Amazon WorkSpaces
개발 모범 사례

네트워크 액세스, 디렉터리 서비스 및 보안

2016년 7월

고지 사항

이 백서는 정보 제공 목적으로만 제공됩니다. 본 백서의 발행일 당시 AWS의 현재 제품 및 실행방법을 설명하며, 예고 없이 변경될 수 있습니다. 고객은 본 백서에 포함된 정보나 AWS 제품 또는 서비스의 사용을 독립적으로 평가할 책임이 있으며, 각 정보 및 제품은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 "있는 그대로" 제공됩니다. 본 백서는 AWS, 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 표현, 계약 약속, 조건 또는 보증을 생성하지 않습니다. 고객에 대한 AWS의 책임 및 의무는 AWS 계약에 준거합니다. 본 백서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

목차

요약

이 백서에서는 Amazon WorkSpaces 배포를 위한 모범 사례를 설명합니다. 이 백서에서 다루는 주제는 네트워크 고려 사항, 디렉터리 서비스 및 사용자 인증, 보안, 모니터링 및 로깅입니다.

이 백서는 4개 범주로 구성되어 있어 관련 정보에 보다 빠르게 액세스할 수 있습니다. 이 백서는 네트워크 엔지니어, 디렉터리 엔지니어 또는 보안 엔지니어를 위해 작성된 것입니다.

서론

Amazon WorkSpaces는 클라우드 기반의 관리형 데스크톱 컴퓨팅 서비스입니다. Amazon WorkSpaces는 하드웨어를 구매 또는 배포하거나 복잡한 소프트웨어를 설치해야 하는 부담 없이 AWS 명령줄 인터페이스(CLI)를 사용하여 AWS Management Console에서 몇 번의 클릭으로, 또는 API를 사용하여 데스크톱 환경을 제공합니다. Amazon WorkSpaces에서는 몇 분만에 데스크톱을 시작하여 온프레미스 또는 외부 네트워크에서 안전하고 안정적이며 신속하게 데스크톱 소프트웨어에 연결 및 액세스할 수 있습니다. 다음을 할 수 있습니다.

- AWS 디렉터리 서비스: AD 커넥터를 사용하여 기존 온프레미스 Microsoft Active Directory(AD)를 활용.
- 디렉터리를 AWS Cloud로 확장.
- AWS 디렉터리 서비스: Microsoft AD 또는 Simple AD로 관리형 디렉터리를 구축하여 사용자 및 WorkSpaces를 관리.

또한 AD 커넥터로 온프레미스 또는 클라우드 호스팅된 RADIUS 서버를 활용하여 WorkSpaces에 멀티 팩터 인증(MFA)을 제공할 수 있습니다.

CLI 또는 API를 사용하여 Amazon WorkSpaces 프로비저닝을 자동화할 수 있습니다. 그러면 Amazon WorkSpaces를 기존 프로비저닝 워크플로에 통합할 수 있습니다.

보안을 위해, WorkSpaces 서비스가 제공하는 통합형 네트워크 암호화 이외에 WorkSpaces에 대해 저장 시 암호화를 사용할 수도 있습니다(보안 단원의 Encrypted WorkSpaces 참조).

Microsoft System Center Configuration Manager(SCCM)와 같은 기존 온프레미스 도구를 사용하거나 Amazon WorkSpaces Application Manager (Amazon WAM)를 활용하여 WorkSpaces에 애플리케이션을 배포할 수 있습니다.

이제부터 Amazon WorkSpaces에 대한 세부 정보, 이 서비스가 작동하는 방식, 이 서비스를 실행하는 데 필요한 사항, 그리고 사용 가능한 옵션 및 기능에 대해 설명합니다.

WorkSpaces 요구 사항

Amazon WorkSpaces 서비스를 사용하려면 세 가지 구성 요소를 성공적으로 배포해야 합니다.

- **WorkSpaces 클라이언트 애플리케이션**. Amazon WorkSpaces 지원 클라이언트 디바이스. 전체 목록은 지원되는 플랫폼 및 디바이스를 참조하십시오.

  또한 PCoIP(Personal Computer over Internet Protocol) 제로 클라이언트를 사용하여 WorkSpaces에 연결할 수도 있습니다. 사용 가능한 디바이스의 목록은 Amazon WorkSpaces용 PCoIP 제로 클라이언트를 참조하십시오.

- **사용자를 인증하고 사용자의 WorkSpace**에 대한 액세스를 제공하기 위한 디렉터리. Amazon WorkSpaces는 현재 AWS 디렉터리 서비스 및 Active Directory와 연동됩니다. AWS 디렉터리 서비스를 사용하는 온프레미스 Active Directory 서버를 통해 WorkSpaces에 대한 기존 엔터프라이즈 사용자 자격 증명을 지원할 수 있습니다.

- **Amazon WorkSpaces가 실행될 Amazon Virtual Private Cloud(Amazon VPC)**. WorkSpaces 배포 시 최소 2개의 서브넷이 필요합니다. 각 AWS 디렉터리 서비스 구조가 다중 AZ 배포에서 2개의 서브넷을 필요로 하기 때문입니다.

네트워크 고려 사항

각 WorkSpace는 해당 WorkSpace를 생성할 때 사용한 특정 Amazon VPC 및 AWS 디렉터리 서비스와 연결됩니다. 모든 AWS 디렉터리 서비스 구조(Simple AD, AD 커넥터 및 Microsoft AD)는 작동하기 위해 서로 다른 가용 영역에 각각 2개의 서브넷이 필요합니다. 서브넷은 디렉터리 서비스 구조와 영구적으로 연결되어 있으며 AWS 디렉터리 서비스를 생성한 다음에는 수정할 수 없습니다. 따라서 디렉터리 서비스 구조를 생성하기 전에 반드시 올바른 서브넷 크기를 결정해야 합니다. 서브넷을 생성하기 전에 다음 사항을 신중하게 고려하십시오.

- 장기적으로 얼마나 많은 WorkSpaces가 필요한가?예상 증가율은 얼마인가?
- 어떤 유형의 사용자를 수용해야 하는가?
- 연결할 Active Directory 도메인이 몇 개인가?
- 엔터프라이즈 사용자 계정이 어디에 상주하는가?

사용자 그룹, 즉 페르소나는 계획 프로세스의 일환으로 필요한 액세스 유형 및 사용자 인증을 기반으로 정의하는 것이 좋습니다. 이러한 사항은 특정 애플리케이션 또는 리소스에 대한 액세스를 제한해야 할 때 도움이 됩니다. 정의된 사용자 페르소나는 AWS 디렉터리 서비스, 네트워크 액세스 제어 목록, 라우팅 테이블 및 VPC 보안 그룹을 사용하여 액세스를 세그먼트화 및 제한하는 데 유용합니다. 각 AWS 디렉터리 서비스 구조는 2개의 서브넷을 사용하며 해당 구조로부터 실행되는 모든 WorkSpaces에 동일한 설정을 적용합니다. 예를 들어 특정 AD 커넥터에 연결된 모든 WorkSpaces에 적용되는 보안 그룹을 사용하여 MFA 인증이 필요한지 여부, 또는 최종 사용자가 자신의 WorkSpace에 대한 로컬 관리자 액세스 권한을 가질 수 있는지 여부를 지정할 수 있습니다.

> **참고** 각 AD 커넥터는 하나의 Microsoft Active Directory 조직 단위(OU)와 연결됩니다. 이 기능의 이점을 활용할 수 있도록 디렉터리 서비스가 사용자 페르소나를 고려하도록 구성해야 합니다.

