샤) 지역에서 WorkSpaces 사용할 예정인가요?		•

질문	WSP	PCoIP
스마트 카드 사전 인증 또는 세션 내 지원이 필요한가요?	•	
최종 사용자가 불안정하거나 지연 시간이 길거나 대역폭이 낮은 연결을 사용하고 있습니까?	•	

이전 질문은 사용해야 하는 프로토콜을 결정하는 데 매우 중요합니다. 권장 프로토콜 사용 사례에 대한 추가 정보는 여기에서 검토할 수 있습니다. 사용된 프로토콜은 나중에 Amazon WorkSpaces Migrate 기능을 사용하여 변경할 수도 있습니다. 이 기능의 사용에 대한 자세한 내용은 여기에서 검토할 수 있습니다.

WSP를 WorkSpaces 사용하여 배포할 때는 WSP 게이트웨이를 허용 목록에 추가하여 서비스 연결을 보장해야 합니다. 또한 WSP를 WorkSpaces 사용하여 WSP에 연결하는 사용자의 경우 최상의 성능을 위해서는 왕복 시간 (RTT) 이 250ms 미만이어야 합니다. RTT가 250밀리초에서 400ms 사이인 연결은 성능이 저하됩니다. 사용자의 연결이 지속적으로 저하되는 경우, 가능하면 최종 사용자와 가장 가까운 서비스 지원 WorkSpaces 지역에 Amazon을 배포하는 것이 좋습니다.

멀티 팩터 인증(MFA)

MFA를 WorkSpaces 구현하려면 Amazon을 디렉터리 서비스로 액티브 디렉터리 커넥터 (AD 커넥터) 또는 MAD (관리형 AWS Microsoft AD) 를 사용하여 구성하고 디렉터리 서비스를 통해 네트워크에 액세스할 수 있는 RADIUS 서버가 있어야 합니다. 심플 액티브 디렉터리는 MFA를 지원하지 않습니다.

AD에 대한 Active Directory 및 디렉터리 서비스 배포 고려 사항과 각 시나리오의 RADIUS 설계 옵션을 다루는 이전 섹션을 참조하십시오.

MFA — 2단계 인증

MFA가 활성화되면 사용자는 사용자 이름, 암호, MFA 코드를 WorkSpaces 클라이언트에 제공하여 해당 데스크톱에 대한 인증을 받아야 합니다. WorkSpaces

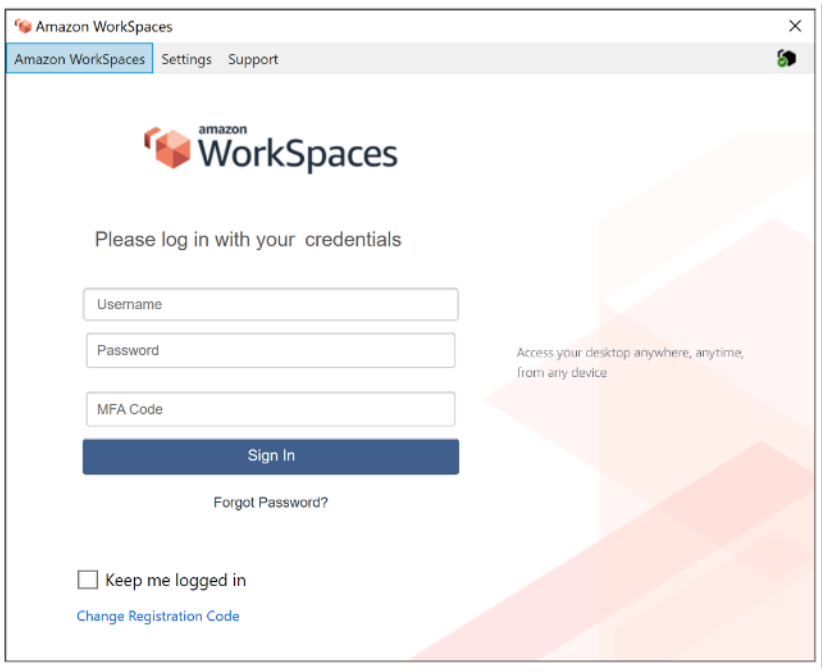

그림 16: WorkSpaces MFA가 활성화된 클라이언트

> **Note**
>
> AWS Directory Service는 사용자별 선택적 또는 상황별 MFA를 지원하지 않습니다. 이는 디렉터리별 글로벌 설정입니다. 선택적 "사용자별" MFA가 필요한 경우 동일한 소스 Active Directory를 가리킬 수 있는 AD 커넥터로 사용자를 구분해야 합니다.

WorkSpaces MFA에는 하나 이상의 RADIUS 서버가 필요합니다. 일반적으로 이러한 솔루션은 RSA 또는 Gemalto와 같이 이미 배포했을 수 있는 기존 솔루션입니다. 또는 EC2 인스턴스의 VPC 내에 RADIUS 서버를 배포할 수 있습니다 (아키텍처 옵션은 이 문서의 AD DS 배포 시나리오 섹션 참조). 새로운 RADIUS 솔루션을 배포하는 경우 듀오 시큐리티 또는 Okta MFA와 같은 SaaS 제품과 함께 FreeRadius와 같은 몇 가지 구현이 있습니다.

솔루션이 장애에 대한 복원력을 갖도록 하려면 여러 RADIUS 서버를 활용하는 것이 가장 좋습니다. MFA용 디렉터리 서비스를 구성할 때는 쉼표로 구분하여 여러 IP 주소를 입력할 수 있습니다 (예: 192.0.0.0,192.0.12). 디렉터리 서비스 MFA 기능은 지정된 첫 번째 IP 주소를 시도하고 첫 번째 IP 주소로 네트워크 접속을 설정할 수 없는 경우 두 번째 IP 주소로 이동합니다. 고가용성 아키텍처를 위한 RADIUS 구성은 각 솔루션 세트마다 다르지만 가장 중요한 권장 사항은 RADIUS 기능의 기본 인스턴스를 서로 다른 가용 영역에 배치하는 것입니다. 한 가지 구성 예가 Duo Security이며, Okta MFA의 경우 동일한 방식으로 여러 Okta RADIUS 서버 에이전트를 배포할 수 있습니다.

MFA용 AWS 디렉터리 서비스를 활성화하기 위한 자세한 단계는 AD 커넥터 및 관리형 AWS Microsoft AD를 참조하십시오.

재해 복구/비즈니스 연속성

WorkSpaces 지역 간 리디렉션

WorkSpaces Amazon은 고객에게 원격 데스크톱 액세스를 제공하는 지역 서비스입니다. 비즈니스 연속성 및 재해 복구 요구 사항 (BC/DR) 에 따라 일부 고객은 서비스를 이용할 수 있는 다른 지역으로의 원활한 장애 조치를 요구합니다 WorkSpaces . 이 BC/DR 요구 사항은 지역 간 리디렉션 옵션을 사용하여 충족할 수 있습니다. WorkSpaces 이를 통해 고객은 FQDN (정규화된 도메인 이름) 을 등록 코드로 사용할 수 있습니다. WorkSpaces

중요한 고려 사항은 페일오버 지역으로의 리디렉션이 발생할 시점을 결정하는 것입니다. 이 결정의 기준은 회사 정책을 기반으로 해야 하지만 RTO (복구 시간 목표) 및 RPO (복구 시점 목표) 를 포함해야 합니다. WorkSpaces Well-Architected 아키텍처 설계에는 서비스 장애 가능성이 포함되어야 합니다. 정상적인 비즈니스 운영 회복에 소요되는 시간 허용 범위도 결정에 영향을 미칩니다.

최종 사용자가 FQDN을 WorkSpaces 등록 WorkSpaces 코드로 사용하여 로그인하면 사용자가 연결될 등록 디렉터리를 결정하는 연결 식별자가 포함된 DNS TXT 레코드가 확인됩니다. 그러면 반환된 연결 식별자와 관련된 등록 디렉터리를 기반으로 WorkSpaces 클라이언트의 로그온 랜딩 페이지가 표시됩니다. 이를 통해 관리자는 FQDN에 대한 DNS 정책에 따라 최종 사용자를 다른 WorkSpaces 디렉터리로 안내할 수 있습니다. 클라이언트 시스템에서 프라이빗 영역을 확인할 수 있다고 가정하면 이 옵션은 퍼블릭 또는 프라이빗 DNS 영역과 함께 사용할 수 있습니다. 지역 간 리디렉션은 수동 또는 자동일 수 있습니다. 연결 식별자가 포함된 TXT 레코드를 원하는 디렉터리를 가리키도록 변경하면 이 두 페일오버를 모두 수행할 수 있습니다.

BC/DR 전략을 개발하는 동안 사용자 데이터를 고려하는 것이 중요합니다. WorkSpaces 지역 간 리디렉션 옵션은 사용자 데이터를 동기화하지 않고 이미지도 동기화하지 않기 때문입니다. WorkSpaces 서로 다른 지역에 WorkSpaces 배포하는 것은 독립된 독립체입니다. AWS 따라서 보조 지역으로의 리디렉션이 발생할 때 WorkSpaces 사용자가 데이터에 액세스할 수 있도록 추가 조치를 취해야 합니다. 지역 간 데이터 볼륨을 동기화하기 위한 Windows FSx (DFS Share) 또는 타사 유틸리티와 같이 WorkSpaces 사용자 데이터 복제에 사용할 수 있는 다양한 옵션이 있습니다. 마찬가지로, 지역 간에 이미지를 복사하는 등 보조 지역이 필요한 WorkSpaces 이미지에 액세스할 수 있는지 확인해야 합니다. 자세한 내용은 Amazon WorkSpaces WorkSpaces 관리 안내서의 Amazon용 지역 간 리디렉션과 다이어그램의 예를 참조하십시오.

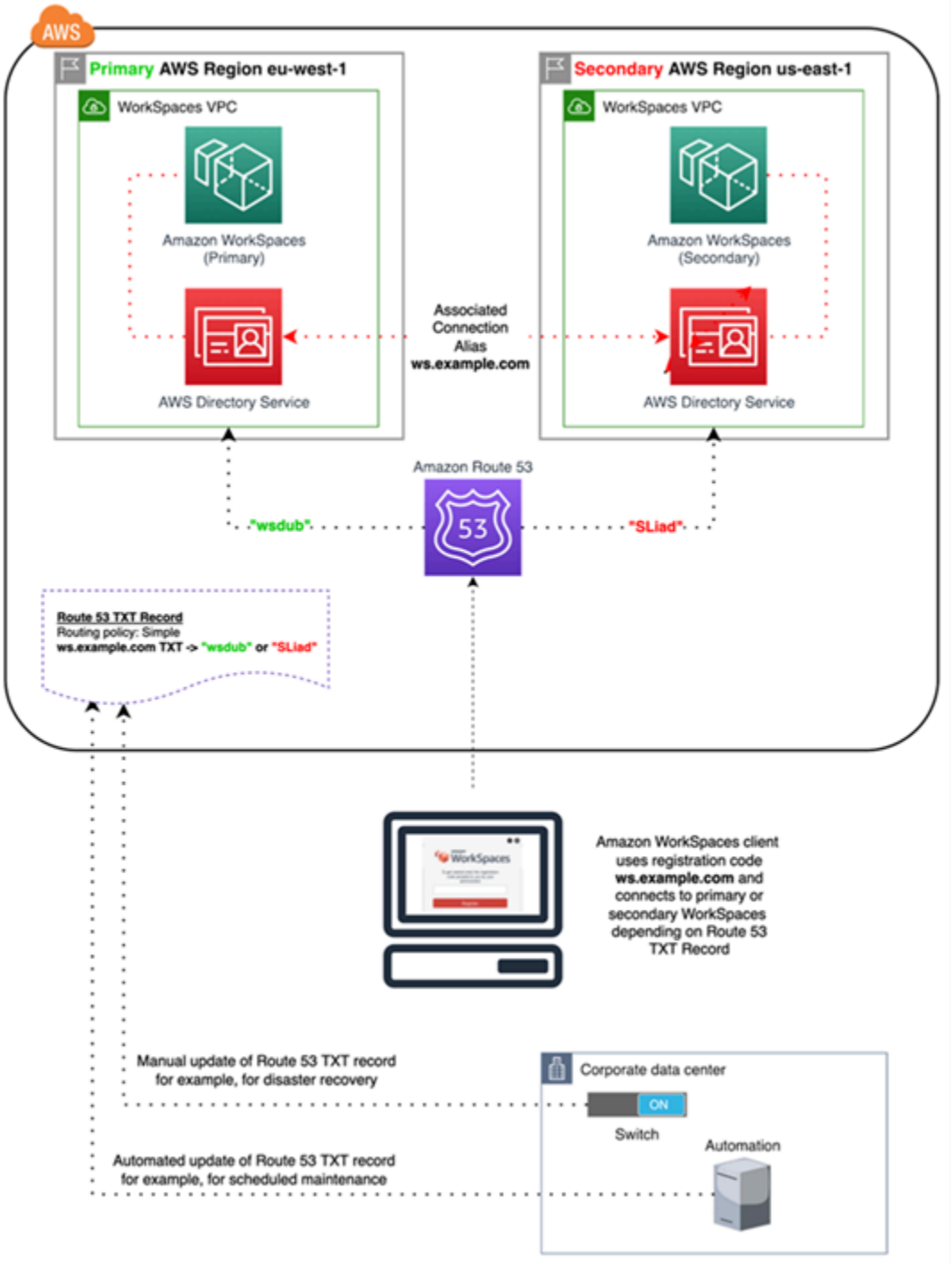

그림 17: Amazon Route 53을 사용한 WorkSpaces 지역 간 리디렉션 예제

WorkSpaces 인터페이스 VPC 엔드포인트 (AWS PrivateLink) — API 호출

Amazon WorkSpaces 퍼블릭 API는 에서 지원됩니다. AWS PrivateLink AWS PrivateLink 데이터가 퍼블릭 인터넷에 노출되는 것을 줄임으로써 클라우드 기반 애플리케이션과 공유되는 데이터의 보안을 강화합니다. WorkSpaces 인터페이스 엔드포인트를 사용하여 VPC 내에서 API 트래픽을 보호할 수 있습니다. 인터페이스 엔드포인트는 지원되는 서비스로 향하는 트래픽의 진입점 역할을 하는 서브넷의 IP 주소 범위에 속하는 프라이빗 IP 주소를 포함하는 Elastic Network Interface입니다. 이렇게 하면 사설 IP 주소를 사용하여 WorkSpaces API 서비스에 비공개로 액세스할 수 있습니다.

또한 WorkSpaces 퍼블릭 PrivateLink API와 함께 사용하면 VPC 내의 리소스에만 REST API를 안전하게 노출하거나 이를 통해 데이터 센터에 연결된 리소스에만 REST API를 노출할 수 있습니다. AWS Direct Connect

선택한 Amazon VPC와 VPC 엔드포인트에 대한 액세스를 제한하고 리소스별 정책을 사용하여 계정 간 액세스를 활성화할 수 있습니다.

엔드포인트 네트워크 인터페이스와 연결된 보안 그룹이 엔드포인트 네트워크 인터페이스와 서비스와 통신하는 VPC의 리소스 간의 통신을 허용하는지 확인하십시오. 보안 그룹이 VPC의 리소스에서 오는 인바운드 HTTPS 트래픽(포트 443)을 제한하는 경우, 엔드포인트 네트워크 인터페이스를 통해 트래픽을 전송할 수 없게 됩니다. 인터페이스 엔드포인트는 TCP 트래픽만을 지원합니다.

- 엔드포인트는 IPv4 트래픽만 지원합니다.
- 엔드포인트를 만들 경우, 연결하려는 서비스에 대한 액세스를 제어하는 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다.
- VPC당 생성할 수 있는 엔드포인트 수에는 할당량이 있습니다.
- 엔드포인트는 동일 리전에서만 지원됩니다. VPC와 다른 리전의 서비스 간에 엔드포인트를 만들 수 없습니다.

인터페이스 엔드포인트 이벤트에 대한 알림을 받을 알림 생성 — 인터페이스 엔드포인트에서 발생하는 특정 이벤트에 대한 알림을 받는 알림을 생성할 수 있습니다. 알림을 생성하려면 Amazon SNS 주제를 알림에 연결해야 합니다. SNS 주제를 구독하여 엔드포인트 이벤트가 발생할 때 이메일 알림을 받을 수 있습니다.

Amazon용 VPC 엔드포인트 정책 생성 WorkSpaces — Amazon용 Amazon WorkSpaces VPC 엔드포인트에 대한 정책을 생성하여 다음을 지정할 수 있습니다.

- 작업을 수행할 수 있는 보안 주체.

- 수행할 수 있는 작업.
- 작업을 수행할 있는 리소스.

VPC에 프라이빗 네트워크 연결 — VPC를 통해 Amazon WorkSpaces API를 호출하려면 VPC 내부의 인스턴스에서 연결하거나 Amazon VPN (가상 사설망) 을 사용하여 프라이빗 네트워크를 VPC에 연결해야 합니다. AWS Direct Connect Amazon VPN에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 VPN 연결을 참조하십시오. 에 대한 AWS Direct Connect 자세한 내용은 AWS Direct Connect 사용 설명서의 연결 생성을 참조하십시오.

VPC 인터페이스 엔드포인트를 통한 Amazon WorkSpaces API 사용에 대한 자세한 내용은 Amazon의 인프라 보안을 참조하십시오. WorkSpaces

스마트 카드 지원

스마트 카드 지원은 마이크로소프트 윈도우와 아마존 리눅스 모두에서 사용할 수 WorkSpaces 있습니다. 일반 액세스 카드 (CAC) 및 개인 신원 확인 (PIV) 을 통한 스마트 카드 지원은 WorkSpaces 스트리밍 프로토콜 (WSP) WorkSpaces 을 사용하는 Amazon에서만 제공됩니다. WSP의 스마트 카드 지원은 조직에서 승인한 연결 엔드포인트에서 스마트 카드 리더기 형태의 특정 하드웨어를 사용하는 사용자를 인증하기 위한 향상된 보안 상태를 WorkSpaces 제공합니다. 먼저 스마트 카드에 사용할 수 있는 지원 범위를 숙지하고 기존 및 향후 WorkSpaces 배포에서 스마트 카드가 어떻게 작동할지 결정하는 것이 중요합니다.

사전 세션 인증 또는 세션 내 인증 중 어떤 유형의 스마트 카드 지원이 필요한지 결정하는 것이 가장 좋습니다. 세션 전 인증은 이 글을 쓰는 시점에서 (미국 서부), 미국 동부 AWS GovCloud (버지니아 북부), 미국 서부 (오레곤), 유럽 (아일랜드), 아시아 태평양 (도쿄) 및 아시아 태평양 (시드니) 에서만 사용할 수 있습니다. 세션 내 스마트 카드 인증은 일반적으로 다음과 같은 몇 가지 고려 사항을 고려하여 사용할 수 있습니다.

- 조직에 Windows Active Directory와 통합된 스마트 카드 인프라가 있습니까?
- OCSP (온라인 인증서 상태 프로토콜) Responder는 공용 인터넷에서 액세스할 수 있습니까?
- 사용자 인증서가 SAN (주체 대체 이름) 필드에 UPN (사용자 계정 이름) 과 함께 발급되었습니까?
- 자세한 고려 사항은 세션 중 및 세션 전 섹션에 자세히 설명되어 있습니다.

스마트 카드 지원은 그룹 정책을 통해 활성화됩니다. WSP용 아마존 WorkSpaces 그룹 정책 관리 템플릿을 Amazon Directory에서 사용하는 Active Directory 도메인의 센트럴 스토어에 추가하는 것이 가장 좋습니다. WorkSpaces 컴퓨터 기반 정책이므로 이 정책을 기존 Amazon WorkSpaces 배포에 적용할

경우 모든 사용자에게 변경 사항이 적용되려면 그룹 정책 업데이트와 재부팅이 WorkSpaces 필요합니다.

루트 CA

Amazon WorkSpaces 클라이언트 및 사용자의 이동성 특성상 사용자가 Amazon에 연결하는 데 사용하는 각 디바이스의 신뢰할 수 있는 루트 인증서 저장소에 타사 루트 CA 인증서를 원격으로 전송해야 합니다. WorkSpaces 스마트 카드가 있는 AD 도메인 컨트롤러와 사용자 장치는 루트 CA를 신뢰해야 합니다. 정확한 요구 사항에 대한 자세한 내용은 Microsoft에서 제공하는 타사 CA 활성화 지침을 검토하세요.

AD 도메인에 가입된 환경에서 이러한 장치는 루트 CA 인증서를 배포하는 그룹 정책을 통해 이 요구 사항을 충족합니다. Amazon WorkSpaces Client를 non-domain-joined 디바이스에서 사용하는 시나리오에서는 타사 루트 CA에 대한 대체 전송 방법 (예: Intune) 을 결정해야 합니다.

세션 중

세션 내 인증은 Amazon WorkSpaces 사용자 세션이 이미 시작된 후 애플리케이션 인증을 간소화하고 보호합니다. 앞서 언급했듯이 Amazon의 기본 동작은 스마트 카드를 WorkSpaces 비활성화하므로 그룹 정책을 통해 활성화해야 합니다. Amazon WorkSpaces 관리 관점에서 볼 때 구성은 인증을 통과하는 애플리케이션 (예: 웹 브라우저) 에 특히 필요합니다. AD 커넥터 및 디렉터리는 변경할 필요가 없습니다.