이 단원에서는 VPC 및 서브넷 크기 설정을 위한 모범 사례, 트래픽 흐름 및 디렉터리 서비스 설계에 대한 영향을 설명합니다.

VPC 설계

확장성, 보안 및 관리 용이성이 뛰어난 WorkSpaces 환경을 구축하려면 Amazon WorkSpaces를 위해 VPC, 서브넷, 보안 그룹, 라우팅 테이블 및 네트워크 ACL을 설계할 때 고려해야 할 몇 가지 사항이 있습니다.

- **VPC**. WorkSpaces 배포 전용의 VPC를 따로 사용하는 것이 좋습니다. 별도 VPC를 사용할 경우, 트래픽 격리를 생성하여 WorkSpaces를 위해 필요한 거버넌스 및 보안 가드 레일을 지정할 수 있습니다.
- **디렉터리 서비스**. 각 AWS 디렉터리 서비스 구조는 Amazon AZ 사이에 분할된 고가용성 디렉터리 서비스를 제공하는 한 쌍의 서브넷을 필요로 합니다.
- **서브넷 크기**. WorkSpaces 배포는 디렉터리 구조와 연결되며 선택한 AWS 디렉터리 서비스와 동일한 VPC 서브넷에 상주합니다. 몇 가지 고려 사항
  - 서브넷 크기는 영구적이며 변경할 수 없습니다. 따라서 향후 성장에 대비해 충분한 여유가 있어야 합니다.
  - 선택한 AWS 디렉터리 서비스에 대해 기본 보안 그룹을 지정할 수 있습니다. 보안 그룹은 특정 AWS 디렉터리 서비스 구조와 연결된 모든 WorkSpaces에 적용됩니다.
  - 여러 AWS 디렉터리 서비스가 동일한 서브넷을 사용하도록 할 수 있습니다.

VPC를 설계할 때 향후 계획을 감안하십시오. 예를 들어 안티바이러스 서버, 패치 관리 서버, 또는 Active Directory 또는 RADIUS MFA 서버를 추가할 수 있습니다. 이러한 요구 사항을 수용하도록 VPC 설계에 추가 가용 IP 주소를 계획하는 것이 가치가 있습니다.

VPC 설계 및 서브넷 크기 설정에 대한 심층적 지침 및 고려 사항은 **re:Invent** 프레젠테이션 How Amazon. com is Moving to Amazon WorkSpaces를 참조하십시오.

네트워크 인터페이스

각 WorkSpace는 2개의 Elastic Network Interface(ENI), 1개의 관리 네트워크 인터페이스(eth0) 및 1개의 주 네트워크 인터페이스(eth1)를 가집니다. AWS는 관리 네트워크 인터페이스를 사용하여 WorkSpace를 관리합니다. 이 인터페이스에서 클라이언트 연결이 끝납니다. AWS는 이 인터페이스를 위해 프라이빗 IP 주소 범위를 활용합니다. 네트워크 라우팅이 제대로 기능하려면 WorkSpaces VPC와 통신이 가능한 어떤 네트워크에서도 이 프라이빗 주소 공간을 사용할 수 없습니다.

AWS가 리전별로 사용하는 프라이빗 IP 범위의 목록은 Amazon WorkSpaces 세부 정보를 참조하십시오.

> **참고** Amazon WorkSpaces 및 연결된 관리 네트워크 인터페이스는 VPC에 상주하지 않으며, AWS Management Console에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 ID를 볼 수 없습니다(그림 4, 그림 5 및 그림 6 참조). 하지만 AWS Management Console에서 주 네트워크 인터페이스(eth1)의 보안 그룹 설정을 보고 수정할 수 있습니다. 또한 각 WorkSpace의 주 네트워크 인터페이스는 ENI Amazon EC2 리소스 제한에 포함됩니다. WorkSpaces를 대량 배포하는 경우 AWS Management Console을 통한 지원 티켓을 개설하여 ENI 제한을 증가시켜야 합니다.

트래픽 흐름

Amazon WorkSpaces 트래픽을 2개의 주요 구성 요소로 분할할 수 있습니다.

- 클라이언트 디바이스와 Amazon WorkSpace 서비스 간 트래픽
- Amazon WorkSpace 서비스와 고객 네트워크 트래픽 간 트래픽

다음 단원에서는 이들 구성 요소를 모두 살펴보겠습니다.

클라이언트 디바이스에서 WorkSpace까지

Amazon WorkSpaces 클라이언트를 실행하는 디바이스는 위치(온프레미스 또는 원격)와 상관없이 WorkSpaces 서비스와 연결을 위해 동일한 2개의 포트를 사용합니다. 클라이언트는 모든 인증 및 세션 관련 정보에는 포트 443을 통해 https를 사용하고 지정된 WorkSpace로 전송되는 픽셀 스트리밍과 네트워크 상태 검사에는 TCP 및 UDP 모두에서 포트 4172(PCoIP 포트)를 사용합니다. 양쪽 포트의 트래픽은 암호화됩니다. 포트 443 트래픽은 인증 및 세션 정보에 사용되고 트래픽 암호화를 위해 TLS를 사용합니다. 픽셀 스트리밍 트래픽은 스트리밍 게이트웨이를 통한 WorkSpace의 etho와 클라이언트 간 통신에 AES-256비트 암호화를 사용합니다. 보다 자세한 정보는 이 백서의 보안 단원을 참조하십시오.

AWS는 PCoIP 스트리밍 게이트웨이 및 네트워크 상태 검사 엔드포인트의 리전별 IP 범위를 게시하빈다. Amazon WorkSpaces을 사용하는 특정 AWS 리전까지의 포트 4172 아웃바운드 트래픽만 허용하여 포트 4172 아웃바운드 트래픽을 사내 네트워크에서 AWS 스트리밍 게이트웨이 및 네트워크 상태 검사 엔드포인트까지 제한할 수 있습니다. IP 범위 및 네트워크 상태 검사 엔드포인트는 Amazon WorkSpaces PCoIP 게이트웨이 IP 범위를 참조하십시오.

Amazon WorkSpaces 클라이언트에는 네트워크 상태 검사가 내장되어 있습니다. 이 유틸리티는 사용자 네트워크가 연결을 지원하는지 여부를 애플리케이션 우측 하단의 상태 표시기를 통해 보여줍니다. 클라이언트의 우측 하단에서 **[Network]**를 선택하면 네트워크 상태를 보다 자세히 볼 수 있습니다. 그림 1과 같은 정보가 제공됩니다.