세션 내 인증 지원이 필요한 대부분의 일반적인 응용 프로그램은 Mozilla Firefox 및 Google Chrome과 같은 웹 브라우저를 사용하는 것입니다. Mozilla Firefox는 세션 내 스마트 카드 지원을 위해 제한된 구성을 필요로 합니다. Amazon Linux WorkSpaces WSP에서는 모질라 파이어폭스와 구글 크롬 모두에 대한 세션 내 스마트 카드 지원을 위해 추가 구성이 필요합니다.

Amazon WorkSpaces Client에 로컬 컴퓨터에 대한 권한이 없을 수 있으므로 문제를 해결하기 전에 루트 CA를 사용자의 개인 인증서 저장소에 로드하는 것이 좋습니다. 또한 스마트 카드에서 의심되는 세션 내 인증 문제를 해결할 때 OpenSC를 사용하여 스마트 카드 장치를 식별하십시오. 마지막으로, 인증서 취소 검사를 통해 응용 프로그램 인증의 보안 상태를 개선하려면 OCSP (온라인 인증서 상태 프로토콜) 응답자를 사용하는 것이 좋습니다.

사전 세션

세션 전 인증을 지원하려면 Windows WorkSpaces 클라이언트 버전 3.1.1 이상 또는 macOS WorkSpaces 클라이언트 버전 3.1.5 이상이 필요합니다. 스마트 카드를 사용한 사전 세션 인증은 표준

인증과 근본적으로 다릅니다. 즉, 사용자가 스마트 카드 삽입과 PIN 코드 입력을 모두 조합하여 인증해야 합니다. 이 인증 유형의 경우 사용자 세션 기간은 Kerberos 티켓의 수명에 따라 제한됩니다. 전체 설치 안내서는 여기에서 확인할 수 있습니다.

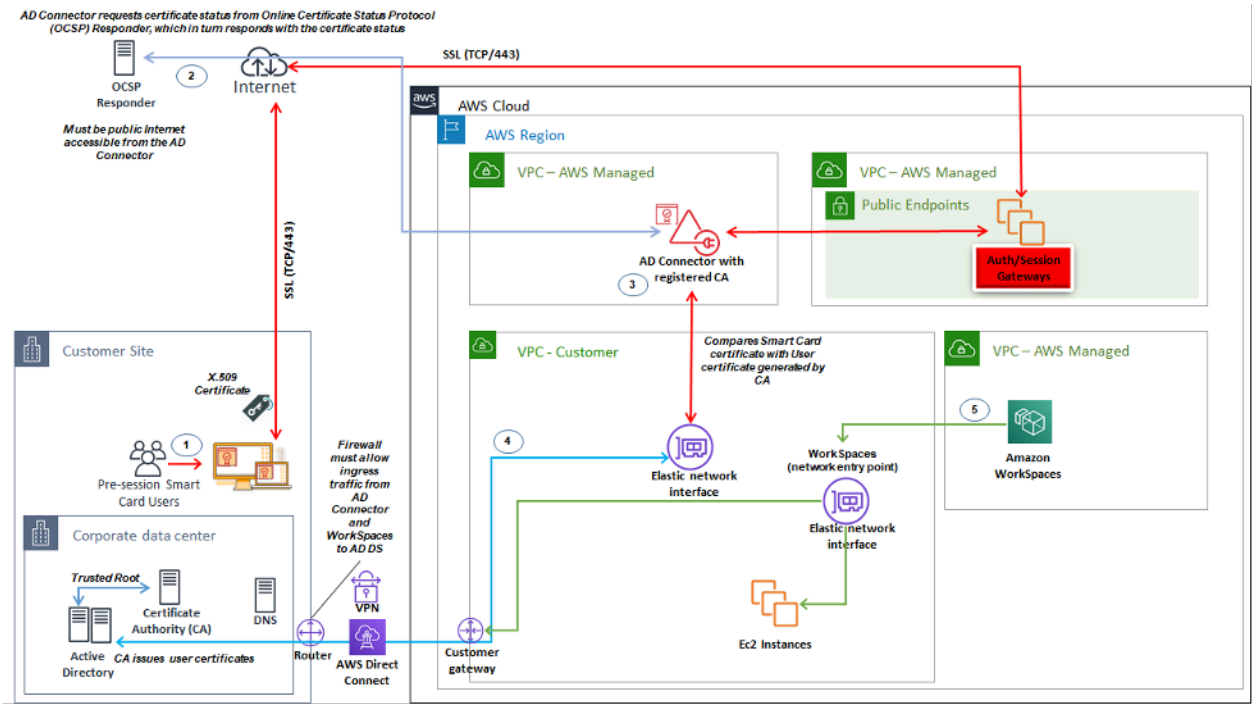

그림 18: 세션 전 인증 개요

1. 사용자가 Amazon WorkSpaces Client를 열고 스마트 카드를 삽입한 다음 PIN을 입력합니다. Amazon WorkSpaces Client는 PIN을 사용하여 X.509 인증서를 해독합니다. 이 인증서는 인증 게이트웨이를 통해 AD Connector로 프록시됩니다.
2. AD Connector는 디렉터리 설정에 지정된 공개적으로 액세스할 수 있는 OCSP 응답자 URL에 대해 X.509 인증서를 검증하여 인증서가 해지되지 않았는지 확인합니다.
3. 인증서가 유효하면 Amazon WorkSpaces Client는 사용자에게 PIN을 다시 입력하라는 메시지를 보내 인증 프로세스를 계속 진행합니다. 그러면 X.509 인증서와 프록시를 AD Connector로 복호화한 다음 AD Connector의 루트 및 중간 인증서와 매칭하여 검증합니다.
4. 인증서 유효성 검사가 성공적으로 완료되면 AD Connector에서 Active Directory를 사용하여 사용자를 인증하고 Kerberos 티켓을 만듭니다.
5. Kerberos 티켓은 사용자의 WorkSpace Amazon으로 전달되어 인증을 받고 WSP 세션을 시작합니다.

고객 관리형 네트워크가 아닌 AWS 관리형 네트워크를 통해 연결이 수행되므로 OCSP Responder는 공개적으로 액세스할 수 있어야 합니다. 따라서 이 단계에서는 사설 네트워크로 라우팅할 수 없습니다.

AD Connector에 제공된 사용자 인증서에는 인증서의 (SAN) 필드에 사용자의 userPrincipalName (UPN) 이 subjectAltName 포함되므로 사용자 이름을 입력할 필요는 없습니다. 스마트 카드를 사용한 세션 전 인증이 필요한 모든 사용자가 Microsoft Management Console에서 개별적으로 수행하는 대신 를 사용하여 PowerShell 인증서의 예상 UPN으로 인증하도록 AD 사용자 개체를 업데이트하도록 자동화하는 것이 가장 좋습니다.

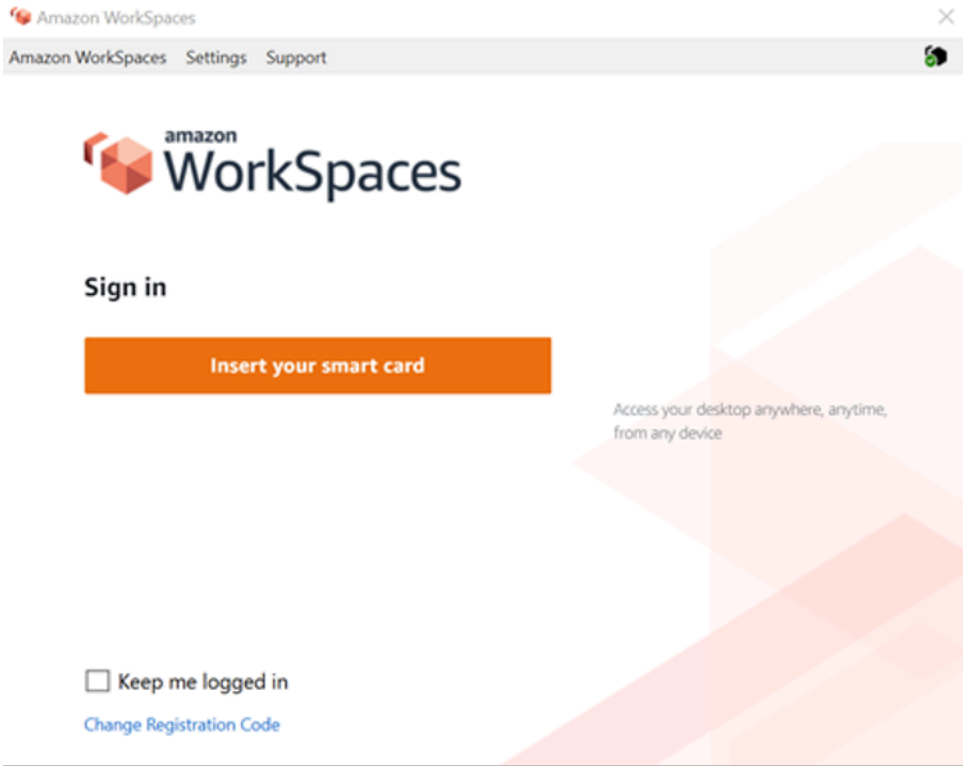

그림 19: WorkSpaces 로그인 콘솔

클라이언트 배포

Amazon WorkSpaces Client (버전 3.X+) 는 관리자가 사용자의 클라이언트를 사전 구성하는 데 활용할 수 있는 표준화된 구성 파일을 사용합니다. WorkSpaces 두 가지 기본 구성 파일의 경로는 다음에서 찾을 수 있습니다.

OS	구성 파일 경로
Windows	C:\Users\USERNAME\AppData\ 로컬\ 아마존 웹 서비스\ 아마존 WorkSpaces
macOS	/사용자/사용자 이름/라이브러리/애플리케이션 지원/아마존 웹 서비스/아마존 WorkSpaces

OS	구성 파일 경로
리눅스 (우분투 18.04)	/홈/우분투/.local/공유/아마존 웹 서비스/아마존/WorkSpaces

이 경로에서 두 구성 파일을 찾을 수 있습니다. 첫 번째 구성 UserSettings 파일은.json으로, 현재 등록, 프록시 구성, 로깅 수준, 등록 목록 저장 기능 등을 설정합니다. 두 번째 구성 파일은.json입니다. RegistrationList 이 파일에는 클라이언트가 올바른 WorkSpaces WorkSpaces 디렉터리에 매핑하는 데 사용할 수 있는 모든 디렉터리 정보가 포함됩니다. RegistrationList.json을 미리 구성하면 클라이언트에 있는 모든 사용자 등록 코드가 채워집니다.

> **Note**
>
> 사용자가 WorkSpaces 클라이언트 버전 2.5.11을 실행하는 경우 proxy.cfg 는 클라이언트 프록시 설정에 사용되고 client_settings.ini 버전은 로그 수준과 등록 목록 저장 기능을 설정합니다. 기본 프록시 설정은 OS 내에서 설정된 설정을 사용합니다.

이러한 파일은 표준화되어 있으므로 관리자는 WorkSpaces 클라이언트를 다운로드하고 적용 가능한 모든 설정을 지정한 다음 모든 최종 사용자에게 동일한 구성 파일을 제공할 수 있습니다. 설정을 적용하려면 새 구성을 설정한 후 클라이언트를 시작해야 합니다. 클라이언트가 실행되는 동안 구성을 변경하면 클라이언트 내에 변경 내용이 설정되지 않습니다.

WorkSpaces 사용자에 대해 설정할 수 있는 마지막 설정은 Windows 클라이언트 자동 업데이트입니다. 이는 구성 파일을 통해 제어되지 않고 대신 Windows 레지스트리를 통해 제어됩니다. 새 버전의 클라이언트가 출시되면 레지스트리 키를 생성하여 해당 버전을 건너뛸 수 있습니다. 이는 컴퓨터\ HKEY_CURRENT_USER\ Software\ Amazon Web Services 경로에 전체 버전 번호 값을 포함하는 문자열 레지스트리 항목 이름을 SkipThisVersion 생성하여 설정할 수 있습니다. LLC\ Amazon WorkSpaces\ WinSparkle 이 옵션은 macOS에서도 사용할 수 있습니다. 그러나 구성은 편집하려면 특수 소프트웨어가 필요한 plist 파일 내에 있습니다. 이 작업을 계속 수행하려는 경우에는 com.amazon.workspaces 도메인 내에 /users/사용자 이름/라이브러리/Preferences 위치에 있는 SU SkippedVersion 항목을 추가하면 됩니다.

Amazon WorkSpaces 엔드포인트 선택

적합한 엔드포인트 선택 WorkSpaces

WorkSpaces Amazon은 Windows 데스크톱부터 아이패드, 크롬북까지 다양한 엔드포인트 디바이스를 지원합니다. Amazon Workspaces 웹 사이트에서 사용 가능한 Amazon WorkSpaces 클라이언트를 다운로드할 수 있습니다. 사용자에게 적합한 엔드포인트를 선택하는 것은 중요한 결정입니다. 사용자가 양방향 오디오/비디오를 사용해야 하고 WorkSpaces 스트리밍 프로토콜을 사용하려는 경우 Windows 또는 macOS 클라이언트를 사용해야 합니다. 모든 클라이언트의 경우 WorkSpacesAmazon의 IP 주소 및 포트 요구 사항에 나열된 IP 주소 및 포트가 클라이언트가 서비스에 연결할 수 있도록 명시적으로 구성되었는지 확인하십시오. 다음은 엔드포인트 디바이스 선택에 도움이 되는 몇 가지 추가 고려 사항입니다.

- Windows — Windows Amazon WorkSpaces 클라이언트를 활용하려면 4.x 클라이언트가 필요한 64비트 Microsoft Windows 8.1, Windows 10 데스크톱을 실행해야 합니다. 사용자는 로컬 시스템에 대한 관리자 권한 없이 자신의 사용자 프로필만으로 클라이언트를 설치할 수 있습니다. 시스템 관리자는 그룹 정책, Microsoft Endpoint Manager Configuration Manager (MEMCM) 또는 환경에서 사용되는 기타 애플리케이션 배포 도구를 사용하여 관리형 엔드포인트에 클라이언트를 배포할 수 있습니다. Windows 클라이언트는 최대 4개의 디스플레이와 3840x2160의 최대 해상도를 지원합니다.
- macOS — 최신 macOS Amazon 클라이언트를 WorkSpaces 배포하려면 macOS 디바이스에서 macOS 10.12 (Sierra) 이상을 실행해야 합니다. 엔드포인트가 OSX 10.8.1 이상을 실행하는 WorkSpaces 경우 이전 버전의 WorkSpaces 클라이언트를 배포하여 PCoIP에 연결할 수 있습니다. macOS 클라이언트는 최대 2개의 4K 해상도 모니터 또는 4개의 WUXGA (1920 x 1200) 해상도 모니터를 지원합니다.
- Linux — Amazon WorkSpaces Linux 클라이언트를 실행하려면 64비트 우분투 18.04 (AMD64) 가 필요합니다. Linux 엔드포인트에서 이 OS 버전을 실행하지 않는 경우 Linux 클라이언트는 지원되지 않습니다. Linux 클라이언트를 배포하거나 사용자에게 등록 코드를 제공하기 전에 WorkSpaces 디렉터리 수준에서 Linux 클라이언트 액세스를 활성화해야 합니다. 이 액세스는 기본적으로 비활성화되며 활성화될 때까지 사용자가 Linux 클라이언트에서 연결할 수 없기 때문입니다. Linux 클라이언트는 4K 해상도 모니터 2개 또는 WUXGA (1920 x 1200) 해상도 모니터 4대를 지원합니다.
- iPad — 아마존 WorkSpaces iPad 클라이언트 애플리케이션은 PCoIP를 WorkSpaces 지원합니다. 지원되는 아이패드는 iOS 8.0 이상이 설치된 아이패드2 이상, iOS 8.0 이상이 설치된 아이패드 레티나, iOS 8.0 이상이 설치된 아이패드 미니, iOS 9.0 이상이 설치된 아이패드 프로입니다. 사용자가 연결할 기기가 해당 기준을 충족하는지 확인하세요. iPad 클라이언트 애플리케이션은 다양한 제스처를 지원합니다. (지원되는 제스처의 전체 목록을 참조하십시오.) Amazon WorkSpaces iPad 클라이

언트 애플리케이션은 스위프트포인트 ProPoint, GT 및 PadPoint 마우스도 지원합니다. 스위프트포인트, 트랙포인트 PenPoint 및 GoPoint 마우스는 지원되지 않습니다.

- 안드로이드/크롬북 — 안드로이드 기기 또는 크롬북을 최종 사용자를 위한 엔드포인트로 배포하려는 경우 고려해야 할 몇 가지 사항이 있습니다. 이 WorkSpaces 클라이언트는 PCoIP만 지원하므로 연결할 사용자가 PCoIP인지 WorkSpaces 확인하세요. WorkSpaces 이 클라이언트는 단일 디스플레이만 지원합니다. 사용자가 다중 모니터 지원을 필요로 하는 경우 다른 엔드포인트를 활용하십시오. Chromebook을 배포하려면 배포하는 모델이 Android 애플리케이션 설치를 지원하는지 확인하세요. 전체 기능 지원은 Android 클라이언트에서만 지원되며 기존 Chromebook 클라이언트에서는 지원되지 않습니다. 이는 일반적으로 2019년 이전에 제조된 크롬북의 경우에만 고려할 사항입니다. Android에서 OS 4.4 이상을 실행하는 경우 태블릿과 휴대폰 모두에 Android 지원이 제공됩니다. 하지만 최신 WorkSpace Android 클라이언트를 활용하려면 Android 기기에서 OS 9 이상을 실행하는 것이 좋습니다. Chromebook에서 WorkSpaces 클라이언트 버전 3.0.1 이상을 실행하는 경우 이제 사용자는 셀프 서비스 기능을 이용할 수 있습니다. WorkSpaces 또한 관리자는 신뢰할 수 있는 기기 인증서를 활용하여 신뢰할 수 있는 기기에 WorkSpaces 대한 액세스를 유효한 인증서로 제한할 수 있습니다.
- 웹 액세스 — 사용자는 웹 브라우저를 사용하여 어느 WorkSpaces 위치에서든 Windows에 액세스할 수 있습니다. 따라서 잠겨진 디바이스 또는 제한적인 네트워크를 사용해야 하는 사용자에게 적합합니다. 기존 원격 액세스 솔루션을 사용하고 적절한 클라이언트 애플리케이션을 설치하는 대신 웹 사이트를 방문하여 작업 리소스에 액세스할 수 있습니다. 사용자는 WorkSpaces 웹 액세스를 사용하여 Windows 10 또는 non-graphics-based Windows Server 2016 (데스크톱 경험 포함) 을 WorkSpaces 실행하는 Windows PCoIP에 연결할 수 있습니다. 사용자는 Chrome 53 이상 또는 Firefox 49 이상을 사용하여 연결해야 합니다. WSP 기반의 WorkSpaces 경우 사용자는 WorkSpaces 웹 액세스를 활용하여 그래픽이 아닌 Windows 기반에 연결할 수 있습니다. WorkSpaces 이러한 사용자는 Microsoft Edge 91 이상 또는 Google Chrome 91 이상을 사용하여 연결해야 합니다. 지원되는 최소 화면 해상도는 960 x 720이고 지원되는 최대 해상도는 2560 x 1600입니다. 다중 모니터는 지원되지 않습니다. 최상의 사용자 경험을 위해 가능하면 OS 버전의 클라이언트를 사용하는 것이 좋습니다.
- PCoIP 제로 클라이언트 — PCoIP가 할당되었거나 할당될 최종 사용자에게 WorkSpaces PCoIP 제로 클라이언트를 배포할 수 있습니다. Tera2 zero 클라이언트에 직접 연결하려면 펌웨어 버전이 6.0.0 이상이어야 합니다. WorkSpace WorkSpacesAmazon에서 다단계 인증을 사용하려면 Tera2 zero 클라이언트 디바이스에서 펌웨어 버전 6.0.0 이상을 실행해야 합니다. 제로 클라이언트 하드웨어에 대한 지원 및 문제 해결은 제조업체와 함께 수행해야 합니다.
- IGEL OS — 펌웨어 버전이 11.04.280 이상이면 엔드포인트 장치에서 IGEL OS를 사용하여 PCoIP 기반으로 WorkSpaces 연결할 수 있습니다. 지원되는 기능은 현재 기존 Linux 클라이언트의 기능과 일치합니다. IGEL OS 클라이언트를 배포하거나 사용자에게 등록 코드를 제공하기 전에 WorkSpaces 디렉터리 수준에서 Linux 클라이언트 액세스를 활성화해야 합니다. 이 기능은 기본적으로 비활성화되어 있고 활성화될 때까지 사용자가 IGEL OS 클라이언트에서 연결할 수 없게 되기

때문입니다. LGel OS 클라이언트는 최대 2개의 4K 해상도 모니터 또는 4개의 WUXGA (1920x1200) 해상도 모니터를 지원합니다.