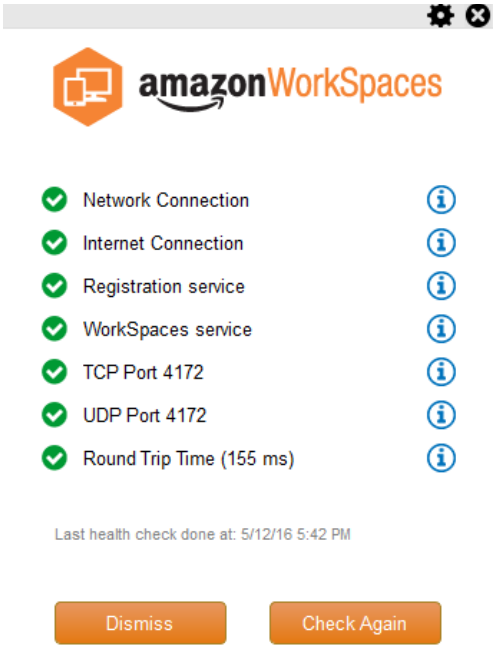

그림 1: WorkSpaces 클라이언트 – 네트워크 검사

사용자가 디렉터리 서비스 구조에 의해 사용되는 디렉터리(일반적으로 기업 디렉터리)에 대한 로그인 정보를 제공하여 클라이언트에서 WorkSpaces까지의 연결을 시작합니다. 로그인 정보는 https를 통해 WorkSpace가 위치한 리전의 Amazon WorkSpaces 서비스의 인증 게이트웨이로 전송됩니다. 그러면 Amazon WorkSpaces의 인증 게이트웨이가 트래픽을 WorkSpace와 연결된 특정 AWS 디렉터리 서비스 서비스 구조로 전달합니다. 에를 들어, AD 커넥터를 사용하는 경우 AD 커넥터가 인증 요청을 온프레미스 또는 AWS VPC에 상주할 수 있는 Active Directory 서비스로 직접 전달합니다(AD DS 배포 시나리오 참조). AD 커넥터는 인증 정보를 저장하지 않으며 상태 비저장 프록시로 작동합니다. 그러므로 AD 커넥터가 Active Directory 서버에 연결할 수 있어야 합니다. AD 커넥터는 AD 커넥터를 생성할 때 정의한 DNS 서버를 사용하여 연결할 Active Directory 서버를 결정합니다.

AD 커넥터를 사용하고 디렉터리에 MFA가 활성화된 경우 디렉터리 서비스 인증 전에 MFA 토큰이 점검됩니다. MFA 검증이 실패할 경우 사용자의 로그인 정보가 AWS 디렉터리 서비스로 전달되지 않습니다.

사용자가 인증되면 스트리밍 트래픽이 포트 4172(PCoIP 포트)에서 AWS 스트리밍 게이트웨어를 거쳐 WorkSpace로 전송됩니다. 세션 관련 정보는 세션 내내 https를 통해 교환됩니다. 스트리밍 트래픽은 VPC에 연결되지 않은 WorkSpace의 첫 번째 ENI(WorkSpace의 eth0)를 사용합니다. 스트리밍 게이트웨이에서 ENI까지의 네트워크 연결은 AWS에서 관리합니다. 스트리밍 게이트웨이에서 WorkSpaces 스트리밍 ENI까지 연결 오류가 발생하는 경우, CloudWatch 이벤트가 생성됩니다(이 백서의 Amazon CloudWatch를 사용한 모니터링 또는 로깅 단원 참조).

Amazon WorkSpaces 서비스와 클라이언트 사이에서 전송되는 데이터량은 픽셀 활동 수준에 따라 달라집니다. 최적의 사용자 환경을 보장하기 위해 WorkSpaces 클라이언트와 WorkSpaces가 위치한 AWS 리전 사이의 왕복 시간(RTT)이 100ms 이하인 것이 좋습니다. 일반적으로 이는 WorkSpaces 클라이언트가 WorkSpace를 호스트하는 리전에서 2,000마일 이내에 위치한다는 의미입니다. Amazon WorkSpaces 서비스를 위해 연결할 최적의 AWS 리전을 결정하는 데 참조할 수 있는 연결 상태 점검 웹 페이지가 제공됩니다.

Amazon WorkSpaces 서비스에서 VPC까지

클라이언트에서 WorkSpace까지 연결이 인증되고 스트리밍 트래픽이 시작되면 WorkSpaces 클라이언트가 VPC와 연결된 Windows 데스크톱(사용자의 WorkSpace)을 표시하며 네트워크는 연결이 설정되었음을 표시해야 합니다. WorkSpace의 주 ENI(eth1로 식별됨)는 VPC가 제공하는 DHCP(Dynamic Host Configuration Protocol) 서비스를 통해 일반적으로 AWS 디렉터리 서비스와 동일한 서브넷 중에서 할당되는 IP 주소를 갖습니다. IP 주소는 해당 WorkSpace의 수명 내내 유지됩니다. VPC에 상주하는 ENI는 VPC의 모든 리소스, 그리고 VPC와 연결한 모든 네트워크에 액세스할 수 있습니다(VPC 피어링, AWS Direct Connect 연결 또는 VPN 연결을 통해).

네트워크 리소스에 대한 ENI 액세스는 AWS 디렉터리 서비스가 각 WorkSpace에 대해 구성한 기본 보안 그룹(여기에서 보안 그룹에 대한 자세한 내용 참조)과 사용자가 ENI에 할당한 추가 보안 그룹에 의해 결정됩니다. AWS Management Console 또는 CLI를 사용하여 VPC를 향하는 ENI에 보안 그룹을 추가할 수 있습니다. 보안 그룹 이외에 지정된 WorkSpace에서 선호하는 호스트 기반 방화벽을 사용하여 VPC 내부 리소스에 대한 네트워크 액세스를 제한할 수 있습니다.

나중에 나오는 AD DS 배포 시나리오의 그림 4에 앞서 설명한 트래픽 흐름이 나와 있습니다.

일반적 구성 예

두 유형의 사용자가 있고 AWS 디렉터리 서비스가 사용자 인증을 위해 Active Directory를 사용하는 시나리오를 생각해봅시다.

- **어디서나 전체 액세스가 필요한 작업자**(예: 정규 직원). 이러한 사용자는 인터넷 및 내부 네트워크에 제한 없이 액세스할 수 있고 VPC에서 방화벽을 지나 온프레미스 네트워크에 액세스합니다.
- **사내 네트워크로부터 제한적 액세스만 허용되는 작업자**(예: 계약업체 및 컨설턴트). 이러한 사용자는 VPC 내에서 프록시 서버를 통한 제한적 인터넷 액세스(특정 웹 사이트만 접속)가 허용되고 VPC 내에서 그리고 온프레미스 네트워크에 대해 제한적 네트워크 액세스가 허용됩니다.

정규 직원에게 WorkSpace에 대한 로컬 관리자 액세스 권한을 부여하여 소프트웨어를 설치하도록 허용하고 MFA로 2팩터 인증을 적용하려고 합니다. 또한 정규 직원이 WorkSpace로부터 제한 없이 인터네에 액세스하도록 허용하려고 합니다.

계약업체의 경우, 미리 설치된 특정 애플리케이션만 사용할 수 있도록 로컬 관리자 액세스를 차단하려고 합니다. 이러한 WorkSpaces에 대해 보안 그룹을 통해 매우 제한적인 네트워크 액세스 제어를 적용하기를 원합니다. 특정 내부 웹 사이트에 대해서만 포트 80 및 443을 개방해야 하며 이들의 인터넷 액세스는 차단하려고 합니다.

이 시나리오에는 네트워크 및 데스크톱 액세스 요구 사항이 상이한 완전히 다른 두 유형의 사용자 페르소나가 있습니다. 이들의 WorkSpaces를 다르게 관리 및 구성하는 것이 모범 사례입니다. 이렇게 하려면 각 사용자 페르소나에 1개씩, 2개의 AD 커넥터를 생성해야 합니다. 각 AD 커넥터는 예상 WorkSpaces 사용 증가를 충족하는 데 충분한 IP 주소를 갖는 2개의 서브넷을 필요로 합니다.

> **참고** 각 AWS VPC 서브넷은 5개의 IP 주소(첫 4개와 마지막 1개)를 관리 목적으로 소비하고 각 AD 커넥터는 해당 주소가 지속되는 각 서브넷에서 1개의 IP 주소를 소비합니다.

이 시나리오에서 추가로 고려할 사항은 다음과 같습니다.