웹 액세스 클라이언트

잠긴 디바이스용으로 설계된 Web Access 클라이언트는 클라이언트 소프트웨어를 배포할 필요 WorkSpaces 없이 Amazon에 대한 액세스를 제공합니다. 웹 액세스 WorkSpaces 클라이언트는 Amazon이 Windows 운영 체제 (OS) 이고 키오스크 환경과 같이 제한된 사용자 워크플로에 사용되는 설정에서만 사용하는 것이 좋습니다. 대부분의 사용 사례는 Amazon WorkSpaces 클라이언트에서 제공하는 기능 세트를 활용합니다. 웹 액세스 클라이언트는 디바이스 및 네트워크 제한으로 인해 대체 연결 방법이 필요한 특정 사용 사례에만 권장됩니다.

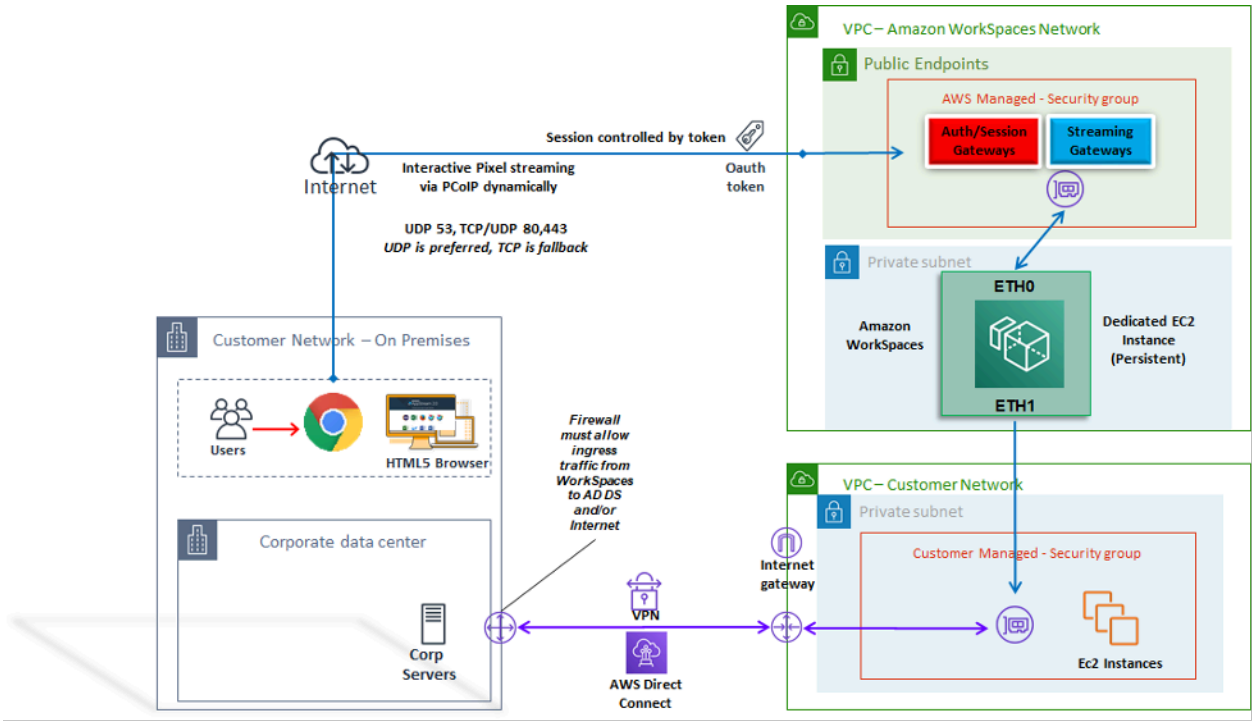

그림 20: 웹 액세스 클라이언트 아키텍처

다이어그램에서 볼 수 있듯이 웹 액세스 클라이언트는 세션을 사용자에게 스트리밍하기 위한 네트워크 요구 사항이 다릅니다. Windows에서는 PCoIP 또는 WSP 프로토콜을 WorkSpaces 사용하여 웹 액세스를 사용할 수 있습니다. 게이트웨이를 통한 인증 및 등록을 위해서는 DNS 및 HTTP/HTTPS가 필요합니다. WorkSpaces WSP 프로토콜을 사용하려면 WSP 게이트웨이 IP 주소 범위에 UDP/TCP 4195를 직접 연결해야 합니다. WorkSpaces 스트리밍 트래픽은 전체 Amazon WorkSpaces 클라이언트에서처럼 고정 포트에 할당되지 않고, 대신 동적으로 할당됩니다. 스트리밍 트래픽에는 UDP를 사용하는 것이 좋지만 UDP가 제한되면 웹 브라우저는 TCP로 대체됩니다. TCP/UDP 포트 4172가 차단되

고 조직적 제한으로 인해 차단을 해제할 수 없는 환경에서 웹 액세스 클라이언트는 사용자에게 대체 연결 방법을 제공합니다.

기본적으로 웹 액세스 클라이언트는 디렉터리 수준에서 사용하지 않도록 설정되어 있습니다. 사용자가 웹 브라우저를 WorkSpaces 통해 Amazon에 액세스할 수 있게 하려면 를 사용하여 디렉터리 설정을 업데이트하거나 프로그래밍 방식으로 WorkspaceAccessProperties API를 사용하여 Allow로 DeviceTypeWeb 수정하십시오. AWS Management Console 또한 관리자는 그룹 정책 설정이 로그인 요구 사항과 충돌하지 않는지 확인해야 합니다.

아마존 WorkSpaces 태그

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- 리소스당 최대 태그 수 - 50개
- 최대 키 길이 - 유니코드 문자 127자
- 최대 값 길이 - 유니코드 문자 255자
- 태그 키와 값은 대/소문자를 구분합니다. 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 공백 및 숫자와 특수 문자 + - = . _ : / @입니다. 선행 또는 후행 공백을 사용하면 안 됩니다.
- aws: 또는 aws:workspaces: 접두사는 사용 전용이므로 태그 이름 또는 값에 사용하지 마십시오. AWS 이러한 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다.

태그를 지정할 수 있는 리소스

- 생성 시 가져온 이미지 WorkSpaces, IP 접근제어 그룹 등의 리소스에 태그를 추가할 수 있습니다.
- 등록된 디렉토리, 사용자 지정 번들, 이미지 WorkSpaces, IP 접근제어 그룹 등의 유형의 기존 리소스에 태그를 추가할 수 있습니다.

  비용 할당 태그 사용

Cost Explorer에서 WorkSpaces 리소스 태그를 보려면 AWS Billing and Cost Management 및 Cost Management 사용 설명서의 사용자 정의 비용 할당 태그 활성화에 나와 있는 지침에 따라 WorkSpaces 리소스에 적용한 태그를 활성화하십시오.

태그는 활성화 후 24시간 후에 나타나지만 해당 태그와 관련된 값이 Cost Explorer에 나타나고 비용 데이터를 제공하는 데 4~5일이 걸릴 수 있습니다. 태그가 지정된 WorkSpaces 리소스에는 해당 기간 동안 요금이 부과되어야 합니다. Cost Explorer에는 태그가 활성화된 이후 이후의 비용 데이터만 표시됩니다. 현재로서는 과거 데이터가 제공되지 않습니다.

태그 관리

를 사용하여 기존 리소스의 태그를 업데이트하려면 태그 생성 및 태그 삭제 명령을 사용합니다. AWS CLI 대량 업데이트와 대량의 WorkSpaces 리소스에서 작업을 자동화하기 위해 Amazon은 AWS Resource Groups Tag Editor에 대한 지원을 WorkSpaces 추가합니다. AWS Resource Groups Tag Editor를 사용하면 다른 AWS 리소스와 WorkSpaces 함께 AWS 태그를 추가, 편집 또는 삭제할 수 있습니다.

아마존 WorkSpaces 서비스 쿼터

Service Quotas를 사용하면 한도라고도 하는 특정 할당량의 값을 쉽게 조회할 수 있습니다. 특정 서비스의 모든 할당량을 조회할 수도 있습니다.

할당량을 보려면 WorkSpaces

1. Service Quotas 콘솔로 이동합니다.
2. 왼쪽 탐색 창에서 서비스를 선택합니다. AWS
3. WorkSpaces목록에서 Amazon을 선택하거나 사전 입력 검색 WorkSpaces 필드에 Amazon을 입력합니다.
4. 설명과 Amazon 리소스 이름 (ARN) 등 할당량에 대한 추가 정보를 보려면 할당량 이름을 선택하십시오.

WorkSpaces Amazon은 이미지, 번들, 디렉터리, 연결 별칭, IP 제어 그룹 등 WorkSpaces 특정 지역의 계정에서 사용할 수 있는 다양한 리소스를 제공합니다. Amazon Web Services 계정을 생성하면 생성할 수 있는 리소스 수에 대한 기본 할당량 (한도라고도 함) 이 설정됩니다.

Service Quotas 콘솔을 사용하여 기본 Service Quotas를 보거나 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다.

자세한 내용은 Service Quotas 사용 설명서의 서비스 할당량 보기 및 할당량 증가 요청을 참조하십시오.

아마존 WorkSpaces 배포 자동화

WorkSpacesAmazon을 사용하면 몇 분 안에 Microsoft Windows 또는 Amazon Linux 데스크톱을 시작하고 온프레미스 또는 외부 네트워크에서 데스크톱 소프트웨어에 안전하고 안정적이며 빠르게 연결하고 액세스할 수 있습니다. Amazon 프로비저닝을 자동화하여 WorkSpaces Amazon을 기존 프로비저닝 WorkSpaces 워크플로에 통합할 수 있습니다.

일반적인 자동화 방법 WorkSpaces

고객은 다양한 도구를 사용하여 Amazon을 신속하게 WorkSpaces 배포할 수 있습니다. 이 도구를 사용하면 관리를 단순화하고 비용을 WorkSpaces 절감하며 빠르게 확장하고 이동할 수 있는 민첩한 환경을 구축할 수 있습니다.

AWS CLI 및 API

대규모 서비스와 안전하게 상호 작용하는 데 사용할 수 있는 Amazon WorkSpaces API 작업이 있습니다. 모든 퍼블릭 API는 AWS CLI SDK 및 Tools for 와 함께 사용할 수 있지만 PowerShell, 이미지 생성과 같은 프라이빗 API는 를 통해서만 사용할 수 있습니다. AWS Management Console WorkSpacesAmazon의 운영 관리 및 비즈니스 셀프 서비스를 고려할 때는 WorkSpaces API를 사용하려면 기술적 전문 지식과 보안 권한이 필요하다는 점을 고려하십시오.

SDK를 사용하여 API를 호출할 수 있습니다. AWS AWS PowerShellWindows용 도구와 PowerShell Core용 AWS 도구는 .NET용 AWS SDK에서 제공하는 기능을 기반으로 구축된 PowerShell 모듈입니다. 이러한 모듈을 사용하면 PowerShell 명령줄에서 AWS 리소스에 대한 작업을 스크립팅하고 기존 도구 및 서비스와 통합할 수 있습니다. 예를 들어 API 호출을 사용하면 AD와 통합하여 사용자의 AD 그룹 구성원을 WorkSpaces 기반으로 프로비저닝 및 서비스 해제를 수행함으로써 WorkSpaces 라이프사이클을 자동으로 관리할 수 있습니다.

AWS CloudFormation

AWS CloudFormation 전체 인프라를 텍스트 파일로 모델링할 수 있습니다. 이 템플릿은 인프라를 위한 단일 정보 소스가 됩니다. 이를 통해 조직 전체에서 사용되는 인프라 구성 요소를 표준화하여 구성을 준수하고 문제 해결 시간을 단축할 수 있습니다.

AWS CloudFormation 안전하고 반복 가능한 방식으로 리소스를 프로비저닝하여 인프라와 애플리케이션을 구축하고 재구축할 수 있도록 합니다. 환경을 CloudFormation 커미셔닝 및 서비스 해제하는 데 사

용할 수 있는데, 이는 반복 가능한 방식으로 구축하고 서비스 해제하려는 계정이 여러 개 있을 때 유용합니다. WorkSpacesAmazon의 운영 관리 및 비즈니스 셀프 서비스를 고려할 때는 기술 전문 지식과 보안 AWS CloudFormation권한이 필요하다는 점을 고려하십시오.

셀프서비스 포털 WorkSpaces

고객은 빌드 온 WorkSpaces API 명령 및 기타 AWS 서비스를 사용하여 WorkSpaces 셀프 서비스 포털을 만들 수 있습니다. 이를 통해 고객은 프로세스를 간소화하여 대규모로 배포하고 WorkSpaces 재확보할 수 있습니다. WorkSpaces 포털을 사용하면 직원들이 각 요청에 대해 IT 부서의 개입이 필요 없는 통합된 승인 워크플로우를 스스로 WorkSpaces 준비하도록 할 수 있습니다. 따라서 IT 운영 비용이 절감되는 동시에 최종 사용자가 더 빨리 시작할 수 있습니다. WorkSpaces 내장된 추가 승인 워크플로우는 기업의 데스크톱 승인 프로세스를 간소화합니다. 전용 포털은 Windows 또는 Linux 클라우드 데스크톱을 프로비저닝하기 위한 자동화된 도구를 제공하여 사용자가 데스크톱을 재구축, 재시작 또는 마이그레이션하고 암호 재설정을 위한 기능을 제공할 수 있도록 합니다 WorkSpace.

이 문서의 추가 정보 섹션에는 셀프 서비스 WorkSpaces 포털을 만드는 방법에 대한 예시가 나와 있습니다. AWS 파트너는 를 통해 사전 구성된 WorkSpaces 관리 포털을 제공합니다. AWS Marketplace

엔터프라이즈 IT 서비스 관리와의 통합

기업이 대규모 가상 데스크톱 솔루션으로 Amazon을 WorkSpaces 채택함에 따라 IT 서비스 관리(ITSM) 시스템을 구현하거나 통합해야 할 필요성이 대두되었습니다. ITSM 통합을 통해 프로비저닝 및 운영을 위한 셀프 서비스 제품을 제공할 수 있습니다. Service Catalog를 사용하면 일반적으로 배포되는 AWS 서비스와 프로비전된 소프트웨어 제품을 중앙에서 관리할 수 있습니다. 이 서비스를 통해 조직은 일관된 거버넌스 및 규정 준수 요구 사항을 달성하는 동시에 사용자는 필요한 승인된 AWS 서비스만 배포할 수 있습니다. Service Catalog는 다음과 같은 IT 서비스 관리 도구 내에서 WorkSpaces Amazon을 위한 셀프 서비스 수명 주기 관리 서비스를 활성화하는 데 사용할 수 있습니다. ServiceNow

WorkSpaces 배포 자동화 모범 사례

WorkSpaces 배포 자동화를 선택하고 설계하는 Well Architected 원칙을 고려해야 합니다.

- 자동화를 위한 설계 — 프로세스에서 수동 개입을 최소한으로 줄여 반복성과 확장이 가능하도록 설계합니다.
- 비용 최적화를 위한 설계 — 자동 생성 및 WorkSpaces 재확보를 통해 리소스를 제공하는 데 필요한 관리 노력을 줄이고 유휴 또는 미사용 리소스로 인해 불필요한 비용이 발생하지 않도록 할 수 있습니다.

- 효율성을 위한 설계 — 생성 및 종료에 필요한 리소스를 최소화합니다. WorkSpaces 가능하면 비즈니스에 Tier 0 셀프 서비스 기능을 제공하여 효율성을 개선하세요.
- 유연성을 위한 설계 — 여러 시나리오를 처리할 수 있는 일관된 배포 메커니즘을 만들고 동일한 메커니즘 (태그가 지정된 사용 사례 및 프로필 식별자를 사용하여 사용자 지정) 으로 확장할 수 있습니다.
- 생산성을 위한 설계 — 리소스를 추가하거나 제거하는 데 필요한 올바른 권한 부여 및 검증이 가능하도록 WorkSpaces 운영을 설계하세요.
- 확장성을 고려한 설계 — Amazon에서 WorkSpaces 사용하는 pay-as-you go 모델은 필요에 따라 리소스를 생성하고 더 이상 필요하지 않을 때는 리소스를 제거함으로써 비용을 절감할 수 있습니다.
- 보안을 위한 설계 — 리소스를 추가하거나 제거하는 데 필요한 올바른 권한 부여 및 검증을 허용하도록 WorkSpaces 운영을 설계하십시오.
- 지원 가능성을 고려한 설계 — 비침습적 지원, 복구 메커니즘 및 프로세스를 허용하도록 WorkSpaces 운영을 설계하십시오.

Amazon WorkSpaces 패치 및 인플레이스 업그레이드

WorkSpacesAmazon에서는 Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise 또는 Ansible과 같은 기존 타사 도구를 사용하여 패치 및 업데이트를 관리할 수 있습니다. 보안 패치를 즉시 배포하면 일반적으로 월별 패치 주기가 유지되며 에스컬레이션 또는 신속한 배포를 위한 추가 프로세스가 포함됩니다. 하지만 전체 운영 체제 업그레이드나 기능 업데이트의 경우 특별한 고려 사항이 필요한 경우가 많습니다.

WorkSpace 유지 관리

WorkSpaces Amazon에는 Amazon WorkSpaces 에이전트 업데이트와 사용 가능한 운영 체제 업데이트를 WorkSpace 설치하는 기본 유지 관리 기간이 있습니다. WorkSpaces 예정된 유지 관리 기간 동안에는 사용자 연결이 불가능합니다.

- AlwaysOn WorkSpaces 기본 유지 관리 기간은 매주 일요일 아침 00시부터 4시까지입니다. WorkSpace

- 시간대 리디렉션은 기본적으로 활성화되며 사용자의 현지 시간대에 맞게 기본 창을 재정의할 수 있습니다.
- 그룹 정책을 WorkSpaces 사용하여 Windows의 시간대 리디렉션을 사용하지 않도록 설정할 수 있습니다. PCoIP Agent conf를 사용하여 WorkSpacesLinux의 시간대 리디렉션을 사용하지 않도록 설정할 수 있습니다.

- AutoStop WorkSpaces 중요한 업데이트를 설치하기 위해 한 달에 한 번 자동으로 시작됩니다. 매월 세 번째 월요일부터 최대 2주 동안 유지 관리 기간은 해당 지역의 시간대를 기준으로 매일 약 00:00 ~ 05:00 에 열립니다. AWS WorkSpace 유지 관리 기간에서 언제든지 유지 관리할 WorkSpace 수 있습니다.

- 유지 관리에 AutoStop WorkSpaces 사용되는 시간대를 수정할 수는 없지만 해당 시간대의 유지 관리 기간은 비활성화할 수 있습니다 AutoStop WorkSpaces.

- 수동 유지 관리 기간은 상태를 ADMIN_MAINTANCE로 설정하여 원하는 일정에 따라 설정할 수 있습니다. WorkSpace

- AWS CLI 명령을 사용하여 WorkSpace 상태를 ADMIN_MAINTANCE로 수정할 modify-workspace-state수 있습니다.

아마존 리눅스 WorkSpaces

Amazon Linux WorkSpaces 사용자 지정 이미지의 업데이트와 패치를 관리하기 위한 고려 사항, 사전 요구 사항 및 제안 패턴은 Amazon WorkSpaces for Linux 이미지 준비 모범 사례 백서를 참조하십시오.

Linux 패치 사전 요구 사항 및 고려 사항

- Amazon Linux 리포지토리는 인터넷에서 액세스할 수 있는 퍼블릭 엔드포인트 또는 프라이빗 엔드포인트를 통해 액세스할 수 있는 Amazon Simple Storage Service (Amazon S3) 버킷에 호스팅됩니다. Amazon Linux에서 인터넷에 액세스할 수 없는 경우 업데이트에 액세스할 수 있도록 하려면 다음 프로세스를 참조하십시오. Amazon Linux 1 또는 Amazon Linux 2를 실행하는 EC2 인스턴스에서 인터넷 액세스 없이 yum을 업데이트하거나 패키지를 설치하려면 어떻게 해야 WorkSpaces 합니까?
- Linux의 기본 유지 관리 기간은 구성할 수 없습니다. WorkSpaces 이 창을 사용자 지정해야 하는 경우 수동 유지 관리 프로세스를 활용할 수 있습니다.

아마존 윈도우 패치

기본적으로 WorkSpaces Windows는 WorkSpaces VPC의 인터넷 액세스를 필요로 하는 Windows Update로부터 업데이트를 수신하도록 구성되어 있습니다. Windows용 자동 업데이트 메커니즘을 직접 구성하려면 Windows 서버 업데이트 서비스 (WSUS) 및 구성 관리자 설명서를 참조하십시오.

아마존 윈도우 인플레이스 업그레이드

- Windows 10에서 이미지를 생성하려는 경우 WorkSpace, 이전 버전에서 업그레이드된 Windows 10 시스템 (Windows 기능/버전 업그레이드) 에서는 이미지 생성이 지원되지 않는다는 점에 유의하십시오. 하지만 Windows 누적 업데이트 또는 보안 업데이트는 WorkSpaces 이미지 생성 및 캡처 프로세스에서 지원됩니다.

- 사용자 지정 Windows 10 BYOL (Bring Your Own License) 이미지는 BYOL 가져오기 프로세스의 소스로 VM에서 지원되는 최신 버전의 Windows로 시작해야 합니다. 자세한 내용은 BYOL 가져오기 설명서를 참조하십시오.

Windows 인플레이스 업그레이드 사전 요구 사항

- Active Directory 그룹 정책 또는 SCCM을 사용하여 Windows 10 업그레이드를 연기하거나 일시 중지한 경우 Windows 10용 운영 체제 업그레이드를 사용하도록 설정하세요. WorkSpaces
- WorkSpace AutoStop WorkSpace인 경우 업그레이드 기간에 AutoStop 맞춰 시간을 최소 3시간으로 변경하십시오.
- 전체 업그레이드 프로세스에서는 기본 사용자 (C:\Users\Default) 의 복사본을 만들어 사용자 프로필을 다시 만듭니다. 기본 사용자 프로필을 사용하여 사용자 지정하지 마십시오. 대신 그룹 정책 개체 (GPO) 를 통해 사용자 프로필을 사용자 지정하는 것이 좋습니다. GPO를 통해 사용자 지정한 내용은 쉽게 수정하거나 롤백할 수 있으며 오류가 발생할 가능성이 적습니다.
- 인플레이스 업그레이드 프로세스는 사용자 프로필을 하나만 백업하고 다시 만들 수 있습니다. D 드라이브에 사용자 프로필이 여러 개 있는 경우 필요한 프로필을 제외한 모든 프로필을 삭제하세요.

Windows 인플레이스 업그레이드 고려 사항

- 전체 업그레이드 프로세스에서는 두 개의 레지스트리 스크립트 (enable-inplace-upgrade.ps1 및 update-pvdrivers.ps1) 를 사용하여 필요한 내용을 변경하고 Windows 업데이트 프로세스를 실행할 수 있도록 합니다. WorkSpaces 이러한 변경에는 D 드라이브 대신 C 드라이브에 임시 사용자 프로필을 만드는 작업이 포함됩니다. 사용자 프로필이 드라이브 D에 이미 있는 경우 원래 사용자 프로필의 데이터는 D 드라이브에 남아 있습니다.
- 전체 업그레이드를 배포한 후에는 사용자 프로필을 D 드라이브에 복원하여 사용자 프로필을 다시 빌드하거나 마이그레이션할 수 있도록 하고 사용자 셸 폴더 리디렉션과 관련된 잠재적 문제를 방지해야 합니다. WorkSpaces BYOL 업그레이드 참조 페이지에 설명된 대로 PostUpgradeRestoreProfileOnD 레지스트리 키를 사용하여 이 작업을 수행할 수 있습니다.

아마존 WorkSpaces 언어 팩

Windows 10 데스크톱 환경을 제공하는 Amazon WorkSpaces 번들은 영어 (미국), 프랑스어 (캐나다), 한국어 및 일본어를 지원합니다. 하지만 스페인어, 이탈리아어, 포르투갈어 및 기타 여러 언어 옵션에 대한 추가 언어 팩을 포함할 수 있습니다. 자세한 내용은 영어가 아닌 클라이언트 언어를 사용하여 새 Windows WorkSpace 이미지를 만들려면 어떻게 해야 하나요? 를 참조하십시오. .

아마존 WorkSpaces 프로필 관리

WorkSpaces Amazon은 모든 프로필 쓰기를 별도의 Amazon EBS (Elastic Block Store) 볼륨으로 리디렉션하여 사용자 프로필을 기본 운영 체제 (OS) 와 분리합니다. 마이크로소프트 윈도우에서는 사용자 프로필이 D:\Users\username 에 저장됩니다. 아마존 리눅스에서는 사용자 프로필이 /home에 저장됩니다. EBS 볼륨은 12시간마다 자동으로 스냅샷이 생성됩니다. WorkSpace 스냅샷은 Amazon을 재구축하거나 복원할 때 사용할 수 있도록 AWS 관리형 S3 버킷에 자동으로 저장됩니다.

대부분의 조직에서 12시간마다 자동 스냅샷을 생성하는 것이 사용자 프로필을 백업하지 않는 기존 데스크톱 배포보다 우수합니다. 그러나 고객은 데스크톱에서 새 AWS OS/지역으로 마이그레이션, DR 지원 등과 같이 사용자 프로필을 보다 세밀하게 제어해야 할 수 있습니다. WorkSpaces Amazon에서 사용할 수 있는 다른 프로필 관리 방법이 WorkSpaces 있습니다.

폴더 리디렉션

폴더 리디렉션은 가상 데스크톱 인프라 (VDI) 아키텍처의 일반적인 설계 고려 사항이지만 Amazon 설계의 모범 사례 또는 일반적인 요구 사항은 아닙니다. WorkSpaces 그 이유는 WorkSpaces Amazon이 애플리케이션 및 사용자 데이터를 별도로 보관할 수 있는 영구 DaaS (Desktop as a Service) 솔루션이기 때문입니다.

재해 복구 (DR) 환경에서 사용자 프로필 데이터에 대한 즉각적인 복구 지점 목표 (RPO) 와 같이 사용자 셸 폴더에 대한 폴더 리디렉션 (예: D:\Users\username\Desktop redirected to\\ Server\ RedirectionShare $\ username\ Desktop) 이 필요한 특정 시나리오가 있습니다.

모범 사례

강력한 폴더 리디렉션을 위한 다음 모범 사례가 나열되어 있습니다.

- Amazon이 출시된 AWS 지역과 동일한 지역 및 WorkSpaces AZ에 Windows 파일 서버를 호스팅합니다.

- AD 보안 그룹 인바운드 규칙에 Windows 파일 서버 보안 그룹 또는 사설 IP 주소가 포함되는지 확인하고, 그렇지 않으면 온프레미스 방화벽이 동일한 TCP 및 UDP 포트 기반 트래픽을 허용하는지 확인하십시오.
- Windows 파일 서버 보안 그룹 인바운드 규칙에 모든 Amazon 보안 그룹에 대한 TCP 445 (SMB) 가 포함되어 있는지 확인하십시오. WorkSpaces
- Amazon WorkSpaces 사용자를 위한 AD 보안 그룹을 생성하여 Windows 파일 공유에 대한 사용자의 액세스 권한을 부여하십시오.
- DFS 네임스페이스 (DFS-N) 및 DFS 복제 (DFS-R) 를 사용하면 Windows 파일 공유가 특정 Windows 파일 서버에 연결되지 않고 민첩하게 작동하고 모든 사용자 데이터가 Windows 파일 서버 간에 자동으로 복제되도록 할 수 있습니다.
- Windows 탐색기에서 네트워크 공유를 검색할 때 공유 이름 끝에 '$'를 추가하여 공유 호스팅 사용자 데이터가 보이지 않게 숨길 수 있습니다.
- 리디렉션된 폴더에 대한 Microsoft의 지침인 오프라인 파일을 사용한 폴더 리디렉션 배포에 따라 파일 공유를 생성합니다. 보안 권한 및 GPO 구성 지침을 자세히 따르세요.
- Amazon WorkSpaces 배포가 BYOL (Bring Your Own License) 인 경우 Microsoft의 지침: 개별 리디렉션된 폴더의 오프라인 파일 비활성화 지침에 따라 오프라인 파일 비활성화도 지정해야 합니다.
- Windows 파일 서버가 Windows Server 2016 이상인 경우 데이터 중복 제거 (일반적으로 '중복 제거'라고 함) 를 설치하고 실행하여 스토리지 소비를 줄이고 비용을 최적화하십시오. 데이터 중복 제거 설치 및 활성화 및 데이터 중복 제거 실행을 참조하십시오.
- 기존 조직 백업 솔루션을 사용하여 Windows 파일 서버 파일 공유를 백업하십시오.

피해야 할 사항

- WAN (광역 네트워크) 연결을 통해서만 액세스할 수 있는 Windows 파일 서버는 사용하지 마십시오. SMB 프로토콜은 이러한 용도로 설계되지 않았기 때문입니다.
- 사용자가 실수로 사용자 셸 폴더를 삭제할 가능성을 줄이기 위해 홈 디렉터리에 사용되는 것과 동일한 Windows 파일 공유를 사용하지 마십시오.
- 파일을 쉽게 복원하려면 VSS (볼륨 섀도 복사본 서비스) 를 사용하도록 설정하는 것이 좋지만, 이 방법만으로는 Windows 파일 서버 파일 공유를 백업해야 하는 요구 사항이 제거되지 않습니다.

기타 고려 사항

- Windows File Server용 Amazon FSx는 Windows 파일 공유를 위한 관리형 서비스를 제공하며, 자동 백업을 포함하여 폴더 리디렉션의 운영 오버헤드를 단순화합니다.
- 기존 조직 백업 솔루션이 없는 AWS Storage Gateway 경우 SMB 파일 공유를 활용하여 파일 공유를 백업하십시오.

프로필 설정

그룹 정책

엔터프라이즈 Microsoft Windows 배포의 일반적인 모범 사례는 GPO (그룹 정책 개체) 및 GPP (그룹 정책 기본 설정) 설정을 통해 사용자 환경 설정을 정의하는 것입니다. 바로 가기, 드라이브 매핑, 레지스트리 키, 프린터 등의 설정은 그룹 정책 관리 콘솔을 통해 정의됩니다. GPO를 통해 사용자 환경을 정의함으로써 얻을 수 있는 이점은 다음과 같지만 이에 국한되지는 않습니다.

- 중앙 집중식 구성 관리
- AD 보안 그룹 구성원 또는 OU 배치에 의해 정의된 사용자 프로필
- 설정 삭제에 대한 보호
- 최초 로그온 시 프로필 생성 및 개인화 자동화
- 향후 업데이트의 용이성

> **Note**
>
> 그룹 정책 성능을 최적화하기 위한 Microsoft의 모범 사례를 따르세요.

대화형 로그온 배너 그룹 정책은 Amazon에서 지원되지 않으므로 사용해서는 안 됩니다. WorkSpaces 배너는 AWS 지원 요청을 통해 Amazon WorkSpaces 클라이언트에 표시됩니다. 또한 이동식 디바이스는 Amazon에서 필수이므로 그룹 정책을 통해 차단해서는 안 됩니다 WorkSpaces.

GPO를 사용하여 WorkSpaces Windows를 관리할 수 있습니다. 자세한 내용은 Windows WorkSpaces 관리를 참조하십시오.

아마존 WorkSpaces 볼륨

각 Amazon WorkSpaces 인스턴스에는 운영 체제 볼륨과 사용자 볼륨이라는 두 개의 볼륨이 있습니다.

- Amazon Windows WorkSpaces — C:\ 드라이브는 운영 체제 (OS) 에 사용되고 D:\ 드라이브는 사용자 볼륨입니다. 사용자 프로필은 사용자 볼륨 (AppData, 문서, 사진, 다운로드 등) 에 있습니다.
- 아마존 리눅스 WorkSpaces — 아마존 WorkSpace 리눅스에서는 시스템 볼륨 (/dev/xvda1) 이 루트 폴더로 마운트됩니다. 사용자 볼륨은 사용자 데이터 및 애플리케이션용이고 /dev/xvdf1은 /home으로 마운트됩니다.

운영 체제 볼륨의 경우 이 드라이브의 시작 크기를 80GB 또는 175GB로 선택할 수 있습니다. 사용자 볼륨의 경우 시작 크기를 10GB, 50GB 또는 100GB로 선택할 수 있습니다. 필요에 따라 두 볼륨 크기를 최대 2TB까지 늘릴 수 있지만 사용자 볼륨을 100GB 이상으로 늘리려면 OS 볼륨이 175GB여야 합니다. 볼륨 변경은 볼륨당 6시간마다 한 번만 수행할 수 있습니다. WorkSpaces 볼륨 크기 수정에 대한 추가 정보는 관리 가이드의 수정 WorkSpace 섹션을 참조하십시오.

WorkSpaces 볼륨 모범 사례

Amazon WorkSpaces 배포를 계획할 때는 OS 설치, 인플레이스 업그레이드 및 OS 볼륨의 이미지에 추가할 추가 핵심 애플리케이션에 대한 최소 요구 사항을 고려하는 것이 좋습니다. 사용자 볼륨의 경우 먼저 디스크 할당량을 줄이고 필요에 따라 사용자 볼륨 크기를 점진적으로 늘리는 것이 좋습니다. 디스크 볼륨의 크기를 최소화하면 실행 비용이 줄어듭니다. WorkSpace

> **Note**
>
> 볼륨 크기는 늘릴 수 있지만 줄일 수는 없습니다.

아마존 WorkSpaces 로깅

Amazon WorkSpaces 환경에는 문제를 해결하고 전체 WorkSpaces 성능을 모니터링하기 위해 캡처할 수 있는 많은 로그 소스가 있습니다.

Amazon WorkSpaces Client 3.x 각 Amazon WorkSpaces 클라이언트의 클라이언트 로그는 다음 디렉터리에 있습니다.

- 윈도우 — %LOCALAPPDATA%\ 아마존 웹 서비스\ 아마존\ 로그 WorkSpaces
- macOS — ~/라이브러리/"애플리케이션 지원"/"아마존 웹 서비스"/"아마존 “/logs WorkSpaces

- 리눅스 (우분투 18.04 이상) — /opt/workspacesclient/workspacesclient/workspacesclient

클라이언트 측에서 세션에 진단 또는 디버깅 세부 정보가 필요한 경우가 많이 있습니다. WorkSpaces 작업 영역 실행 파일에 “-l3"을 추가하여 고급 클라이언트 로그를 활성화할 수도 있습니다. 예:

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

아마존 WorkSpaces 서비스

Amazon WorkSpaces 서비스는 Amazon CloudWatch 지표, CloudWatch 이벤트 등과 통합되어 CloudTrail 있습니다. 이 통합을 통해 성능 데이터와 API 호출을 중앙 AWS 서비스에 로깅할 수 있습니다.

Amazon WorkSpaces 환경을 관리할 때는 특정 CloudWatch 지표를 지속적으로 모니터링하여 전반적인 환경 상태를 파악하는 것이 중요합니다. 지표

Amazon에서 사용할 수 있는 다른 CloudWatch 지표도 있지만 WorkSpaces (WorkSpaces 사용 CloudWatch 지표 모니터링 참조) 다음 세 가지 지표는 WorkSpace 인스턴스 가용성을 유지하는 데 도움이 됩니다.

- 비정상 — 비정상 상태를 WorkSpaces 반환한 건수입니다.
- SessionLaunchTime— 세션을 시작하는 데 걸리는 시간. WorkSpaces
- InSessionLatency— WorkSpaces 클라이언트와 클라이언트 간의 왕복 시간. WorkSpace

WorkSpaces 로깅 옵션에 대한 자세한 내용은 사용별 Amazon WorkSpaces API 호출 로깅을 참조하십시오 CloudTrail. 추가 CloudWatch 이벤트는 사용자 세션의 클라이언트측 IP, 사용자가 세션에 연결한 시기, 연결 중에 사용된 엔드포인트를 캡처하는 데 도움이 됩니다. WorkSpaces 이러한 모든 세부 정보는 문제 해결 세션 중에 사용자가 보고한 문제를 찾아내거나 정확히 찾아내는 데 도움이 됩니다.

> **Note**
>
> 일부 CloudWatch 지표는 관리형 AD에서만 사용할 수 있습니다. AWS

아마존 리눅스용 컨테이너 및 윈도우 서브시스템 WorkSpaces

컨테이너와 아마존 WorkSpaces

Amazon에서 컨테이너 워크로드를 처리하려는 고객은 주로 최종 사용자 컴퓨팅을 이용합니다. WorkSpaces 가능하긴 하지만 이 솔루션은 선호되거나 권장되지 않습니다. 컨테이너의 잠재적 비용 및 운영 비용 절감을 실현하고자 하는 고객은 Amazon Elastic Container Service (Amazon ECS) 및/또는 Amazon Elastic Kubernetes 서비스 (Amazon EKS) 를 평가해 보는 것이 좋습니다.

고객 요구 사항에 따라 WorkSpaces Amazon을 사용하여 컨테이너를 활성화해야 하는 경우 Docker를 사용할 수 있는 기술 사용 방법이 게시되었습니다. 이를 위해서는 다른 후행 서비스가 필요하며 분리된 네이티브 컨테이너 서비스와 비교할 때 비용과 복잡성이 증가한다는 사실을 고객에게 알려야 합니다.

Linux용 Windows 서브시스템

아마존의 기본 운영 체제로 윈도우 서버 2019가 출시되면서 고객들은 리눅스용 윈도우 서브시스템 (WSL) WorkSpaces, 특히 WSL2를 구현하기를 열망하고 있습니다. WSL2는 기능을 수행하기 위해 가상 머신 (Hyper-V) 을 호출하기 때문에 하이퍼바이저로 관리되는 WorkSpaces Amazon에서는 실행할 수 없습니다. AWS 고객은 이러한 이유로 WSL1만 사용할 수 있다는 점을 알고 WSL1과 WSL2의 차이점을 이해해야 합니다.

아마존 WorkSpaces 마이그레이션

Amazon WorkSpaces 마이그레이션 기능을 사용하면 사용자 볼륨 데이터를 새 번들로 가져올 수 있습니다. 이 기능을 사용하여 다음을 수행할 수 있습니다.

- Windows 7 환경에서 Windows 10 데스크톱 환경으로 마이그레이션하십시오 WorkSpaces .
- PCoIP에서 WorkSpaces 스트리밍 프로토콜 (WSP) WorkSpace 으로 마이그레이션하십시오. WorkSpace
- 한 퍼블릭 또는 커스텀 WorkSpaces 번들에서 다른 번들로 마이그레이션하세요. 예를 들어 GPU 지원 (그래픽 및 GraphicsPro) 번들에서 GPU를 지원하지 않는 번들로 또는 그 반대로 마이그레이션할 수 있습니다.

마이그레이션 프로세스

WorkSpaces 마이그레이션을 사용하면 대상 WorkSpaces 번들을 지정할 수 있습니다. 마이그레이션 프로세스에서는 대상 번들 이미지의 새 루트 볼륨과 최신 원본 사용자 볼륨 스냅샷의 사용자 볼륨을 WorkSpace 사용하여 를 다시 생성합니다. 호환성 향상을 위해 마이그레이션 중에 새 사용자 프로필이 생성됩니다. 새 프로필로 이동할 수 없는 이전 사용자 프로필의 데이터는 .NotMigrated 폴더에 저장됩니다.

마이그레이션하는 동안 사용자 볼륨 (드라이브 D) 의 데이터는 보존되지만 루트 볼륨 (C:\ 드라이브) 의 모든 데이터는 손실됩니다. 즉, 설치된 애플리케이션, 설정 및 레지스트리 변경 사항은 유지되지 않습니다. 이전 사용자 프로필 폴더는 를 사용하여 이름이 바뀝니다. NotMigrated 접미사가 추가되고 새 사용자 프로필이 생성됩니다.

마이그레이션 프로세스는 한 번에 최대 1시간이 소요됩니다. WorkSpace 또한 마이그레이션 워크플로에서 프로세스를 완료하지 못할 경우 서비스가 마이그레이션 전의 원래 상태로 자동 롤백하여 데이터 손실 위험을 최소화합니다. WorkSpace

WorkSpace 원본에 할당된 모든 태그는 마이그레이션 중에 그대로 유지됩니다. 의 실행 WorkSpace 모드는 보존됩니다. WorkSpace 마이그레이션된 항목은 새 WorkSpace ID, 컴퓨터 이름 및 IP 주소를 가집니다. 마이그레이션 절차

Amazon WorkSpaces 콘솔, migrate-workspace 명령 또는 Amazon WorkSpaces WorkSpaces API를 AWS CLI 사용하여 마이그레이션할 수 있습니다. 모든 마이그레이션 요청은 대기열에 추가되며, 마이그레이션 요청이 너무 많으면 서비스에서 자동으로 총 마이그레이션 요청 수를 조절합니다. 마이그레이션 제한

- 퍼블릭 또는 사용자 지정 Windows 7 데스크톱 환경 번들로는 마이그레이션할 수 없습니다.
- BYOL Windows 7 번들로 마이그레이션할 수 없습니다.
- BYOL은 다른 BYOL WorkSpaces 번들로만 마이그레이션할 수 있습니다.
- 공개 또는 사용자 지정 번들에서 WorkSpace 만든 번들은 BYOL 번들로 마이그레이션할 수 없습니다.
- Linux 마이그레이션은 WorkSpaces 현재 지원되지 않습니다.
- 두 개 이상의 언어를 지원하는 AWS 지역에서는 언어 번들 WorkSpaces 간에 마이그레이션할 수 있습니다.
- 소스 번들과 타겟 번들은 서로 달라야 합니다. (하지만 두 개 이상의 언어를 지원하는 지역에서는 언어가 다르더라도 동일한 Windows 10 번들로 마이그레이션할 수 있습니다.) 동일한 번들을 WorkSpace 사용하여 새로 고치려면 WorkSpace 대신 번들을 다시 빌드하세요.
- 지역 간에는 WorkSpaces 마이그레이션할 수 없습니다.
- WorkSpaces ADMIN_MAINTANCE 모드에 있는 경우에는 마이그레이션할 수 없습니다.

비용

마이그레이션이 발생한 달에는 새 버전과 원래 버전 모두에 대해 비례 할당으로 계산된 요금이 부과됩니다. WorkSpaces 예를 들어, 5월 10일에 WorkSpace A를 WorkSpace B로 마이그레이션하는 경우 5월 1일부터 5월 10일까지는 WorkSpace A 요금이 부과되고, 5월 11일부터 5월 30일까지는 WorkSpace B 요금이 부과됩니다.