- AWS VPC 서브넷은 프라이빗 서브넷이어야 합니다. 그래야 인터넷 액세스와 같은 트래픽이 NAT 게이트웨이 또는 클라우드의 프록시-NAT 서버를 통해 제어되거나 온프레미스 트래픽 관리 시스템으로 다시 라우팅될 수 있습니다.
- 온프레미스 네트워크를 향하는 모든 VPC 트래픽에 대해 방화벽이 실행됩니다.
- Microsoft Active Directory 서버와 MFA RADIUS 서버는 온프레미스(시나리오 1: AD 커넥터를 사용하여 인증을 온프레미스 AD DS로 프록시 참조)이거나 AWS Cloud 구현의 일부입니다(시나리오 2 및 3, AD DS 배포 시나리오 참조).

모든 WorkSpaces에 일부 형태의 인터넷 액세스가 허용되고 모든 WorkSpaces가 프라이빗 서브넷에서 호스팅된다고 가정하면 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있는 퍼블릭 서브넷도 생성해야 합니다. 정규 직원에 대해서는 인터넷 액세스를 허용하기 위해 NAT 게이트웨이가 필요하고, 컨설턴트 및 계약업체에 대해서는 특정 내부 웹 사이트로 액세스를 제한하기 위해 프록시-NAT 서버가 필요합니다. 오류 대비 계획을 수립하고, 고가용성으로 설계하고, AZ 간 트래픽 요금을 제한하려면 다중 AZ 배포로 2개의 서브넷에서 2개의 NAT 게이트웨이 및 NAT 또는 프록시 서버를 사용해야 합니다. 퍼블릿 서브넷으로 선택하는 2개의 AZ는 AZ가 3개 이상인 리전에서 WorkSpaces 서브넷용으로 사용하는 2개의 AZ와 일치해야 합니다. 모든 트래픽을 각 WorkSpaces AZ에서 해당 퍼블릭 서브넷까지 라우팅하여 AZ 간 트래픽 요금을 제한하고 보다 쉽게 관리할 수 있습니다. 그림 2에는 VPC 구성이 나와 있습니다.

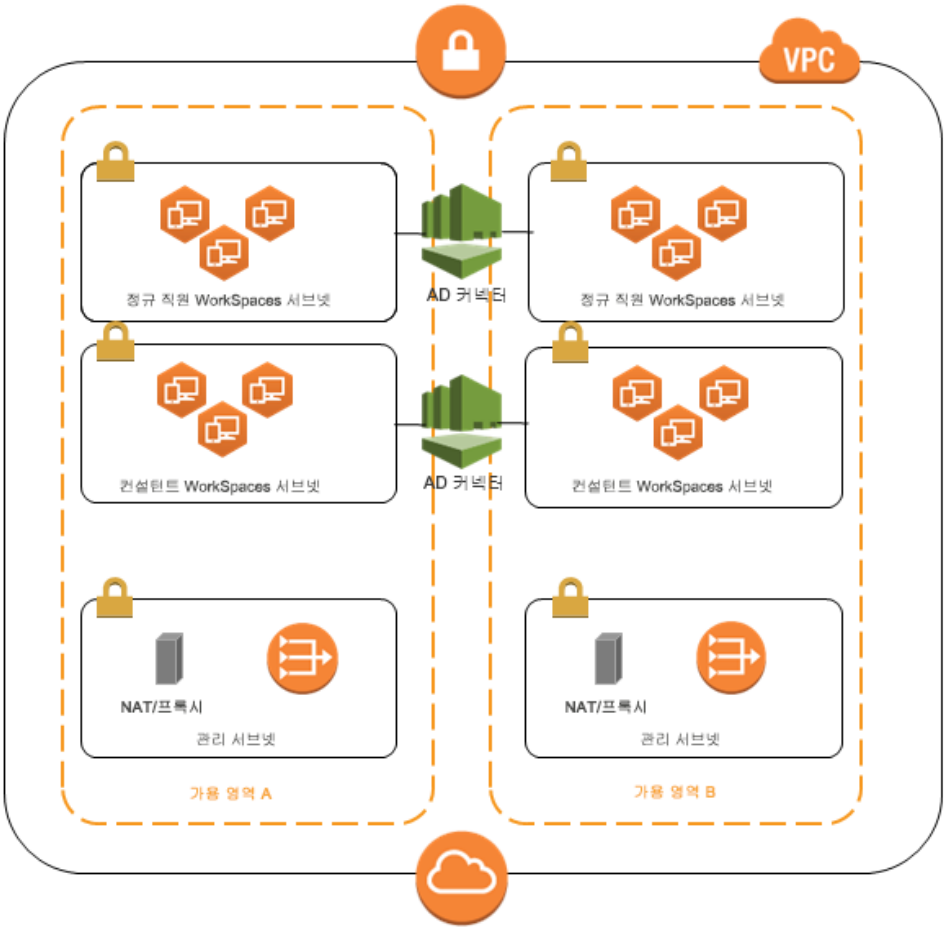

그림 2: 상위 수준 VPC 설계

다음은 앞서 설명한 2개의 WorkSpaces 유형을 구성하는 방법입니다.

- **정규 직원:** Amazon WorkSpaces Management Console의 메뉴 모음에서 **[Directories]** 옵션을 선택하고 정규 직원을 호스팅하는 디렉터리를 선택한 다음 **[Local Administrator Setting]**을 선택합니다. 이 옵션을 활성화하면 새로 생성되는 WorkSpace에 로컬 관리자 권한이 부여됩니다. 인터넷 액세스를 허용하려면 VPC로부터 아웃바운드 인터넷 액세스에 대해 NAT(Network Address Translation)을 구성해야 합니다. MFA를 활성화하려면 RADIUS 서버, 서버 IP, 포트 및 사전 공유 키를 지정해야 합니다.

정규 직원용 WorkSpaces의 경우, AD 커넥터 설정을 통한 기본 보안 그룹을 적용하여 WorkSpace에 대한 인바운드 트래픽을 헬프데스크 서브넷의 RDP(Remote Desktop Protocol)로 제한합니다.

- **계약업체 및 컨설턴트:** Amazon WorkSpaces Management Console에서 **[Internet Access]** 및 **[Local Administrator Setting]**을 비활성화합니다. 그런 다음 **[Security Group]** 설정 섹션 아래에 보안 그룹을 추가하여 해당 디렉터리에서 생성되는 모든 신규 WorkSpaces에 보안 그룹을 적용합니다.

  컨설턴트용 WorkSpaces의 경우, AD 커넥터 설정을 통한 기본 보안 그룹을 AD 커넥터와 연결된 모든 WorkSpaces에 적용하여 WorkSpaces에 대한 아웃바운드 및 인바운드 트래픽을 제한합니다. 이 보안 그룹은 HTTP 및 HTTPS 트래픽, 그리고 온프레미스 네트워크에서 헬프데스크 서브넷으로부터 RDP로 가는 인바운드 트래픽을 제외하고 WorkSpaces로부터 아웃바운드 액세스를 모두 금지합니다.

참고 보안 그룹은 VPC에 상주하는 ENI(WorkSpace의 eth1)에만 적용되고, WorkSpaces 클라이언트로부터 WorkSpace에 대한 액세스는 보안 그룹 때문에 제한되지 않습니다. 그림 3에는 앞서 설명한 최종 WorkSpaces VPC 설계가 나와 있습니다.

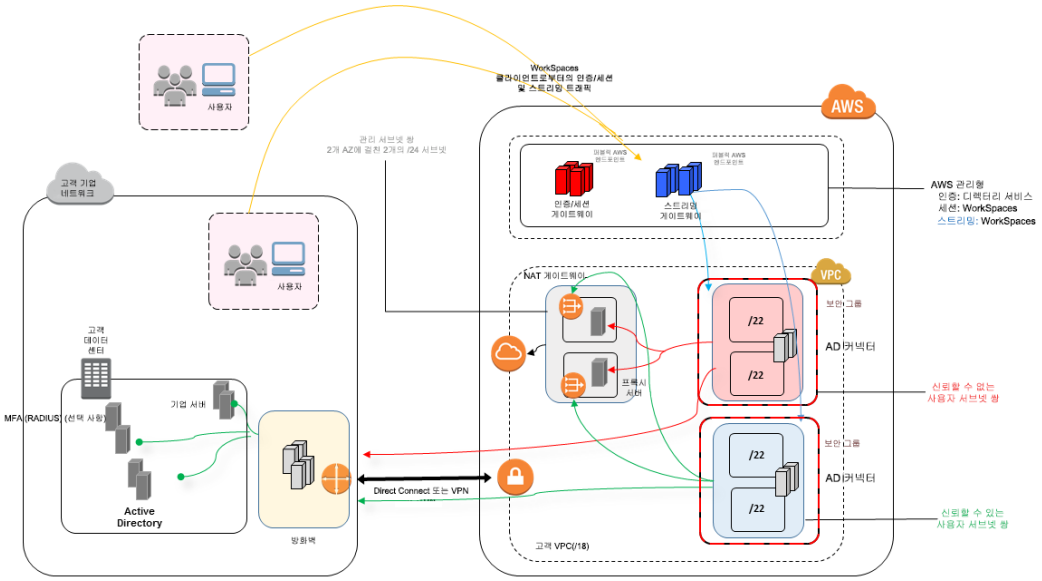

그림 3: 사용자 페르소나를 사용한 WorkSpaces 설계

AWS 디렉터리 서비스

서론에서 언급한 대로, Amazon WorkSpaces는 AWS 디렉터리 서비스를 토대로 합니다. AWS 디렉터리 서비스를 통해 3가지 유형의 디렉터리를 생성할 수 있습니다. 처음 두 유형은 AWS 클라우드에서 상주합니다.

- Microsoft Active Directory(엔터프라이즈 에디션)용 AWS 디렉터리 서비스 **Microsoft AD** - Windows Server 2012 R2로 구동되는 관리형 Microsoft Active Directory.
- **Simple AD** - Samba 4로 구동되는 독립형 Microsoft Active Directory 호환 관리형 디렉터리 서비스.

세 번째 유형 **AD 커넥터**는 인증 요청 및 사용자 또는 그룹 조회를 기존 온프레미스 Microsoft Active Directory로 프록시할 수 있게 해주는 디렉터리 게이트웨이입니다.

다음 단원에서는 Amazon WorkSpaces 브로커 서비스와 AWS 디렉터리 서비스 간 인증을 위한 통신 흐름, AWS 디렉터리 서비스를 사용한 WorkSpaces 구현 모범 사례, MFA와 같은 고급 개념을 설명합니다. 또한 Amazon WorkSpaces at scale의 인프라 아키텍처 개념, Amazon VPC에 대한 요구 사항, 그리고 온프레미스 Microsoft Active Directory 도메인 서비스(AD DS)와 통합을 비롯한 AWS 디렉터리 서비스에 대해서도 논합니다.

AD DS 배포 시나리오

Amazon WorkSpaces는 AWS 디렉터리 서비스를 토대로 하므로 디렉터리 서비스를 올바로 설계 및 배포하는 것이 매우 중요합니다. 다음 세 시나리오는 *Microsoft Active Directory 도메인 서비스* 빠른 시작 가이드를 기반으로 구성된 것으로 AD DS, 특히 WorkSpaces와 통합에 대한 모범 사례 배포 옵션을 자세히 설명합니다. 이 장의 *설계 고려 사항* 단원은 전체 WorkSpaces 설계 개념의 핵심 부분인 WorkSpaces를 위한 AD 커넥터 사용에 대한 특정 요구 사항 및 모범 사례를 다룹니다.

- **시나리오 1: AD 커넥터를 사용하여 인증을 온프레미스 AD DS로 프록시.** 이 시나리오에서 네트워크 연결(VPN/Direct Connect(DX))은 고객까지 설정되며 모든 인증은 AWS 디렉터리 서비스(AD 커넥터)를 통해 고객 온프레미스 AD DS로 프록시됩니다.

- **시나리오 2: 온프레미스 AD DS를 AWS로 확장(복제본).** 이 시나리오는 시나리오 1과 비슷하지만, 여기서는 고객 AD DS의 복제본이 AD 커넥터와 함께 AWS에 배포되어 AD DS 및 AD DS 글로벌 카탈로그에 대한 인증/쿼리 요청의 지연 시간을 단축합니다.
- **시나리오 3: AWS Cloud에서 AWS 디렉터리 서비스를 사용한 독립형 격리형 배포.** 이 시나리오는 격리형이고 인증을 위한 고객과의 연결을 포함하지 않습니다. 이 접근 방식은 AWS 디렉터리 서비스(Microsoft AD)와 AD 커넥터를 사용합니다. 이 시나리오가 인증을 위해 고객과 연결하지 않지만 VPN 또는 DX에서 필요할 경우 애플리케이션 트래픽을 프로비저닝합니다.

시나리오 1: AD 커넥터를 사용하여 인증을 온프레미스 AD DS로 프록시

이 시나리오는 고객이 온프레미스 AD DS를 AWS로 확장하기를 원치 않는 경우 또는 AD DS의 신규 배포가 옵션이 아닌 경우를 위한 것입니다. 그림 4: 온프레미스 Active Directory 측 AD 커넥터는 각 구성 요소를 상위 수준에서 설명하고 사용자 인증 흐름을 보여줍니다.