WorkSpaces 마이그레이션 모범 사례

WorkSpacea를 마이그레이션하기 전에 다음을 수행하십시오.

- C 드라이브의 중요한 데이터를 다른 위치로 백업합니다. 마이그레이션 중에 C 드라이브의 모든 데이터가 지워집니다.
- 사용자 볼륨의 스냅샷이 생성되었는지 확인하려면 WorkSpace 마이그레이션하는 것이 12시간 이상 경과되었는지 확인하십시오. Amazon WorkSpaces 콘솔의 Migrate WorkSpaces 페이지에서 마지막 스냅샷의 시간을 참조할 수 있습니다. 마지막 스냅샷 이후에 생성된 모든 데이터는 마이그레이션 중에 손실됩니다.
- 잠재적 데이터 손실을 방지하려면 사용자가 해당 서버에서 로그아웃하고 마이그레이션 프로세스가 완료될 때까지 다시 로그인하지 않도록 하십시오. WorkSpaces
- WorkSpaces 마이그레이션하려는 상태가 [사용 가능], [중지됨] 또는 [오류] 인지 확인하십시오.

- 마이그레이션하는 데 필요한 IP 주소가 충분한지 확인하십시오. WorkSpaces 마이그레이션하는 동안 새 IP 주소가 에 WorkSpaces 할당됩니다.
- 스크립트를 사용하여 WorkSpaces 마이그레이션하는 경우 한 WorkSpaces 번에 25개 이하의 일괄 처리로 마이그레이션하십시오.

Well-Architected 프레임워크

AWS Well-Architected는 클라우드 설계자가 애플리케이션과 워크로드를 위한 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 인프라를 구축할 수 있도록 지원합니다. 클라우드에서 워크로드를 설계하고 실행하기 위한 주요 개념, 설계 원칙, 아키텍처 모범 사례를 설명합니다. 이는 다음과 같은 다섯 가지 핵심 요소를 기반으로 합니다.

- 운영 우수성
- 보안
- 신뢰성
- 성능 효율성
- 비용 최적화

Amazon WorkSpaces 환경을 설계할 때는 이러한 주요 요소를 평가하여 배포 성숙도 수준을 결정하고 Amazon과 함께 사용할 수 있는 추가 기능을 찾는 것이 중요합니다. WorkSpaces AWS Well-Architect Framework에 대한 전반적인 지침이 나와 있지만, 다음은 다섯 가지 요소를 각각 고려하기 위해 WorkSpaces 배포 계획 단계에 포함할 수 있는 몇 가지 주요 질문을 제공합니다.

일반

- 이 프로젝트의 비즈니스 동력은 무엇입니까?

운영 우수성

- 사용자와 여러 관리자 그룹 간에 액세스 제어를 분리하려면 어떻게 해야 할까요?

보안

1. 를 WorkSpaces 운영하기 위해 고려해야 할 보안 및 규정 준수 요구 사항은 무엇입니까?
2. 외부 IP 주소로의 라우팅에 제한이 있습니까?
3. 필요한 WorkSpaces 포트가 기업 방화벽을 통과할 수 있습니까?
4. 이 배포에 다단계 인증을 사용할 예정입니까? 아니면 사용할 예정입니까?
5. 현재 얼마나 많은 사용자 ID 및 권한 부여 요청을 하고 있습니까?

신뢰성

1. 데스크톱의 데이터 보존 정책은 무엇입니까?
2. 최종 사용자 데이터의 복구 시점 목표 (RPO) 는 무엇입니까?
3. 최종 사용자 데이터의 복구 시간 목표 (RTO) 는 얼마입니까?

비용 최적화

1. WorkSpaces 번들 크기가 사용자 사례 및 애플리케이션에 적합했습니까?
2. 사용자들이 한 달에 82시간 WorkSpaces 이상을 소비할까요?

위의 질문은 고려해야 할 항목의 전체 목록을 구성하지는 않지만 Well-Architected Amazon 배포를 지원하는 몇 가지 중요한 지침을 제공합니다. WorkSpaces

보안

이 섹션에서는 Amazon WorkSpaces 서비스를 사용할 때 암호화를 사용하여 데이터를 보호하는 방법을 설명합니다. 전송 중 및 저장 시 암호화와 보안 그룹을 사용하여 네트워크 액세스를 보호하는 방법에 대해 설명합니다 WorkSpaces. 또한 이 섹션에서는 신뢰할 수 있는 장치 및 IP 액세스 제어 그룹을 사용하여 최종 장치 액세스를 제어하는 방법에 대한 정보를 제공합니다. WorkSpaces

AWS Directory Service의 인증 (MFA 지원 포함) 에 대한 추가 정보는 이 섹션에서 확인할 수 있습니다.

전송 중 암호화

WorkSpaces Amazon은 암호화를 사용하여 다양한 통신 단계 (전송 중) 에서 기밀을 보호하고 저장 데이터 (암호화) 도 보호합니다. WorkSpaces WorkSpaces Amazon이 전송 중에 사용하는 암호화의 각 단계 프로세스는 다음 섹션에 설명되어 있습니다.

저장 중 암호화에 대한 자세한 내용은 이 문서의 암호화된 WorkSpaces 섹션을 참조하십시오.

등록 및 업데이트

데스크톱 클라이언트 애플리케이션은 HTTPS를 사용하여 Amazon과 통신하여 업데이트 및 등록을 요청합니다.

인증 단계

데스크톱 클라이언트는 인증 게이트웨이에 자격 증명을 전송하여 인증을 시작합니다. 데스크톱 클라이언트와 인증 게이트웨이 간의 통신은 HTTPS를 사용합니다. 이 단계가 끝나면 인증에 성공하면 인증 게이트웨이는 동일한 HTTPS 연결을 통해 데스크톱 클라이언트에 OAuth 2.0 토큰을 반환합니다.

> **Note**
>
> 데스크톱 클라이언트 애플리케이션은 포트 443 (HTTPS) 트래픽, 업데이트, 등록 및 인증을 위한 프록시 서버 사용을 지원합니다.

클라이언트로부터 자격 증명을 받은 후 인증 게이트웨이는 AWS Directory Service에 인증 요청을 보냅니다. 인증 게이트웨이에서 AWS Directory Service로의 통신은 HTTPS를 통해 이루어지므로 사용자 자격 증명이 일반 텍스트로 전송되지 않습니다.

인증 — 액티브 디렉터리 커넥터 (ADC)

AD Connector는 Kerberos를 사용하여 온-프레미스 AD와 인증된 통신을 설정하므로 LDAP에 바인딩하고 후속 LDAP 쿼리를 실행할 수 있습니다. ADC의 클라이언트측 LDAPS 지원을 통해 Microsoft AD와 애플리케이션 간의 쿼리를 암호화할 수도 있습니다. AWS 클라이언트측 LDAPS 기능을 구현하기 전에 클라이언트측 LDAPS의 사전 요구 사항을 검토하십시오.

AWS 디렉터리 서비스는 TLS를 통한 LDAP도 지원합니다. 사용자 자격 증명은 언제라도 일반 텍스트로 전송되지 않습니다. 보안을 강화하기 위해 VPN 연결을 사용하여 WorkSpaces VPC를 온프레미스 네트워크 (AD가 있는 네트워크) 에 연결할 수 있습니다. AWS 하드웨어 VPN 연결을 사용하는 경우 고객은 AES-128 또는 AES-256 대칭 암호화 키를 사용하는 표준 IPSEC (인터넷 키 교환 (IKE) 및 IPSEC SA), 무결성 해시의 경우 SHA-1 또는 SHA-256, 완벽한 순방향 보안 (PFS) 을 사용하는 DH 그룹 (1단계는 2,14-18, 22, 23 및 24, 2단계는 1,2,5, 14-18, 22, 23, 24) 을 사용하여 전송 중 암호화를 설정할 수 있습니다..

브로커 스테이지

(인증에 성공한 경우 인증 게이트웨이에서) OAuth 2.0 토큰을 수신한 후 데스크톱 클라이언트는 HTTPS를 사용하여 Amazon WorkSpaces 서비스 (브로커 연결 관리자) 를 쿼리합니다. 데스크톱 클라이언트는 OAuth 2.0 토큰을 전송하여 스스로를 인증하고, 그 결과 클라이언트는 스트리밍 게이트웨이의 엔드포인트 정보를 수신합니다. WorkSpaces

스트리밍 스테이지

데스크톱 클라이언트가 OAuth 2.0 토큰을 사용하여 스트리밍 게이트웨이를 사용하여 PCoIP 세션을 열도록 요청합니다. 이 세션은 AES-256 암호화되며 PCoIP 포트를 통신 제어 (4172/TCP) 에 사용합니다.

스트리밍 게이트웨이는 OAuth2.0 토큰을 사용하여 HTTPS를 통해 Amazon WorkSpaces 서비스에 사용자별 WorkSpaces 정보를 요청합니다.

또한 스트리밍 게이트웨이는 클라이언트로부터 TGT를 수신하고 (클라이언트 사용자 암호를 사용하여 암호화됨) Kerberos TGT 패스스루를 사용하여 게이트웨이는 사용자가 검색한 Kerberos TGT를 사용하여 에서 Windows 로그인을 시작합니다. WorkSpace

WorkSpace 그런 다음 표준 Kerberos 인증을 사용하여 구성된 AWS 디렉터리 서비스에 대한 인증 요청을 시작합니다.

성공적으로 로그인하면 WorkSpace PCoIP 스트리밍이 시작됩니다. 클라이언트는 포트 TCP 4172에서 연결을 시작하고 트래픽은 포트 UDP 4172에서 반환합니다. 또한 관리 인터페이스를 통한 스트리

밍 게이트웨이와 WorkSpaces 데스크톱 간의 초기 연결은 UDP 55002를 통해 이루어집니다. (Amazon의 IP 주소 및 포트 요구 사항은 설명서를 참조하십시오 WorkSpaces. 초기 아웃바운드 UDP 포트는 55002입니다. 포트 4172 (TCP 및 UDP) 를 사용하는 스트리밍 연결은 AES 128비트 및 256비트 암호를 사용하여 암호화되지만 기본값은 128비트입니다. 고객은 WorkSpaces Windows용 PCoIP 전용 AD 그룹 정책 설정을 사용하거나 Amazon Linux용 pcoip-agent.conf 파일을 사용하여 이를 256비트로 적극적으로 변경할 수 있습니다. WorkSpaces WorkSpacesAmazon의 그룹 정책 관리에 대한 자세한 내용은 설명서를 참조하십시오.

네트워크 인터페이스

각 WorkSpace Amazon에는 기본 네트워크 인터페이스와 관리 네트워크 인터페이스라는 두 개의 네트워크 인터페이스가 있습니다.

기본 네트워크 인터페이스는 AWS Directory Service, 인터넷 및 고객 기업 네트워크에 대한 액세스와 같은 고객 VPC 내부의 리소스에 대한 연결을 제공합니다. 이 기본 네트워크 인터페이스에 보안 그룹을 연결할 수 있습니다. 개념적으로 이 ENI에 연결된 보안 그룹은 배포 범위에 따라 구분됩니다 (WorkSpaces 보안 그룹 및 ENI 보안 그룹).

관리 네트워크 인터페이스

보안 그룹을 통해 관리 네트워크 인터페이스를 제어할 수는 없지만 고객은 호스트 기반 방화벽을 사용하여 포트를 차단하거나 액세스를 WorkSpaces 제어할 수 있습니다. 관리 네트워크 인터페이스에는 제한을 적용하지 않는 것이 좋습니다. 고객이 이 인터페이스를 관리하기 위해 호스트 기반 방화벽 규칙을 추가하기로 결정한 경우 Amazon WorkSpaces 서비스가 해당 인터페이스의 상태 및 접근성을 관리할 수 있도록 포트 몇 개를 열어야 합니다. WorkSpace 자세한 내용은 Amazon Workspaces 관리 안내서의 네트워크 인터페이스를 참조하십시오.

WorkSpaces 보안 그룹

기본 보안 그룹은 AWS Directory Service별로 생성되며 WorkSpaces 해당 특정 디렉터리에 속하는 모든 그룹에 자동으로 연결됩니다.

Amazon은 다른 많은 AWS 서비스와 WorkSpaces 마찬가지로 보안 그룹을 사용합니다. WorkSpaces Amazon은 사용자가 WorkSpaces 서비스에 디렉터리를 등록할 때 두 개의 AWS 보안 그룹을 생성합니다. 하나는 디렉터리 컨트롤러 디렉터리ID_Controllers용이고 다른 하나는 디렉터리 ID_WorkspacesMembers 디렉터리에 있는 디렉터리용입니다 WorkSpaces . 이 보안 그룹 중 어느 것도 삭제하지 마십시오. 그렇지 않으면 보안이 손상될 수 있습니다. WorkSpaces 기본적으

로 WorkSpaces 구성원 보안 그룹의 이그레스는 0.0.0.0/0까지 열려 있습니다. 디렉터리에 기본 WorkSpaces 보안 그룹을 추가할 수 있습니다. 새 보안 그룹을 WorkSpaces 디렉터리에 연결하면 새로 WorkSpaces 시작하거나 WorkSpaces 재구축한 기존 보안 그룹에 새 보안 그룹이 생깁니다. 이 새 기본 보안 그룹을 WorkSpaces 재구축하지 않고 기존 보안 그룹에 추가할 수도 있습니다. 여러 보안 그룹을 WorkSpaces 디렉터리에 연결하는 경우 각 보안 그룹의 규칙을 단일 규칙 세트로 WorkSpaces 집계하십시오. 보안 그룹 규칙은 가능한 한 응축하는 것이 좋습니다. 보안 그룹에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC용 보안 그룹을 참조하십시오.

WorkSpaces 디렉터리 또는 기존 WorkSpace 디렉터리에 보안 그룹을 추가하는 방법에 대한 자세한 내용은 관리 안내서를 참조하십시오. WorkSpaces

일부 고객은 WorkSpaces 트래픽이 유출할 수 있는 포트와 목적지를 제한하고자 합니다. 에서 들어오는 송신 트래픽을 제한하려면 서비스 통신에 필요한 특정 포트를 그대로 두어야 합니다. 그렇지 않으면 사용자가 해당 포트에 로그인할 수 없습니다. WorkSpaces WorkSpaces

WorkSpaces 로그인하는 WorkSpace 동안 고객 VPC의 ENI (엘라스틱 네트워크 인터페이스) 를 활용하여 도메인 컨트롤러와 통신합니다. 사용자가 WorkSpaces 성공적으로 로그인할 수 있도록 하려면 다음 포트가 _WorkspacesMembers 보안 그룹의 도메인 컨트롤러를 포함하는 CIDR 범위 또는 도메인 컨트롤러에 액세스할 수 있도록 허용해야 합니다.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 인증
- TCP/UDP 389 — LDAP
- TCP/UDP 445 - SMB
- TCP 3268-3269 - 글로벌 카탈로그
- TCP/UDP 464 - 케르베로스 비밀번호 변경
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 - NTP
- TCP/UDP 49152-65535 RPC용 임시 포트

다른 애플리케이션, 인터넷 또는 기타 위치에 WorkSpaces 액세스해야 하는 경우 _WorkspacesMembers 보안 그룹 내에서 CIDR 표기법으로 해당 포트 및 대상을 허용해야 합니다. 이러한 포트와 대상을 추가하지 않으면 위에 나열된 포트 외에는 접속할 수 없습니다. WorkSpaces 마지막으로 고려할 사항은 기본적으로 새 보안 그룹에는 인바운드 규칙이 없다는 것입니다. 따라서 보안 그룹에 인바운드 규칙을 추가하기 전에는 또 다른 호스트에서 시작하여 인스턴스로 가는 인바운드 트래

픽이 허용되지 않습니다. 위 단계는 에서 나가는 것을 제한하거나 액세스 권한이 있어야 하는 리소스 WorkSpaces 또는 CIDR 범위로만 수신 규칙을 잠그려는 경우에만 필요합니다.

> **Note**
>
> 새로 연결된 보안 그룹은 수정 후 WorkSpaces 생성되거나 재구축되는 그룹에만 연결됩니다.

ENI 보안 그룹

기본 네트워크 인터페이스는 일반 ENI이므로 다양한 AWS 관리 도구를 사용하여 관리할 수 있습니다. 자세한 내용은 엘라스틱 네트워크 인터페이스를 참조하십시오. Amazon WorkSpaces 콘솔 WorkSpaces 페이지에서 WorkSpace IP 주소로 이동한 다음, 해당 IP 주소를 필터로 사용하여 (Amazon EC2 콘솔의 네트워크 인터페이스 섹션에서) 해당 ENI를 찾습니다.

ENI를 찾으면 보안 그룹에서 직접 관리할 수 있습니다. 기본 네트워크 인터페이스에 보안 그룹을 수동으로 할당할 때는 WorkSpaces Amazon의 포트 요구 사항을 고려하십시오. 자세한 내용은 Amazon Workspaces 관리 안내서의 네트워크 인터페이스를 참조하십시오.

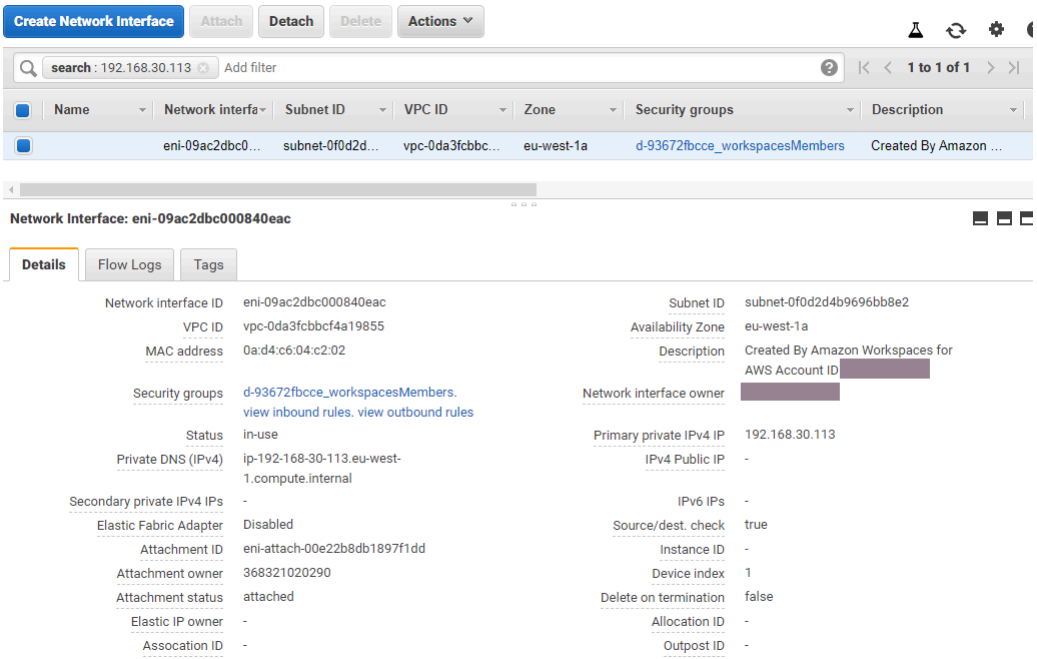

그림 21: WorkSpaces MFA가 활성화된 클라이언트

네트워크 액세스 제어 목록(ACL)

또 다른 방화벽 관리가 복잡해짐에 따라 네트워크 ACL은 매우 복잡한 배포에 일반적으로 사용되며 일반적으로 모범 사례로 사용되지는 않습니다. 네트워크 ACL은 VPC의 서브넷에 연결되므로 OSI 모델의 계층 3 (네트워크) 에 기능이 집중됩니다. Amazon은 디렉터리 서비스를 기반으로 WorkSpaces 설계되었으므로 두 개의 서브넷을 정의해야 합니다. 네트워크 ACL은 디렉터리 서비스와는 별도로 관리되며, 네트워크 ACL은 WorkSpaces '할당된 서브넷 중 하나에만 할당될 수 있을 가능성이 큽니다.

상태 비저장 방화벽이 필요한 경우 네트워크 ACL은 보안을 위한 모범 사례입니다. 네트워크 ACL에서 기본 설정을 초과하여 변경한 모든 내용은 서브넷별로 유효성을 검사하는 것이 가장 좋습니다. 네트워크 ACL이 의도한 대로 작동하지 않는 경우 VPC 흐름 로그를 사용하여 트래픽을 분석해 보십시오.

AWS 네트워크 방화벽

AWS Network Firewall은 기본 보안 그룹 및 네트워크 ACL이 제공하는 것 이상의 기능을 제공하지만 비용이 듭니다. HTTPS 기반 웹 사이트를 위한 서버 이름 검사 (SNI), 침입 탐지 및 방지, 도메인 이름에 대한 허용 및 거부 목록 등 네트워크 연결과 관련된 보안을 강화할 수 있는 기능을 요구하는 고객들은 이에 대한 대체 방화벽을 찾아야 했습니다. AWS Marketplace 이러한 방화벽의 배포가 복잡하기 때문에 표준 EUC 관리자의 숙련도를 넘어서는 문제가 발생했습니다. AWS Network Firewall은 레이어 3에서 7까지의 보호를 지원하는 동시에 기본 AWS 환경을 제공합니다. 조직에 EUC AWS 네트워크 보호를 모두 적용할 수 있는 다른 수단 (클라우드로 전송할 수 있는 타사 방화벽에 대한 기존 온프레미스 라이선스 또는 방화벽을 관리하는 별도의 팀 제외) 이 없는 경우 Network Firewall을 NAT Gateway와 함께 사용하는 것이 좋습니다. NAT 게이트웨이는 AWS 네트워크 방화벽과 함께 무료로 제공됩니다.