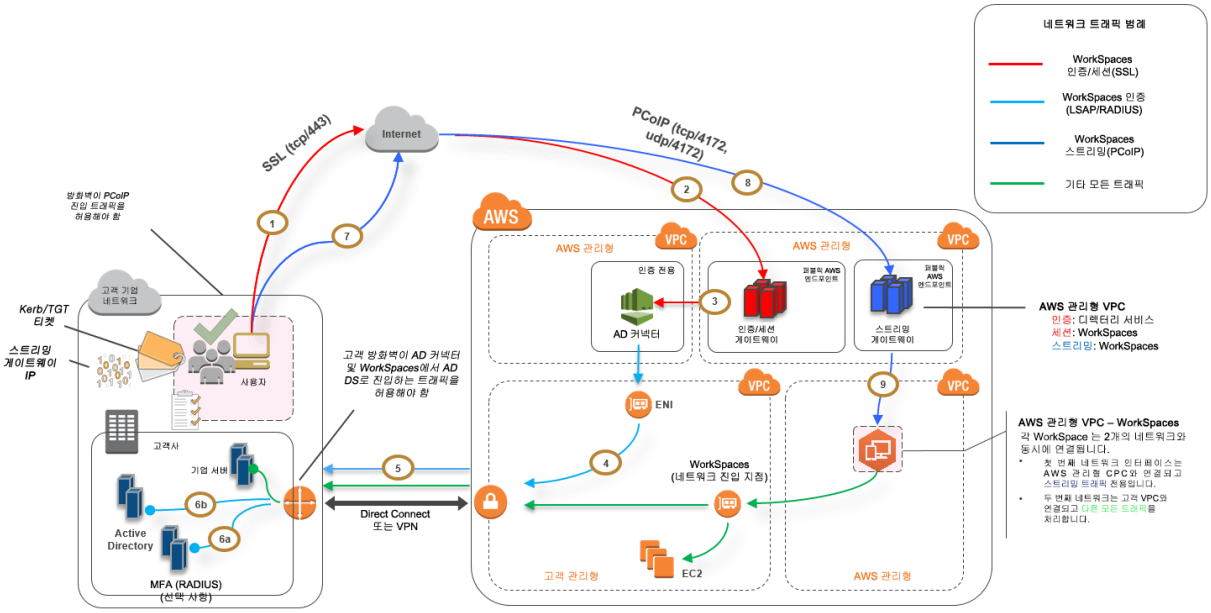

그림 4: 온프레미스 Active Directory 측 AD 커넥터

이 시나리오에서는 AWS 디렉터리 서비스(AD 커넥터)가 온프레미스 AD DS 측 AD 커넥터(그림 5)를 통해 프록시되는 모든 사용자 또는 MFA 인증에 대해 사용됩니다. 인증 프로세스에 사용되는 프로토콜 또는 암호화에 대한 자세한 내용은 이 백서의 보안 단원을 참조하십시오.

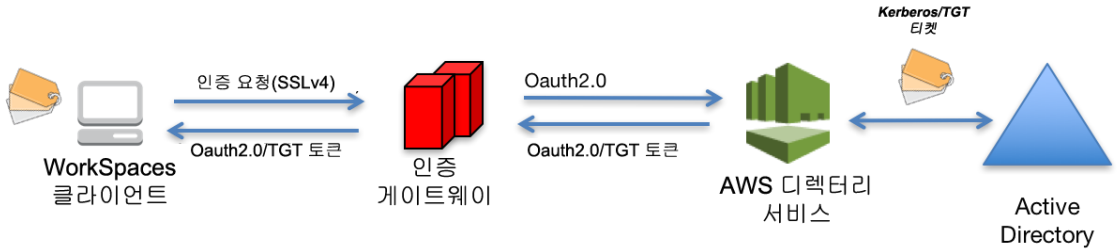

그림 5: 인증 게이트웨이를 통한 사용자 인증

시나리오 1은 고객이 이미 AWS에 그리고 WorkSpaces를 통해 액세스할 수 있는 온프레미스 데이터 센터에 리소스를 보유할 수 있는 하이브리드 아키텍처를 보여줍니다. 고객은 사용자 및 MFA 인증에 기존 온프레미스 AD DS 및 RADIUS 서버를 활용할 수 있습니다.

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

Amazon Web Services:

- **Amazon VPC:** 두 가용 영역에 걸쳐 2개 이상의 프라이빗 서브넷으로 Amazon VPC를 생성.
- **DHCP 옵션 세트:** Amazon VPC DHCP 옵션 세트를 생성. 이를 통해 고객이 지정한 도메인 이름 및 도메인 이름 서버(DNS)(온프레미스 서버)를 정의할 수 있습니다. (자세한 내용은 DHCP 옵션 세트를 참조하십시오.)
- **Amazon 가상 프라이빗 게이트웨이:** IPsec VPN 터널 또는 AWS Direct Connect 연결을 통해 자체 네트워크와 통신을 활성화.
- **AWS 디렉터리 서비스:** AD 커넥터가 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- **Amazon WorkSpaces:** WorkSpaces가 AD 커넥터와 동일한 프라이빗 서브넷에 배포됩니다(*설계 고려 사항*, AD 커넥터 참조).

고객사:

- **네트워크 연결:** 기업 VPN 또는 Direct Connect 엔드포인트.
- **AD DS:** 기업 AD DS.
- **MFA(선택 사항):** 기업 RADIUS 서버.
- **최종 사용자 디바이스:** Amazon WorkSpaces 서비스에 액세스하는 데 사용되는 사내 또는 BYOL 최종 사용자 디바이스(예: Windows, Mac, iPad 또는 Android 태블릿, 제로 클라이언트, Chromebook)(지원되는 플랫폼 및 디바이스 참조).

이 솔루션이 AD DS를 클라우드로 배포하지 않으려는 고객에게는 유용하지만 단점이 있습니다.

- **연결 의존도:** 데이터 센터와 연결이 끊어질 경우 사용자가 자신의 WorkSpaces에 로그인할 수 없고 기존 연결이 Kerberos/TGT 수명 동안 활성화됩니다.
- **지연 시간:** 연결을 통한 지연 시간이 존재할 경우(DX보다는 VPN에서 가능성이 더 높음), WorkSpaces 인증, 그리고 그룹 정책(GPO) 시행과 같은 AD DS 관련 작업이 더 오래 걸립니다.
- **트래픽 비용:** 모든 인증이 VPN 또는 DX 링크를 통과해야 하며, 따라서 연결 유형에 의존합니다. 유형은 Amazon EC2에서 인터넷까지의 데이터 전송 아웃바운드 또는 데이터 전송 아웃바운드(DX)입니다.

> **참고** AD 커넥터는 프록시 서비스입니다. 사용자 자격 증명을 저장 또는 캐싱하지 않습니다. 대신, 모든 인증, 조회 및 관리 요청이 Active Directory에 의해 처리됩니다. 모든 사용자 정보를 읽고 컴퓨터를 도메인에 조인시킬 수 있도록 위임 권한을 가진 계정이 디렉터리 서비스에 필요합니다.

AD 커넥터에 대해 디렉터리 내 사용자를 구성하는 방법에 대한 자세한 내용은 연결 권한 위임을 참조하십시오.

일반적으로 WorkSpaces 환경은 그림 4에 표시된 항목 5에 크게 의존합니다.

시나리오 2: 온프레미스 AD DS를 AWS로 확장(복제본).

이 시나리오는 시나리오 1과 비슷합니다. 하지만 시나리오 2에서는 고객 AD DS의 복제본이 AD 커넥터와 함께 AWS에 배포됩니다. 그러면 AD DS에 대한 인증 또는 쿼리 요청의 지연 시간이 줄어듭니다. 그림 6에는 각 구성 요소의 상위 수준 보기와 사용자 인증 흐름이 나와 있습니다.

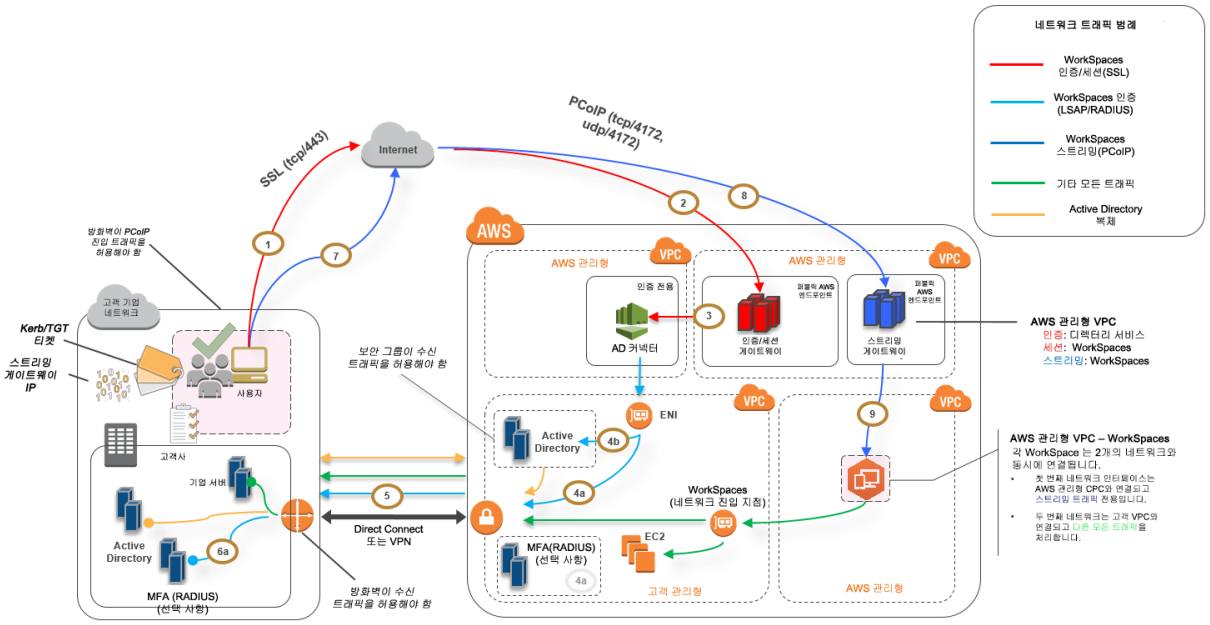

그림 6: 고객 Active Directory 도메인을 클라우드로 확장

시나리오 1에서와 같이, 모든 사용자 ㄸ또는 MFA 인증에 AD 커넥터가 사용되며, 이 인증은 고객 AD DS로 프록시됩니다(그림 5). 시나리오 2에서는 고객 AD DS가 AWS Cloud에서 실행되는 고객의 온프레미스 Active Directory 포리스트에서 도메인 컨트롤러로 승격되는 Amazon EC2 인스턴스에서 가용 영역에 걸쳐 배포됩니다. 각 도메인 컨트롤러는 VPC 프라이빗 서브넷으로 배포되어 AD DS가 AWS Cloud에서 고가용성을 유지합니다. AWS Cloud에서 AD DS를 배포하기 위한 모범 사례는 이 백서의 설계 고려 사항 을 참조하십시오.

WorkSpaces 인스턴스가 배포되면 이들은 안전하고 짧은 지연 시간의 디렉터리 서비스 및 DNS를 위해 클라우드 기반 도메인 컨트롤러에 액세스할 수 있습니다 DNS. AD DS 통신, 인증 요청 및 Active Directory 복제를 포함한 모든 네트워크 트래픽은 프라이빗 서브넷 내부에서 또는 고객 VPN 터널 또는 DX에 걸쳐 보안이 유지됩니다.

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

Amazon Web Services:

- **Amazon VPC:** 두 가용 영역에 걸쳐 최소 4개의 프라이빗 서브넷을 사용하여 Amazon VPC를 생성(2개는 고객 AD DS용이고, 2개는 AD 커넥터 또는 WorkSpaces용).
- **DHCP 옵션 세트:** Amazon VPC DHCP 옵션 세트를 생성. 이를 통해 고객이 지정한 도메인 이름 및 DNS를 정의할 수 있습니다(AD DS 로컬). 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- **Amazon 가상 프라이빗 게이트웨이:** IPsec VPN 터널 또는 AWS Direct Connect 연결을 통해 자체 네트워크와 통신을 활성화.
- **Amazon EC2:**
  - 전용 프라이빗 VPC 서브넷에서 Amazon EC2 인스턴스에 배포된 고객의 기업 AD DS 도메인 컨트롤러.
  - 고객의 MFA용 RADIUS 서버(선택 사항).
- **AWS 디렉터리 서비스:** AD 커넥터가 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- **Amazon WorkSpaces:** WorkSpaces가 AD 커넥터와 동일한 프라이빗 서브넷에 배포됩니다(*설계 고려 사항*, AD 커넥터 참조).

고객사:

- **네트워크 연결:** 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- **AD DS:** 기업 AD DS(복제를 위해 필요).
- **MFA(선택 사항):** 기업 RADIUS 서버.
- **최종 사용자 디바이스:** Amazon WorkSpaces 서비스에 액세스하는 데 사용되는 사내 또는 BYOL 최종 사용자 디바이스(예: Windows, Mac, iPad 또는 Android 태블릿, 제로 클라이언트, Chromebook)(지원되는 플랫폼 및 디바이스 참조).

시나리오 1과 달리, 이 솔루션은 동일한 단점이 없습니다. 따라서 WorkSpaces와 AWS 디렉터리 서비스는 연결 의존도가 없습니다.

- **연결 의존도:** 고객 데이터 센터와 연결이 끊어질 경우 인증 및 "선택 사항" MFA가 로컬에서 처리되므로 최종 사용자가 작업을 계속할 수 있습니다.
- **지연 시간:** 복제 트래픽(*설계 고려 사항:* AD DS 사이트 및 서비스 참조)을 제외하고 모든 인증이 로컬에서 처리되고 지연 시간이 낮습니다.
- **트래픽 비용:** 이 시나리오에서 인증은 로컬에서 처리되며 AD DS 복제만 VPN 또는 DX 링크를 통과해야 하므로 데이터 전송이 줄어듭니다.

일반적으로 WorkSpaces 환경이 향상되고 그림 6에 표시된 대로 항목 5에 크게 의존하지 않습니다. WorkSpaces를 수천 개의 데스크톱으로 확장할 때, 특히 AD DS 글로벌 카탈로그 쿼리와 관련하여 이러한 장점이 두드러집니다. 이 트래픽은 WorkSpaces 환경에 로컬로 유지되지 때문입니다.

시나리오 3: AWS Cloud에서 AWS 디렉터리 서비스를 사용한 독립형 격리형 배포

이 시나리오(그림 7)는 AD DS가 독립형 격리 배포로 AWS Cloud에 배포됩니다. AWS 디렉터리 서비스는 이 시나리오에서만 사용됩니다. AD DS를 사용자가 전적으로 관리하는 대신, 고가용성 디렉터리 토폴로지 구축, 도메인 컨트롤러 모니터링, 백업 및 스냅샷 구성과 같은 작업은 AWS 디렉터리 서비스가 처리합니다.