AWS Network Firewall 배포는 기존 EUC 설계를 중심으로 설계되었습니다. 단일 VPC 설계에서는 방화벽 엔드포인트용 서브넷과 별도의 인터넷 송신 라우팅 고려 사항을 포함하는 간소화된 아키텍처를 구현할 수 있는 반면, 다중 VPC 설계는 방화벽 및 Transit Gateway 엔드포인트가 있는 통합 검사 VPC의 이점을 크게 누릴 수 있습니다.

설계 시나리오

시나리오 1: 기본 인스턴스 잠금

기본 WorkSpaces 보안 그룹은 인바운드 트래픽을 허용하지 않습니다. 보안 그룹은 기본적으로 거부되고 스테이트풀이기 때문입니다. 즉, WorkSpaces 인스턴스 자체의 보안을 강화하기 위해 추가로 구성해야 할 구성이 없습니다. 모든 트래픽을 허용하는 아웃바운드 규칙과 사용 사례에 적합한지 고려해 보세요. 예를 들어 LDAP의 경우 389, LDAP의 경우 636, SMB의 경우 445 등과 같이 포트 사용 사례에

맞는 특정 IP 범위 및 모든 주소로 포트 443으로 향하는 모든 아웃바운드 트래픽을 거부하는 것이 가장 좋습니다. 하지만 환경의 복잡성으로 인해 여러 규칙이 필요하므로 네트워크 ACL 또는 방화벽 어플라이언스를 통해 더 잘 서비스될 수 있습니다.

시나리오 2: 인바운드 예외

일정한 요구 사항은 아니지만 네트워크 트래픽이 인바운드로 시작되는 경우가 있을 수 있습니다. WorkSpaces 예를 들어 WorkSpaces 클라이언트가 연결할 수 없는 경우 인스턴스를 분류하려면 대체 원격 연결이 필요합니다. 이러한 경우에는 고객 ENI의 보안 그룹에 인바운드 TCP 3389를 일시적으로 활성화하는 것이 가장 좋습니다. WorkSpace

또 다른 시나리오는 중앙 집중식 인스턴스에서 시작되는 인벤토리 또는 자동화 기능을 위한 명령을 수행하는 조직 스크립트입니다. 인바운드의 특정 중앙 집중식 인스턴스로부터 해당 포트의 트래픽을 보호하는 것은 영구적으로 구성할 수 있지만 계정 내 여러 배포에 적용할 수 있으므로 디렉터리 구성에 연결된 추가 보안 그룹에서 이 작업을 수행하는 것이 가장 좋습니다. AWS

마지막으로, 일부 네트워크 트래픽은 상태 저장 기반이 아니므로 인바운드 예외에 임시 포트를 지정해야 합니다. 쿼리와 스크립트가 실패하는 경우 연결 실패의 근본 원인을 파악하면서 최소한 일시적으로 임시 포트를 허용하는 것이 좋습니다.

시나리오 3: 단일 VPC 검사

단순화된 배포 WorkSpaces (예: 확장 계획이 없는 단일 VPC) 에는 검사를 위해 별도의 VPC가 필요하지 않으므로 VPC 피어링을 통해 다른 VPC와의 연결을 단순화할 수 있습니다. 그러나 해당 엔드포인트에 대한 라우팅과 IGW (Internet Gateway) 이그레스 라우팅을 구성하여 방화벽 엔드포인트에 대해 별도의 서브넷을 생성해야 합니다. 그렇지 않으면 구성하지 않아도 됩니다. 모든 서브넷이 VPC CIDR 블록 전체를 사용하는 경우 기존 배포에 사용 가능한 IP 공간이 없을 수 있습니다. 이러한 경우에는 배포가 이미 초기 설계 이상으로 확장되었으므로 시나리오 4가 더 유용할 수 있습니다.

시나리오 4: 중앙 집중식 검사

AWS 네트워크 방화벽의 스테이트풀 및 스테이트리스 규칙의 관리를 단순화하므로 한 AWS 지역에 여러 EUC를 배포할 때 선호되는 경우가 많습니다. 기존 VPC 피어는 Transit Gateway로 대체됩니다. 이 설계에서는 Transit Gateway 첨부 파일과 해당 첨부 파일을 통해서만 구성할 수 있는 검사 라우팅을 사용해야 하기 때문입니다. 이 구성에도 더 높은 수준의 제어가 적용되므로 기본 환경을 넘어서는 보안이 가능합니다. WorkSpaces

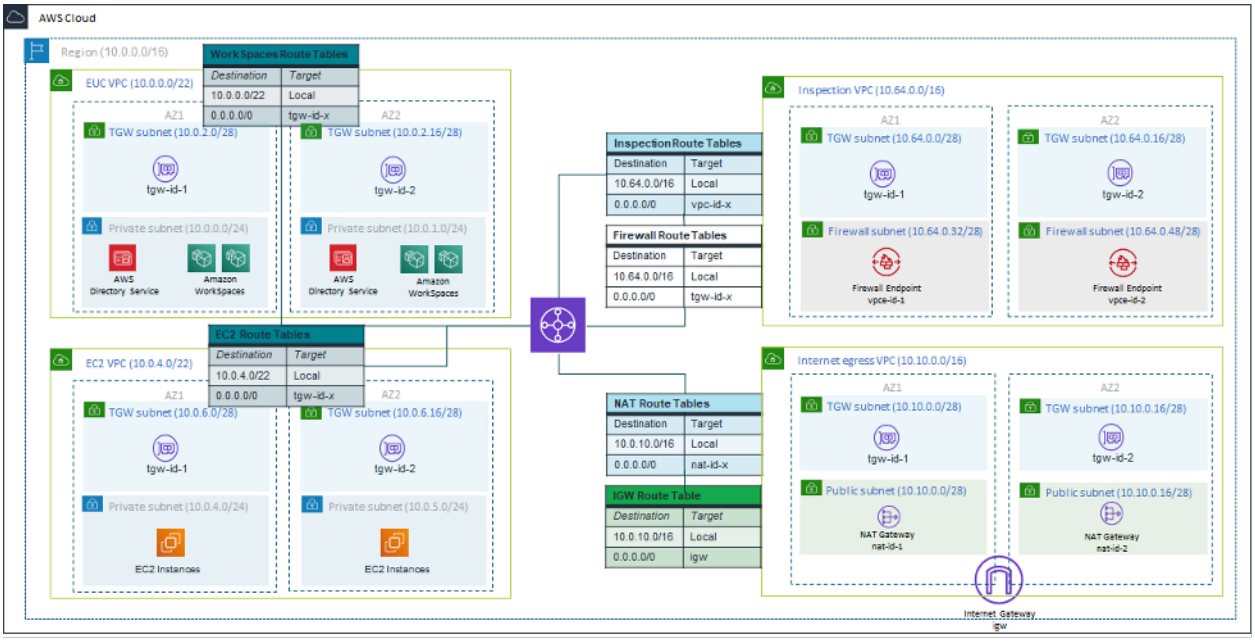

그림 22: Transit Gateway 첨부 파일을 사용하는 샘플 아키텍처

암호화됨 WorkSpaces

각 WorkSpace Amazon에는 루트 볼륨 (Windows의 경우 C: 드라이브 WorkSpaces, Amazon Linux의 경우 루트 WorkSpaces) 및 사용자 볼륨 (Windows의 경우 D: 드라이브 WorkSpaces, Amazon Linux의 경우 /home) 이 제공됩니다. WorkSpaces 암호화된 WorkSpaces 기능을 사용하면 볼륨 하나 또는 둘 모두를 암호화할 수 있습니다.

무엇을 암호화하나요?

저장된 데이터, 볼륨에 대한 디스크 입력/출력 (I/O), 암호화된 볼륨에서 생성된 스냅샷은 모두 암호화됩니다.

암호화는 언제 이루어지나요?

시작 (생성) 시 a에 대한 암호화를 WorkSpace 지정해야 WorkSpace 합니다. WorkSpaces 볼륨은 시작 시에만 암호화할 수 있습니다. 실행 후에는 볼륨 암호화 상태를 변경할 수 없습니다. 다음 그림은 새 버전을 출시할 때 암호화를 선택할 수 있는 Amazon WorkSpaces 콘솔 페이지를 보여줍니다 WorkSpace.

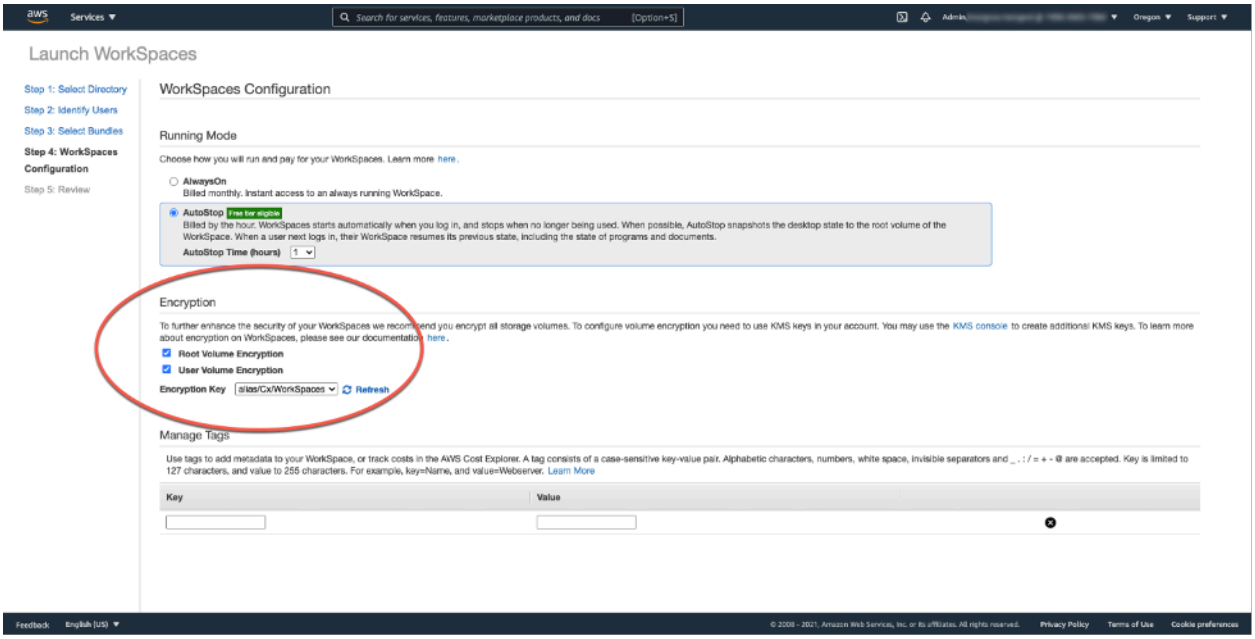

그림 23: 루트 볼륨 암호화 WorkSpace

새 WorkSpace 암호화는 어떻게 이루어지나요?

고객은 Amazon WorkSpaces 콘솔에서 또는 AWS CLI 고객이 새 앱을 시작할 때 Amazon WorkSpaces API를 사용하여 암호화 WorkSpaces 옵션을 선택할 수 WorkSpace 있습니다.

Amazon은 볼륨을 암호화하기 위해 CMK from AWS Key Management Service () AWS KMS 을 WorkSpaces 사용합니다. 기본 AWS KMS CMK는 지역에서 처음 실행될 WorkSpace 때 생성됩니다. (CMK에는 지역 범위가 있습니다.)

고객은 암호화된 상태로 사용할 고객 관리형 CMK를 만들 수도 있습니다. WorkSpaces CMK는 Amazon WorkSpaces 서비스가 각 볼륨을 암호화하는 데 사용하는 데이터 키를 암호화하는 데 사용됩니다. WorkSpace (엄밀히 말하면 볼륨을 암호화하는 것은 Amazon EBS입니다.) 현재 CMK 한도는 리소스 할당량을 참조하십시오. AWS KMS

> **Note**
>
> 암호화된 이미지에서 사용자 지정 이미지를 생성하는 WorkSpace 것은 지원되지 않습니다. 또한 루트 볼륨 암호화가 활성화된 상태에서 WorkSpaces 시작한 경우 프로비저닝하는 데 최대 1시간이 걸릴 수 있습니다.

WorkSpaces 암호화 프로세스에 대한 자세한 설명은 Amazon의 WorkSpaces 사용 방법을 참조하십시오 AWS KMS. WorkSpace 암호화에 대한 요청이 올바르게 처리되도록 CMK 사용을 모니터링하는 방법을 고려해 보십시오. AWS KMS 키 및 데이터 키에 대한 추가 정보는 페이지를 참조하십시오. AWS KMS

액세스 제어 옵션 및 신뢰할 수 있는 장치

WorkSpaces Amazon은 액세스할 수 있는 클라이언트 디바이스를 관리할 수 있는 옵션을 고객에게 제공합니다 WorkSpaces. 고객은 신뢰할 수 있는 디바이스에만 WorkSpaces 액세스를 제한할 수 있습니다. macOS 및 Microsoft Windows PC에서 디지털 인증서를 사용하여 액세스를 WorkSpaces 허용할 수 있습니다. 또한 iOS, 안드로이드, 크롬 OS, 리눅스, 제로 클라이언트 및 WorkSpaces 웹 액세스 클라이언트에 대한 액세스를 허용하거나 차단할 수 있습니다. 이러한 기능을 통해 보안 태세를 더욱 개선할 수 있습니다.

새로운 배포에서는 사용자가 Windows, macOS, iOS, Android, ChromeOS 및 Zero Client의 WorkSpaces 클라이언트에서 액세스할 수 있도록 액세스 제어 옵션을 사용할 수 있습니다. 웹 액세스 또는 Linux WorkSpaces 클라이언트를 사용한 액세스는 새 WorkSpaces 배포에서 기본적으로 활성화되지 않으므로 활성화해야 합니다.

신뢰할 수 있는 장치 (관리 대상 장치라고도 함) 에서 회사 데이터에 액세스하는 데 제한이 있는 경우 유효한 인증서가 있는 신뢰할 수 있는 장치로만 WorkSpaces 액세스를 제한할 수 있습니다. 이 기능을 활성화하면 Amazon은 인증서 기반 인증을 WorkSpaces 사용하여 디바이스를 신뢰할 수 있는지 확인합니다. WorkSpaces 클라이언트 애플리케이션이 디바이스를 신뢰할 수 있는지 확인할 수 없는 경우 디바이스에서 로그인하거나 다시 연결하려는 시도를 차단합니다.

신뢰할 수 있는 장치 지원은 다음 클라이언트에 제공됩니다.

- WorkSpaces 안드로이드 및 안드로이드 호환 크롬 OS 기기에서 실행되는 구글 플레이의 Amazon Android 클라이언트 앱
- WorkSpaces macOS 디바이스에서 실행되는 Amazon macOS 클라이언트 앱
- WorkSpaces 윈도우 디바이스에서 실행되는 Amazon Windows 클라이언트 앱

액세스할 WorkSpaces 수 있는 디바이스를 제어하는 방법에 대한 자세한 내용은 신뢰할 수 있는 디바이스에 WorkSpaces 대한 액세스 제한을 참조하십시오.

> **Note**
>
> 신뢰할 수 있는 디바이스의 인증서는 Amazon WorkSpaces 윈도우, macOS 및 Android 클라이언트에만 적용됩니다. 이 기능은 Amazon WorkSpaces Web Access 클라이언트 또는 Teradici PCoIP 소프트웨어 및 모바일 클라이언트, Teradici PCoIP 제로 클라이언트, RDP 클라이언트 및 원격 데스크톱 애플리케이션을 포함하되 이에 국한되지 않는 타사 클라이언트에는 적용되지 않습니다.

IP 액세스 제어 그룹

고객은 IP 주소 기반 제어 그룹을 사용하여 신뢰할 수 있는 IP 주소 그룹을 정의 및 관리하고, 사용자가 신뢰할 수 있는 네트워크에 연결된 WorkSpaces 경우에만 해당 그룹에 액세스하도록 허용할 수 있습니다. 이 기능을 통해 고객은 보안 상태를 보다 효과적으로 제어할 수 있습니다.

WorkSpaces 디렉토리 수준에서 IP 접근제어 그룹을 추가할 수 있습니다. 두 가지 방법으로 IP 접근제어 그룹을 사용할 수 있습니다.

- IP 접근제어 페이지 — WorkSpaces 관리 콘솔에서 IP 접근제어 페이지에 IP 접근제어 그룹을 생성할 수 있습니다. 액세스할 수 있는 IP 주소 또는 IP 범위를 입력하여 이러한 그룹에 규칙을 추가할 WorkSpaces 수 있습니다. 그런 다음 업데이트 세부 정보 페이지의 디렉터리에 이러한 그룹을 추가할 수 있습니다.
- Workspace WorkSpaces API — API를 사용하여 그룹을 생성, 삭제 및 확인하고, 액세스 규칙을 생성 또는 삭제하거나, 디렉터리에 그룹을 추가 및 제거할 수 있습니다.

Amazon WorkSpaces 암호화 프로세스에서 IP 액세스 제어 그룹을 사용하는 방법에 대한 자세한 설명은 사용자를 위한 IP 액세스 제어 그룹을 참조하십시오 WorkSpaces.

Amazon을 사용한 모니터링 또는 로깅 CloudWatch

네트워크, 서버 및 로그 모니터링은 모든 인프라의 필수적인 부분입니다. Amazon을 배포하는 고객은 배포, 특히 개인의 전반적인 상태 및 연결 상태를 WorkSpaces 모니터링해야 합니다. WorkSpaces

에 대한 아마존 CloudWatch 메트릭스 WorkSpaces

CloudWatch 에 대한 WorkSpaces 지표는 관리자에게 개인의 전반적인 상태 및 연결 상태에 대한 추가 통찰력을 제공하도록 설계되었습니다 WorkSpaces. 지표는 지정된 디렉터리 내의 조직 내에서 사용할 수 있거나 전체 WorkSpaces 조직에 대해 집계하여 사용할 수 있습니다. WorkSpace

모든 지표와 마찬가지로 이러한 CloudWatch CloudWatch 지표는 AWS Management Console (다음 그림 참조) 에서 보고, API를 통해 액세스하고, CloudWatch 경보 및 타사 도구를 통해 모니터링할 수 있습니다.

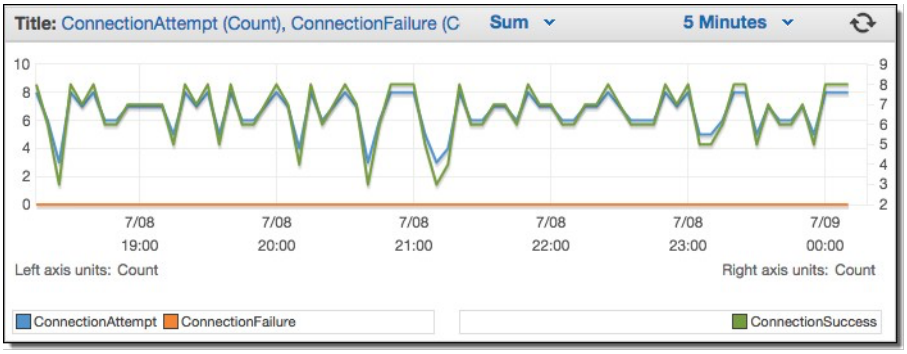

그림 24: CloudWatch 지표: ConnectionAttempt / ConnectionFailure

기본적으로 다음 지표가 활성화되며 추가 비용 없이 사용할 수 있습니다.

- 사용 가능 - WorkSpaces 상태 확인에 대한 응답이 이 지표에 포함됩니다.
- 비정상 상태 — 동일한 상태 확인에 응답하지 WorkSpaces 않는 비정상은 이 지표에 포함됩니다.
- ConnectionAttempt— a에 대한 연결 시도 횟수. WorkSpace
- ConnectionSuccess— 성공한 연결 시도 횟수.
- ConnectionFailure— 실패한 연결 시도 횟수.
- SessionLaunchTime— 세션을 시작하는 데 걸린 시간 (클라이언트가 측정한 시간). WorkSpaces
- InSessionLatency— 클라이언트가 측정 및 WorkSpaces 보고한 WorkSpaces 클라이언트와 클라이언트 간의 왕복 소요 시간.
- SessionDisconnect— 사용자가 시작한 세션과 자동으로 종료된 세션 수.

또한 다음 그림과 같이 경보를 생성할 수 있습니다.

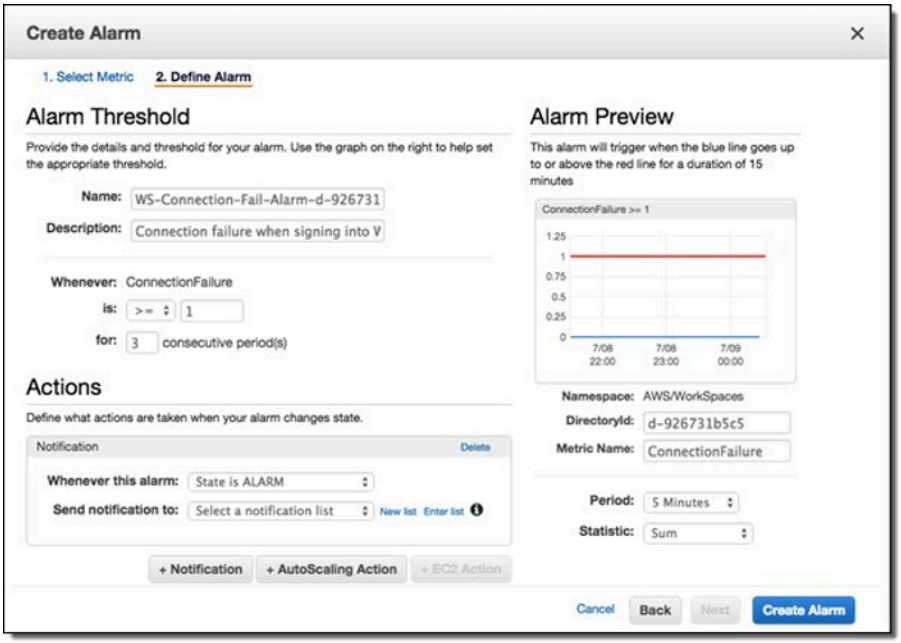

그림 25: WorkSpaces 연결 오류에 대한 CloudWatch 알람 생성

아마존 CloudWatch 이벤트 대상 WorkSpaces

Amazon CloudWatch Events의 이벤트는 보고, 검색하고, 다운로드하고, 보관하고, 분석하고, 로그인에 성공하면 응답하는 데 사용할 수 있습니다. WorkSpaces 이 서비스는 사용자 로그인에 대한 클라이언트 WAN IP 주소, 운영 체제, WorkSpaces ID 및 디렉터리 ID 정보를 모니터링할 수 있습니다. WorkSpaces 예를 들어 다음과 같은 목적으로 이벤트를 사용할 수 있습니다.

- 나중에 참조할 수 있도록 WorkSpaces 로그인 이벤트를 로그로 저장하거나 보관하고, 로그를 분석하여 패턴을 찾고, 해당 패턴을 기반으로 조치를 취하십시오.
- WAN IP 주소를 사용하여 사용자가 로그인하는 위치를 확인한 다음 정책을 사용하여 액세스 CloudWatch 이벤트 유형에 있는 액세스 기준에 맞는 파일 또는 WorkSpaces 데이터에만 사용자가 WorkSpaces 액세스하도록 허용하십시오.
- 정책 제어를 사용하여 권한이 없는 IP 주소에서 파일 및 애플리케이션에 대한 액세스를 차단합니다.

CloudWatch 이벤트 사용 방법에 대한 자세한 내용은 Amazon CloudWatch Events 사용 설명서를 참조하십시오. CloudWatch 이벤트에 대한 WorkSpaces 자세한 내용은 Cloudwatch 이벤트 WorkSpaces 사용 모니터링을 참조하십시오.

YubiKey 아마존 지원 WorkSpaces

추가 보안 계층을 추가하기 위해 고객은 다단계 인증으로 도구와 사이트를 보호하기로 선택하는 경우가 많습니다. 일부 고객은 YubiKey Yubico를 사용하여 이 작업을 수행하기로 선택합니다. WorkSpaces Amazon은 일회용 암호 (OTP) 와 FIDO U2F 인증 프로토콜을 모두 지원합니다. YubiKeys

Amazon은 WorkSpaces 현재 OTP 모드를 지원하며, 관리자나 최종 사용자가 OTP를 사용하기 위해 추가 단계를 거쳐야 할 필요는 없습니다. YubiKey 사용자는 이를 컴퓨터에 연결하고 키보드가 해당 영역 WorkSpace (특히 OTP를 입력해야 YubiKey 하는 필드) 에 초점을 맞췄는지 확인한 다음, 키보드의 금색 접점을 터치할 수 있습니다. YubiKey YubiKey 그러면 선택한 필드에 OTP가 자동으로 입력됩니다.

YubiKey 및 와 함께 FIDO U2F 모드를 WorkSpaces 활용하려면 추가 단계가 필요합니다. U2F 리디렉션을 활용하려면 다음과 같은 지원 YubiKey 모델 중 하나를 사용자에게 발급해야 합니다. WorkSpaces

- YubiKey 4
- YubiKey 5 NFC
- YubiKey 5 나노
- YubiKey 5C
- YubiKey 5C 나노
- YubiKey 5 NFC

U2F용 USB 리디렉션을 활성화하려면 YubiKey

기본적으로 PCoIP에는 USB 리디렉션이 비활성화되어 있습니다 WorkSpaces. U2F 모드를 사용하려면 이를 사용하도록 설정해야 합니다. YubiKeys

1. PCoIP (32비트) 용 최신 WorkSpaces 그룹 정책 관리 템플릿 또는 PCoIP (64비트) 용 WorkSpaces 그룹 정책 관리 템플릿을 설치했는지 확인하십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 (gpmc.msc) 를 열고 PCoIP 세션 변수로 이동합니다. WorkSpaces
3. 사용자가 설정을 재정의하도록 허용하려면 재정의 가능한 관리자 기본값을 선택합니다. 그렇지 않으면 [재정의할 수 없는 관리자 기본값] 을 선택합니다.
4. PCoIP 세션에서 USB 활성화/비활성화 설정을 엽니다.
5. 활성화됨을 선택한 다음 확인을 선택합니다.

6. PCoIP USB 허용되는 디바이스 규칙 및 허용되지 않는 디바이스 규칙 구성 설정을 엽니다.
7. 활성화됨을 선택하고 USB 권한 부여 테이블 입력(규칙 최대 10개)에서 USB 디바이스 허용 목록 규칙을 구성합니다.
   a. 권한 부여 규칙 - 110500407. 이 값은 제공업체 ID(VID)와 제품 ID(PID)의 조합입니다. VID/PID 조합의 형식은 다음과 같습니다. 여기서 는 1xxxxyyyy 16진수 형식의 xxxx VID이고 는 16진수 형식의 PID입니다. yyyy 이 예시에서 1050은 VID이고 0407은 PID입니다. USB 값에 대한 자세한 내용은 USB ID 값을 참조하십시오. YubiKey YubiKey
8. USB 인증 테이블 입력 (최대 10개 규칙) 에서 USB 장치 차단 목록 규칙을 구성합니다.
   a. 권한 미부여 규칙의 경우 빈 문자열을 설정합니다. 인증 목록에 있는 USB 디바이스만 허용한다는 뜻입니다.

> **Note**
>
> 최대 10개의 USB 권한 부여 규칙과 최대 10개의 USB 권한 미부여 규칙을 정의할 수 있습니다. 세로 막대(|) 문자를 사용하여 여러 규칙을 구분합니다. 권한 부여/권한 부여 규칙에 대한 자세한 내용은 Windows용 Teradici PCoIP 표준 에이전트를 참조하십시오.

9. 확인을 선택합니다.
10. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 이후 및 세션이 다시 시작된 후에 적용됩니다. WorkSpace WorkSpace 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
    a. 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    b. 관리 명령 프롬프트에서 gpupdate /force를 입력합니다.
11. 설정이 적용된 후에는 USB 디바이스 규칙 설정을 통해 제한을 WorkSpaces 구성하지 않는 한 지원되는 모든 USB 디바이스를 리디렉션할 수 있습니다.

U2F용 USB 리디렉션을 활성화한 후에는 Fido의 YubiKey U2F 모드를 사용할 수 YubiKey 있습니다.

비용 최적화

셀프서비스 관리 기능 WorkSpace

WorkSpacesAmazon에서는 셀프 서비스 WorkSpace 관리 기능을 사용하여 사용자가 경험을 더 잘 제어할 수 있도록 할 수 있습니다. 사용자에게 셀프 서비스 기능을 허용하면 WorkSpaces Amazon의 IT 지원 직원 업무량을 줄일 수 있습니다. 셀프 서비스 기능이 활성화되면 사용자는 Amazon용 Windows, macOS 또는 Linux 클라이언트에서 다음 작업 중 하나 이상을 직접 수행할 수 있습니다. WorkSpaces

- 클라이언트에서 자격 증명을 캐시합니다. 이를 통해 사용자는 자격 증명을 다시 WorkSpace 입력하지 않고도 서버에 다시 연결할 수 있습니다.
- 다시 시작하세요. WorkSpace
- 의 루트 및 사용자 볼륨 크기를 늘리십시오 WorkSpace.
- 해당 컴퓨팅 유형 (번들) 을 변경합니다 WorkSpace.
- 그들의 실행 모드를 WorkSpace 전환하십시오.
- 다시 빌드하세요. WorkSpace

사용자에게 재시작 및 재구축 옵션을 허용하는 것은 비용에 지속적으로 영향을 미치지 않습니다. WorkSpaces 사용자는 재구축 프로세스가 진행되는 동안 장치를 다시 WorkSpace 빌드하면 최대 한 시간 동안 사용할 수 없게 된다는 점에 유의해야 합니다. WorkSpace

볼륨 크기를 늘리고, 컴퓨팅 유형을 변경하고, 실행 모드를 전환하는 옵션을 사용하면 추가 비용이 발생할 수 있습니다. WorkSpaces 가장 좋은 방법은 셀프 서비스를 활성화하여 지원 팀의 업무량을 줄이는 것입니다. 추가 비용 항목에 대한 셀프 서비스는 추가 요금에 대한 승인을 받았는지 확인하는 워크플로우 프로세스 내에서 허용되어야 합니다. 이는 전용 셀프 서비스 포털을 통하거나 WorkSpaces, 다음과 같은 기존 정보 기술 서비스 관리 (ITSM) 서비스와 통합하여 수행할 수 있습니다. ServiceNow

자세한 내용은 사용자를 위한 셀프 서비스 WorkSpace 관리 기능 활성화를 참조하십시오. 사용자 셀프 서비스를 위해 구조화된 포털을 활성화하는 방법을 설명하는 예는 셀프 서비스 포털을 WorkSpaces 통한 Amazon 자동화를 참조하십시오.

아마존 WorkSpaces 코스트 옵티마이저

Amazon WorkSpaces 비용 최적화 솔루션은 모든 Amazon WorkSpaces 사용 데이터를 분석합니다. 사용량에 따라 가장 비용 효율적인 결제 옵션 (시간당 또는 월간) WorkSpace 으로 자동 전환됩니다.

이 솔루션을 사용하면 WorkSpace 사용량을 모니터링하고 비용을 최적화할 수 있으며, 24시간마다 사용량을 분석하고 개별적으로 WorkSpaces 전환하는 AWS CloudFormation 데 필요한 AWS 서비스를 자동으로 프로비저닝 및 구성할 수 있습니다. 최신 버전인 2.4는 고객에게 기존 VPC에 솔루션을 배포하고 지역 및 종료에 맞게 선택적으로 구성할 수 있는 유연성을 제공합니다. 또한 청구 시간 계산의 정확성이 향상되고 보고 메타데이터가 향상되었습니다. WorkSpaces 이전에 이 솔루션의 이전 버전 (v2.2.1 이하) 을 배포한 경우, 업데이트 스택 설명서에 따라 Amazon WorkSpaces Cost Optimizer CloudFormation 스택을 업데이트하여 솔루션 프레임워크의 최신 버전을 가져오십시오.

a의 실행 모드에 따라 즉각적인 가용성과 WorkSpace 청구 여부가 결정됩니다. 현재 실행 중인 WorkSpaces 실행 모드는 다음과 같습니다.

AlwaysOn— 무제한 사용에 대해 월 고정 요금을 지불할 때 사용합니다 WorkSpaces. 이 모드는 자신의 데스크톱을 기본 WorkSpace 데스크톱으로 사용하고 항상 실행 중인 WorkSpace 시스템에 즉시 액세스해야 하는 사용자에게 적합합니다.

AutoStop— 시간당 요금을 WorkSpaces 지불할 때 사용합니다. 이 모드를 사용하면 지정된 시간 동안 사용하지 않으면 WorkSpaces 중지하고 앱 및 데이터 상태가 저장됩니다. 자동 중지 시간을 설정하려면 시간 (AutoStop 시간) 을 사용합니다. 이 모드는 시간제 액세스만 필요한 사용자에게 적합합니다. WorkSpaces

가장 좋은 방법은 Amazon WorkSpaces Cost Optimizer와 같은 솔루션을 사용하여 사용량을 모니터링하고 Amazon의 실행 모드를 가장 WorkSpaces 비용 효율적인 모드로 설정하는 것입니다. 이 솔루션은 24시간마다 AWS Lambda함수를 호출하는 Amazon CloudWatch 이벤트 규칙을 배포합니다.

이 솔루션은 임계값에 도달한 후 언제든지 개인을 WorkSpaces 시간당 청구 모델에서 월별 청구 모델로 전환할 수 있습니다. 솔루션이 시간당 청구를 월별 청구로 전환하는 경우 솔루션은 사용량이 임계값 미만인 경우에만 다음 달이 시작될 때까지 WorkSpace 다시 시간당 청구로 전환하지 않습니다. WorkSpace 하지만 청구 모델은 AWS Management Console 또는 Amazon WorkSpaces API를 사용하여 언제든지 수동으로 변경할 수 있습니다. 솔루션 AWS CloudFormation 템플릿에는 이러한 전환을 실행하는 파라미터가 포함되어 있으며, 솔루션을 테스트 실행 모드에서 실행하여 권장 사항에 대한 보고서를 제공할 수 있습니다.

태그를 사용하여 옵트아웃하기

솔루션이 결제 모델 WorkSpace 간에 전환되지 않도록 하려면 Skip_Convert라는 태그 키와 태그 값을 WorkSpace 사용하는 사용자에게 리소스 태그를 적용하세요. 이 솔루션은 태그가 지정된 것을 로그에 WorkSpaces 기록하지만 태그가 지정된 것을 변환하지는 않습니다. WorkSpaces 해당 태그에 대한 자동 변환을 재개하려면 언제든지 태그를 제거하세요. WorkSpace 자세한 내용은 Amazon WorkSpaces 비용 최적화 도구를 참조하십시오.

지역 선택

기본적으로 이 솔루션은 동일한 WorkSpaces AWS 계정에서 WorkSpaces Amazon에 등록된 디렉터리를 스캔하여 사용 가능한 모든 AWS 지역에서 모니터링합니다. 지역 목록 입력 파라미터에 모니터링할 AWS 지역을 쉼표로 구분하여 제공하여 모니터링할 AWS 지역을 제한할 수 있습니다.

기존 VPC에 배포

이 솔루션에는 ECS 작업을 실행할 VPC가 필요합니다. 기본적으로 솔루션은 새 VPC를 생성하지만 입력 파라미터의 일부로 서브넷 ID 및 보안 그룹 ID를 제공하여 기존 VPC에 배포할 수 있습니다. 현재 서브넷에는 ECS 작업이 퍼블릭 Amazon ECR 리포지토리에 호스팅된 Docker 이미지를 가져올 수 있도록 인터넷으로 연결되는 경로가 있습니다.

미사용 종료 WorkSpaces

이 솔루션을 사용하면 모든 기준이 충족되는 달의 마지막 WorkSpaces 날에 미사용을 종료할 수 있습니다. TerminateUnusedWorkSpaces입력 매개변수를 CloudFormation 템플릿으로 변경하여 이 기능을 옵트인할 수 있습니다. 가장 좋은 방법은 이 기능을 몇 달 동안 드라이런 모드에서 실행하고 월별 보고서를 확인하여 종료 WorkSpaces 표시가 있는지 검토하는 것입니다.

아마존을 위한 아마존 커넥트 최적화 WorkSpaces

콜센터 상담원의 오디오 품질이 저하되면 상담원이 서비스를 받는 고객에게 좋지 않은 통화 경험을 제공하기 때문에 상담원의 최종 사용자 경험을 최우선 과제로 삼아야 합니다. 원격 데스크톱에서 컨택 센터 솔루션을 실행할 때 음성 트래픽이 네트워크 연결보다 우선시되지 않으면 오디오 성능에 어느 정도 영향을 미칠 수 있습니다. 이러한 영향은 오디오가 오디오 엔드포인트에서 가상 세션으로 흐른 다음 스트리밍 프로토콜을 통해 압축되어 최종 사용자에게 전달되기 때문입니다. 이러한 추가 라우팅으로 인해 네트워크 병목 현상으로 인해 오디오 성능이 저하될 수 있습니다.

이러한 동작을 방지하는 방법은 오디오를 세션 밖으로 분리하는 것입니다. 즉, 오디오 스트림은 세션 밖에 있는 동안 컨택 센터 상담원의 모든 리소스는 세션 내에 남아 있게 됩니다. 이렇게 분할하면 오디오가 오디오 엔드포인트에서 최종 사용자에게 직접 스트리밍되는 동시에 상담원이 보고 있는 PII를 비롯한 다른 모든 통화 리소스는 보안 세션을 유지할 수 있습니다. 이 오디오 최적화는 고객의 통화 경험을 최대한 좋게 만들기 때문에 모범 사례로 간주됩니다.

Amazon Connect는 관리자가 비즈니스 요구 사항에 맞게 CCP (연락처 제어판) 를 사용자 지정할 수 있는 스트림 API를 제공합니다. 관리자가 사용할 수 있는 옵션 중 하나는 사용자 지정 CCP가 통화에 대한 오디오를 수신할 수 있는지 여부를 제어하는 것입니다. 이러한 설정을 통해 분할 CCP를 구성할 수 있습니다. 즉, 세션 외 사용을 위한 오디오 전용 CCP, 세션 중일 때는 미디어 없는 CCP를 구성할 수 있습니다. 관리자가 이러한 사용자 지정 CCP를 구성하고 나면 Amazon Connect 오디오 최적화를 활용할 수 있습니다. WorkSpaces CCP는 브라우저 내에서 전달되므로 관리자는 이 설정을 통해 오디오 전용 CCP URL을 디렉터리에 제공할 수 있습니다. WorkSpaces 구성이 완료되면 WorkSpaces Connect 컨택 센터 상담원이 해당 WorkSpaces 상담원에게 성공적으로 인증되면 WorkSpaces 클라이언트는 상담원의 로컬 기본 브라우저에서 제공된 오디오 전용 CCP URL을 자동으로 엽니다. 이렇게 하면 미디어가 없는 CCP가 보안 세션 내에서 다른 모든 작업을 처리하는 동안 오디오가 상담원의 로컬 컴퓨터로 직접 전달됩니다. WorkSpaces

아키텍처 다이어그램

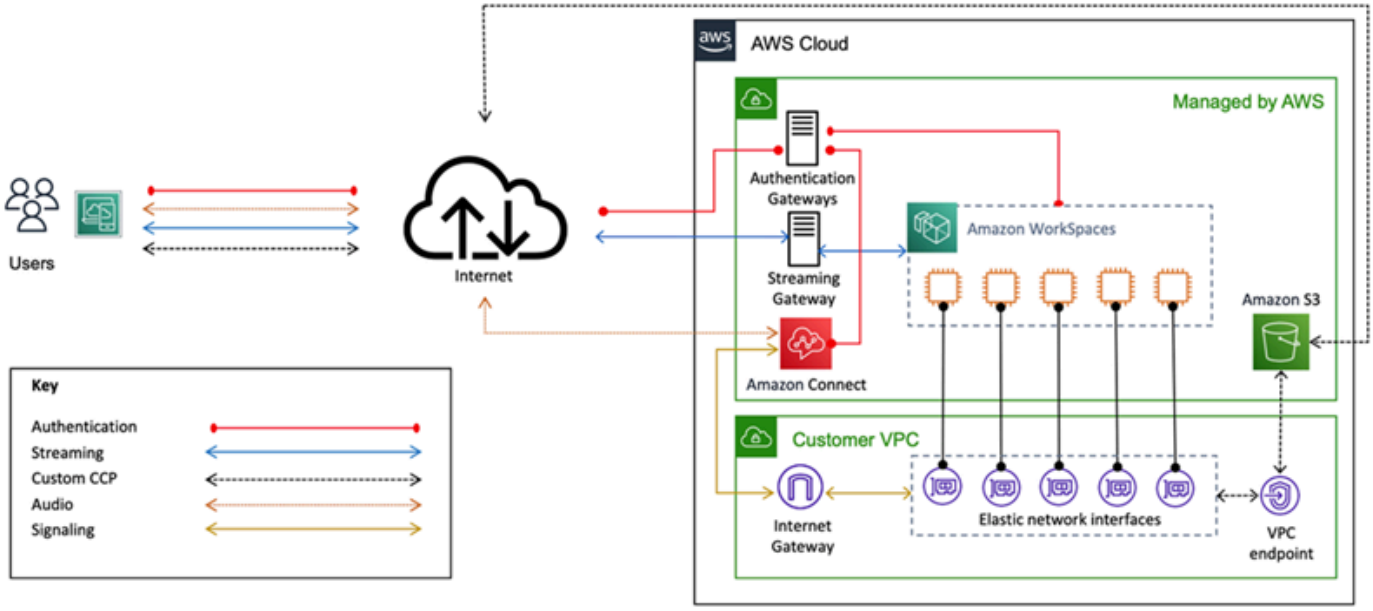

그림 26 — 아마존 커넥트 및 WorkSpaces 아키텍처 다이어그램

문제 해결

디바이스가 WorkSpaces 등록 서비스에 연결할 수 없거나 대화형 로그온 배너를 통해 연결할 수 없음과 같은 오류 메시지와 같은 일반적인 관리 및 클라이언트 문제는 Amazon WorkSpaces Administration Guide의 클라이언트 및 관리자 문제 해결 페이지에서 확인할 수 있습니다. WorkSpace

주제

- AD 커넥터가 액티브 디렉터리에 연결할 수 없습니다.
- WorkSpace 사용자 지정 이미지 생성 오류 문제 해결
- 비정상으로 WorkSpace 표시된 Windows 문제 해결
- 디버깅을 위한 지원 로그 번들 수집 WorkSpaces
- 가장 가까운 AWS 지역까지의 지연 시간을 확인하는 방법

AD 커넥터가 액티브 디렉터리에 연결할 수 없습니다.

AD Connector가 온프레미스 디렉터리에 연결하려면 온프레미스 네트워크의 방화벽에 VPC의 두 서브넷 모두에 대해 CIDR에 대해 특정 포트가 열려 있어야 합니다. 시나리오 1: AD 커넥터를 사용하여 온-프레미스 Active Directory 서비스에 대한 프록시 인증을 참조하십시오. 이러한 조건이 충족되는지 테스트하려면 다음 단계를 수행하십시오.

연결을 테스트하려면:

1. VPC에서 Windows 인스턴스를 실행하고 RDP를 통해 연결합니다. VPC 인스턴스에서 나머지 단계를 수행합니다.
2. DirectoryServicePortTest테스트 애플리케이션을 다운로드하고 압축을 풉니다. 필요한 경우 테스트 응용 프로그램을 수정할 수 있도록 소스 코드와 Microsoft Visual Studio 프로젝트 파일이 포함되어 있습니다.
3. Windows 명령 프롬프트에서 다음 옵션을 사용하여 DirectoryServicePortTest 테스트 응용 프로그램을 실행합니다.

```
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>— 포리스트 및 도메인 기능 수준을 테스트하는 데 사용되는 정규화된 도메인 이름입니다. 도메인 이름을 제외하면 기능 수준이 테스트되지 않습니다.

< 서버_IP_주소> — 온프레미스 도메인에 있는 도메인 컨트롤러의 IP 주소입니다. 포트는 이 IP 주소를 기준으로 테스트됩니다. IP 주소를 제외하면 포트는 테스트되지 않습니다.

이 테스트는 VPC에서 도메인으로 필요한 포트가 열려 있는지 확인합니다. 또한 테스트 앱은 최소 포리스트 및 도메인 기능 수준도 테스트합니다.

WorkSpace 사용자 지정 이미지 생성 오류 문제 해결

Windows 또는 Amazon WorkSpace Linux를 시작하고 사용자 지정한 경우 이를 기반으로 사용자 지정 이미지를 생성할 수 WorkSpace 있습니다. 사용자 지정 이미지에는 운영 체제, 애플리케이션 소프트웨어 및 에 대한 설정이 포함됩니다 WorkSpace.

Windows 사용자 지정 이미지를 생성하기 위한 요구 사항 또는 Amazon Linux 사용자 지정 이미지를 생성하기 위한 요구 사항을 검토하십시오. 이미지를 생성하려면 먼저 모든 사전 요구 사항을 충족해야 이미지 생성을 시작할 수 있습니다.

Windows가 이미지 생성 요구 사항을 WorkSpace 충족하는지 확인하려면 이미지 검사기를 실행하는 것이 좋습니다. 이미지 검사기는 이미지가 생성되는 WorkSpace 시기에 대해 일련의 테스트를 수행하고 발견된 문제를 해결하는 방법에 대한 지침을 제공합니다. 자세한 내용은 이미지 검사기 설치 및 구성을 참조하십시오.

모든 테스트를 WorkSpace 통과하면 “검증 성공” 메시지가 나타납니다. 이제 사용자 지정 번들을 생성할 수 있습니다. 그렇지 않으면 테스트 실패 및 경고를 유발하는 모든 문제를 해결하고 모든 테스트를 WorkSpace 통과할 때까지 이미지 검사기 실행 프로세스를 반복하세요. 이미지를 만들려면 먼저 모든 실패와 경고를 해결해야 합니다.

자세한 내용은 이미지 검사기에서 감지한 문제 해결 팁을 참조하십시오.

비정상으로 WorkSpace 표시된 Windows 문제 해결

Amazon WorkSpaces 서비스는 상태 요청을 WorkSpace 전송하여 a의 상태를 정기적으로 확인합니다. 에서 적시에 응답을 받지 못하면 비정상으로 표시됩니다. WorkSpace WorkSpace 이 문제의 일반적인 원인은 다음과 같습니다.

- 의 WorkSpace 애플리케이션이 Amazon WorkSpaces 서비스와 서비스 간의 네트워크 연결을 차단하고 WorkSpace 있습니다.

- 의 CPU 사용률이 높습니다 WorkSpace.
- 의 컴퓨터 WorkSpace 이름이 변경되었습니다.
- Amazon 서비스에 응답하는 에이전트 또는 WorkSpaces 서비스가 실행 상태가 아닙니다.

다음 문제 해결 단계를 통해 WorkSpace 를 정상 상태로 되돌릴 수 있습니다.

- 먼저 Amazon WorkSpace WorkSpaces 콘솔에서 를 재부팅합니다. 재부팅해도 문제가 WorkSpace 해결되지 않으면 RDP를 사용하거나 SSH를 사용하여 Amazon WorkSpace Linux에 연결하십시오.
- 다른 프로토콜로 에 WorkSpace 연결할 수 없는 경우 Amazon 콘솔에서 다시 WorkSpace 빌드하십시오. WorkSpaces
- WorkSpaces 연결을 설정할 수 없는 경우 다음을 확인하십시오.

CPU 사용률 확인

Open Task Manager를 사용하여 CPU 사용률이 높은지 확인하십시오. WorkSpace 문제가 발생한 경우 다음 문제 해결 단계 중 하나를 시도하여 문제를 해결하십시오.

1. CPU를 많이 사용하는 모든 서비스를 중지하십시오.
2. 현재 사용되는 것보다 큰 컴퓨팅 유형으로 크기를 조정하십시오. WorkSpace
3. 를 재부팅합니다. WorkSpace

> **Note**
>
> 높은 CPU 사용률을 진단하고 위 단계를 수행해도 높은 CPU 사용률 문제가 해결되지 않는 경우 지침을 보려면 CPU 병목 현상이 발생하지 않을 때 EC2 Windows 인스턴스에서 높은 CPU 사용률을 진단하려면 어떻게 해야 합니까? 를 참조하십시오.

의 컴퓨터 이름을 확인하십시오. WorkSpace

Workspace의 컴퓨터 이름이 변경된 경우 원래 이름으로 다시 변경하십시오.

1. Amazon WorkSpaces 콘솔을 연 다음 Unhealth를 펼쳐 세부 WorkSpace 정보를 표시합니다.
2. 컴퓨터 이름을 복사합니다.
3. RDP를 WorkSpace 사용하여 연결합니다.

4. 명령 프롬프트를 연 다음 호스트 이름을 입력하여 현재 컴퓨터 이름을 확인합니다.
   a. 이름이 2단계의 컴퓨터 이름과 일치하면 다음 문제 해결 섹션으로 건너뛰십시오.
   b. 이름이 일치하지 않으면 sysdm.cpl 를 입력하여 시스템 속성을 연 다음 이 섹션의 나머지 단계를 따르십시오.
5. [변경] 을 선택한 다음 2단계의 컴퓨터 이름을 붙여넣습니다.
6. 메시지가 표시되면 도메인 사용자 자격 증명을 입력합니다.
7. 실행 SkyLightWorkspaceConfigService상태인지 확인합니다.
   a. 서비스에서 서비스가 실행 SkyLightWorkspaceConfigService 상태인지 확인합니다. WorkSpace 그렇지 않은 경우 서비스를 시작하세요.

방화벽 규칙 확인

Windows 방화벽과 실행 중인 타사 방화벽에 다음 포트를 허용하는 규칙이 있는지 확인하십시오.

- 포트 4172의 인바운드 TCP: 스트리밍 연결을 설정합니다.
- 포트 4172의 인바운드 UDP: 사용자 입력을 스트리밍합니다.
- 포트 8200의 인바운드 TCP: 관리 및 구성합니다. WorkSpace
- 포트 55002의 아웃바운드 UDP: PCoIP 스트리밍.

방화벽이 상태 비저장 필터링을 사용하는 경우 임시 포트 49152-65535를 열어 리턴 통신을 허용하십시오.

방화벽이 스테이트풀 필터링을 사용하는 경우 임시 포트 55002가 이미 열려 있는 것입니다.

디버깅을 위한 지원 로그 번들 수집 WorkSpaces

WorkSpaces 문제를 해결할 때는 해당 WorkSpaces 클라이언트와 클라이언트가 설치된 호스트에서 로그 번들을 수집해야 합니다. WorkSpace 로그에는 두 가지 기본 범주가 있습니다.

- 서버측 로그: 이 시나리오에서는 서버가 서버이므로 자체적으로 존재하는 로그입니다. WorkSpace WorkSpace
- 클라이언트측 로그: 최종 사용자가 연결하는 데 사용하는 장치의 로그입니다. WorkSpace

- Windows 및 macOS 클라이언트만 로컬에서 로그를 기록합니다.

- Zero 클라이언트와 iOS 클라이언트는 로그하지 않습니다.
- Android 로그는 로컬 스토리지에서 암호화되어 WorkSpaces 클라이언트 엔지니어링 팀에 자동으로 업로드됩니다. 해당 팀만 Android 기기의 로그를 검토할 수 있습니다.

WSP 서버측 로그

모든 WSP 구성 요소는 로그 파일을 다음 두 폴더 중 하나에 기록합니다.

- 기본 위치: `C:\ProgramData\Amazon\WSP\` 및 `C:\ProgramData\NICE\dcv\log\`
- 아카이브 위치: `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Windows에서 로그 파일 상세 정보 표시 변경하기

로그 상세 수준 그룹 정책 설정을 구성하여 WSP Windows의 로그 파일 세부 정보 표시 수준을 WorkSpaces 대규모로 구성할 수 있습니다.

개별 WorkSpaces 로그 파일의 상세 정보를 변경하려면 Windows 레지스트리 편집기를 사용하여 키를 구성하십시오. `h_log_verbosity_options`

1. Windows 레지스트리 편집기를 관리자 권한으로 엽니다.
2. `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`로 이동합니다.
3. `WSP`키가 없는 경우 마우스 오른쪽 버튼을 클릭하고 새로 만들기 > 키를 선택하고 이름을 지정합니다. `WSP`
4. `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP`로 이동합니다.
5. `h_log_verbosity_options`값이 없는 경우 마우스 오른쪽 버튼을 클릭하고 새로 만들기 > DWORD를 선택하고 이름을 지정합니다. `h_log_verbosity_options`
6. 새 `h_log_verbosity_options` DWORD를 클릭하고 필요한 세부 정보 수준에 따라 값을 다음 숫자 중 하나로 변경합니다.
   - 0 — 오류
   - 1 — 경고
   - 2 — 정보
   - 3 — 디버그
7. 확인을 선택하고 Windows 레지스트리 편집기를 닫습니다.
8. 를 다시 시작합니다. WorkSpace

PCoIP 서버측 로그

모든 PCoIP 구성 요소는 로그 파일을 다음 두 폴더 중 하나에 기록합니다.

- 기본 위치: `C:\ProgramData\Teradici\PCoIPAgent\logs`
- 아카이브 위치: `C:\ProgramData\Teradici\logs`

복잡한 문제를 처리할 AWS Support 때 PCoIP Server 에이전트를 자세한 로깅 모드로 설정해야 하는 경우가 있습니다. 이 기능을 활성화하려면:

1. 다음 레지스트리 키를 엽니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults`
2. `pcoip_admin_defaults`키에서 다음과 같은 32비트 DWORD를 생성합니다. `pcoip.event_filter_mode`
3. 의 값을 “3" (12/16진수) `pcoip.event_filter_mode` 로 설정합니다.

참고로 다음은 이 DWORD에서 정의할 수 있는 로그 임계값입니다.

- 0 — (중요)
- 1 — (오류)
- 2 — (정보)
- 3 — (디버그)

`pcoip_admin_default`DWORD가 존재하지 않는 경우 기본적으로 로그 레벨이 설정됩니다2. 더 이상 자세한 로그가 필요하지 않은 후에는 값을 2 DWORD로 복원하는 것이 좋습니다. DWORD는 크기가 훨씬 크고 디스크 공간을 불필요하게 소비하기 때문입니다.

WebAccess 서버측 로그

PCoIP 및 WSP (버전 1.0+) 의 WorkSpaces 경우 WorkSpaces 웹 액세스 클라이언트는 STXHD 서비스를 사용합니다. 웹 액세스 로그는 에 저장됩니다. WorkSpaces `C:\ProgramData\Amazon\Stxhd\Logs`

WSP (버전 2.0+) 의 WorkSpaces 경우 WorkSpaces 웹 액세스 로그는 에 저장됩니다. `C:\ProgramData\Amazon\WSP\`

클라이언트측 로그

이러한 로그는 사용자가 연결하는 WorkSpaces 클라이언트에서 생성되므로 최종 사용자의 컴퓨터에 기록됩니다. Windows 및 Mac의 로그 파일 위치는 다음과 같습니다.

- Windows: `"%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"`
- macOS: `~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs`
- Linux: `~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

사용자가 겪을 수 있는 문제를 해결하는 데 도움이 되도록 모든 Amazon WorkSpaces 클라이언트에서 사용할 수 있는 고급 로깅을 활성화하십시오. 고급 로깅은 비활성화될 때까지 모든 후속 클라이언트 세션에 대해 활성화됩니다.

1. 에 연결하기 전에 최종 사용자는 WorkSpaces 클라이언트에 대한 고급 로깅을 활성화해야 합니다. WorkSpace
2. 그런 다음 최종 사용자는 평소와 같이 연결하여 사용하고 문제를 재현해 봐야 합니다. WorkSpace
3. 고급 로깅은 상세 성능 데이터를 비롯하여 진단 정보와 디버깅 수준 세부 정보가 포함된 로그 파일을 생성합니다.

이 설정은 명시적으로 해제할 때까지 유지됩니다. 사용자가 자세한 로그온 문제를 성공적으로 재현한 후에는 로그 파일이 커지므로 이 설정을 사용하지 않도록 설정해야 합니다.

Windows용 자동 서버측 로그 번들 수집

`Get-WorkSpaceLogs.ps1`스크립트는 서버 측 로그 번들을 빠르게 수집하는 데 유용합니다. AWS Support 지원 사례에서 AWS Support 요청하여 스크립트를 요청할 수 있습니다.

1. 클라이언트를 사용하거나 RDP (원격 데스크톱 프로토콜) 를 사용하여 연결합니다. WorkSpace
2. 관리 명령 프롬프트를 시작합니다 (관리자 권한으로 실행).
3. 명령 프롬프트에서 다음 명령을 사용하여 스크립트를 실행합니다.

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. 스크립트는 사용자 데스크톱에 로그 번들을 생성합니다.

스크립트는 다음 폴더가 포함된 zip 파일을 만듭니다.

- C — 스카이라이트, EC2Config, Teradici ProgramData, 이벤트 뷰어 및 Windows 로그 (Panther 및 기타) 와 관련된 프로그램 파일, 프로그램 파일 (x86) 및 Windows의 파일을 포함합니다.
- cliXML — 대화형 필터링에 사용하여 Powershell에서 가져올 수 있는 XML 파일을 포함합니다. `Import-CliXML` 가져오기-Clixml을 참조하십시오.
- Config - 수행된 각 검사에 대한 세부 로그
- ScriptLogs— 스크립트 실행에 대한 로그 (조사와는 관련이 없지만 스크립트가 수행하는 작업을 디버깅하는 데 유용함).
- tmp —임시 폴더 (비어 있어야 함)
- 추적 - 로그 수집 중에 수행된 패킷 캡처입니다.

가장 가까운 AWS 지역까지의 지연 시간을 확인하는 방법

Connection Health Check 웹사이트는 Amazon을 사용하는 모든 필수 서비스에 연결할 WorkSpaces 수 있는지 여부를 신속하게 확인합니다. 또한 WorkSpaces Amazon을 사용할 수 있는 각 AWS 지역에 대한 성능 검사를 수행하여 사용자에게 어느 지역이 가장 빠를지 알려줍니다.

결론

조직이 민첩성을 높이고 데이터를 더 잘 보호하며 직원의 생산성을 높이기 위해 노력함에 따라 최종 사용자 컴퓨팅에 전략적인 변화가 일어나고 있습니다. 클라우드 컴퓨팅으로 이미 실현된 이점 중 상당수는 최종 사용자 컴퓨팅에도 적용됩니다. WorkSpacesAmazon을 통해 Windows 또는 Linux 데스크톱을 AWS 클라우드로 이전함으로써 조직은 직원 추가에 따라 빠르게 확장하고, 데이터를 디바이스에서 분리하여 보안 태세를 개선하고, 직원들이 원하는 디바이스로 어디서나 액세스할 수 있는 휴대용 데스크톱을 제공할 수 있습니다.

WorkSpaces Amazon은 기존 IT 시스템 및 프로세스에 통합되도록 설계되었으며, 이 백서에서는 이를 위한 모범 사례를 설명했습니다. 이 백서의 지침을 따른 결과 AWS 글로벌 인프라에서 비즈니스와 함께 안전하게 확장할 수 있는 비용 효율적인 클라우드 데스크톱 배포가 가능해졌습니다.

기여자

다음은 이 문서의 기여자입니다.

- 앤드류 모건, EUC 솔루션 아키텍트, Amazon Web Services
- 돈 스콧, 수석 EUC 전문 컨설턴트, Amazon Web Services
- 클라우스 베커, 수석 EUC 스페셜리스트 솔루션 아키텍트, Amazon Web Services
- 나비에로 매기, 아마존 웹 서비스 수석 솔루션 아키텍트
- 로버트 파운틴, EUC 전문 컨설턴트, Amazon Web Services
- 스티븐 스테틀러, 수석 EUC 솔루션 아키텍트, Amazon Web Services

참조 자료

추가 정보는 다음을 참조하세요.

- 아마존 WorkSpaces 관리 가이드
- Amazon WorkSpaces 개발자 가이드
- 아마존 WorkSpaces 클라이언트
- 퍼펫 AWS OpsWorks 엔터프라이즈용으로 아마존 리눅스 2 아마존 WorkSpaces 관리하기
- 아마존 리눅스 커스터마이징 WorkSpace
- 클라이언트측 LDAPS를 사용하여 AWS Directory Service의 LDAP 보안을 개선하는 방법
- Amazon과 함께 Amazon CloudWatch WorkSpaces AWS Lambda Events를 사용하여 플릿 가시성을 높이세요.
- 아마존이 WorkSpaces 사용하는 방법 AWS KMS
- AWS CLI 명령 참조 — WorkSpaces
- 아마존 WorkSpaces 메트릭스 모니터링
- MATE 데스크톱 환경
- AWS Directory 서비스 관리 문제 해결
- Amazon WorkSpaces 관리 문제 해결
- Amazon WorkSpaces 클라이언트 문제 해결
- 셀프 서비스 WorkSpaces 포털로 Amazon을 자동화하세요

문서 수정

이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
마이너 업데이트	AD 디렉터리 서비스, 재해 복구/비즈니스 연속성 및 지역 간 리디렉션에 대한 콘텐츠가 업데이트되었습니다. Amazon Connect 오디오 최적화가 추가되었습니다 WorkSpaces . 서식에 대한 사소한 업데이트.	2022년 5월 26일
마이너 업데이트	비포함 언어를 수정하세요.	2022년 4월 6일
백서 업데이트	업데이트된 콘텐츠	2022년 3월 24일
백서 업데이트	AWS Network Firewall, MAD 복제 디렉터리, YubiKey 지원, 컨테이너, WSLv1, 스마트 카드 지원, WorkSpaces 서비스 할당량 및 신뢰할 수 있는 장치에 대한 콘텐츠가 업데이트되었습니다.	2021년 12월 20일
백서 업데이트	WorkSpaces 스트리밍 프로토콜, 스마트 카드 인증, 다이어그램, 클라이언트 배포, 최종 장치 선택 및 웹 액세스에 대한 콘텐츠가 업데이트되었습니다.	2021년 4월 28일
백서 업데이트	업데이트된 콘텐츠	2020년 12월 1일
백서 업데이트	최초 발행 이후 콘텐츠가 업데이트되고 새 다이어그램이 추가되었습니다.	2020년 5월 1일

최초 게시	처음 게시되었습니다.	2016년 7월 1일

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 (a) 정보 제공만을 목적으로 하고, (b) 사전 통지 없이 변경될 수 있는 현재의 AWS 제품 제안 및 관행을 나타내며, (c) 계열사, 공급업체 또는 라이선스 제공자로부터 AWS 어떠한 약정이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 “있는 그대로” 제공됩니다. AWS 고객에 대한 책임과 책임은 AWS 계약에 의해 통제되며, 본 문서는 고객과 체결한 계약의 일부가 아니며 수정하지도 않습니다. AWS

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오. AWS 용어집

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.