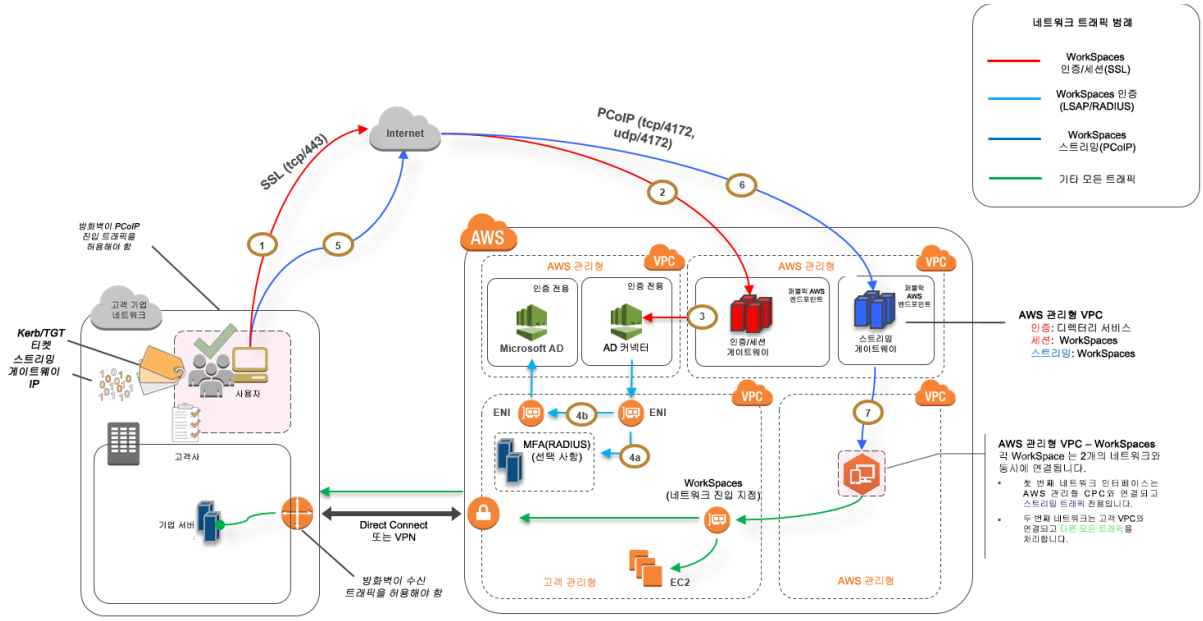

그림 7: 클라우드 전용 - AWS 디렉터리 서비스(Microsoft AD)

시나리오 2에서와 같이, AD DS(Microsoft AD)가 두 가용 영역에 걸친 전용 서브넷에 배포되어 AD DS가 AWS Cloud에서 고가용성을 유지합니다. Microsoft AD 이외에, AD 커넥터가 WorkSpaces 인증 또는 MFA용으로 배포됩니다(3개 시나리오 모두). 그러면 Amazon VPC 내에서 역할 또는 기능 분리가 보장됩니다. 이는 표준 모범 사례입니다(*설계 고려 사항*: 분할된 네트워크 단원 참조).

시나리오 3은 AWS가 AWS 디렉터리 서비스의 배포, 패칭, 고가용성 및 모니터링을 관리하기 원하는 고객에게 알맞은 표준 올인 구성입니다. 운영 이외에 격리 모드 덕분에 이 시나리오는개념 증명 및 랩 환경에도 적합합니다.

AWS 디렉터리 서비스 배치 이외에, 그림 7에는 사용자에서 WorkSpace까지의 트래픽 흐름과 WorkSpace가 어떻게 AD 서버 및 MFA 서버와 상호작용하는지 나와 있습니다.

이 아키텍처는 다음 구성 요소 또는 구조를 사용합니다.

Amazon Web Services:

- **Amazon VPC:** 두 가용 영역에 걸쳐 최소 4개의 프라이빗 서브넷을 사용하여 Amazon VPC를 생성(2개는 AD DS *Microsoft AD*용이고, 2개는 AD 커넥터 또는 WorkSpaces용). "*역할 분리*."
- **DHCP 옵션 세트:** Amazon VPC DHCP 옵션 세트를 생성. 이를 통해 고객이 지정한 도메인 이름 및 DNS를 정의할 수 있습니다(Microsoft AD). 자세한 내용은 DHCP 옵션 세트를 참조하십시오.
- **선택 사항: Amazon 가상 프라이빗 게이트웨이:** IPsec VPN 터널(VPN) 또는 AWS Direct Connect 연결을 통해 자체 네트워크와 통신을 활성화합니다. 온프레미스 백엔드 시스템 액세스를 위해 사용합니다.
- **AWS 디렉터리 서비스:** 한 쌍의 전용 VPC 서브넷에 배포된 Microsoft AD(AD DS 관리형 서비스).
- **Amazon EC2:** 고객의 MFA용 RADIUS 서버(선택 사항).
- **AWS 디렉터리 서비스**: AD 커넥터가 한 쌍의 Amazon VPC 프라이빗 서브넷에 배포됩니다.
- **Amazon WorkSpaces:** WorkSpaces가 AD 커넥터와 동일한 프라이빗 서브넷에 배포됩니다(*설계 고려 사항*, AD 커넥터 참조).

고객사:

- **선택 사항: 네트워크 연결:** 기업 VPN 또는 AWS Direct Connect 엔드포인트.
- **최종 사용자 디바이스:** Amazon WorkSpaces 서비스에 액세스하는 데 사용되는 사내 또는 BYOL 최종 사용자 디바이스(예: Windows, Mac, iPad 또는 Android 태블릿, 제로 클라이언트, Chromebook)(지원되는 플랫폼 및 디바이스 참조).

시나리오 2와 마찬가지로, 이 솔루션은 설계상 격리형 또는 클라우드 전용 시나리오이므로 고객 온프레미스 데이터 센터 연결 의존도, 지연 시간 또는 데이터 출력 전송 비용(인터넷 액세스가 VPC 내 WorkSpaces에 대해 활성화된 경우는 제외) 문제가 없습니다.

설계 고려 사항

AWS Cloud에서 AD DS 배포는 Active Directory 개념과 특정 AWS 서비스 모두에 대한 정확한 이해를 요구합니다. 이 단원에서는 WorkSpaces용 AD DS 배포 시 주요 설계 고려 사항, AWS 디렉터리 서비스에 대한 , VPC 모범 사례, DHCP 및 DNS 요구 사항, AD 커넥터 관련 사항, Active Directory 사이트 및 서비스에 대해 설명합니다.

VPC 설계

이 백서의 네트워크 고려 사항 단원에서 설명하고 시나리오 2 및 3 에서 언급했듯이, AWS Cloud 에서의 AD DS 는 AD 커넥터 또는 WorkSpaces 서브넷과 격리하여 두 가용 영역에 걸쳐 한 쌍의 전용 프라이빗 서브넷으로 배포해야 합니다. 이 구조는 WorkSpaces 용 AD DS 서비스에 대한 짧은 지연 시간의 고가용성 액세스를 제공하며 Amazon VPC 내에서 역할 또는 기능을 분리하는 표준 모범 사례를 유지합니다.

그림 8은 전용 프라이빗 서브넷에 배포된 AD DS 및 AD 커넥터의 격리를 보여줍니다(시나리오 3). 이 예에서 모든 서비스는 동일한 Amazon VPC에 상주합니다.

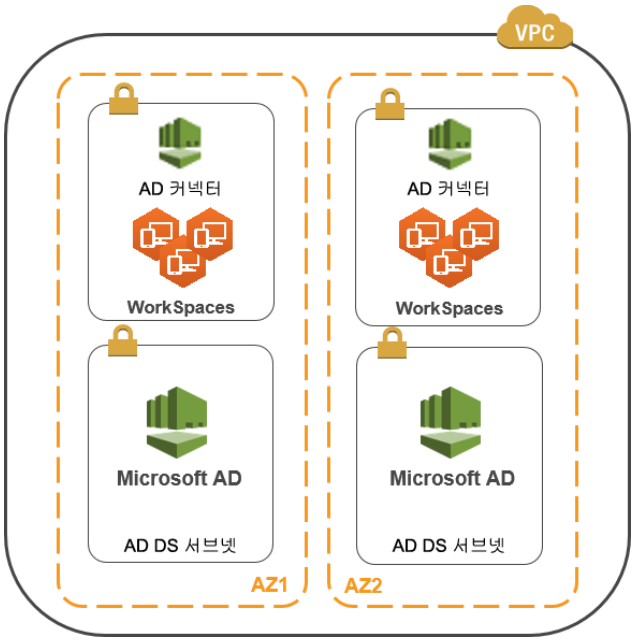

그림 8: AD DS 네트워크 격리

그림 9에는 시나리오 1과 비슷한 설계가 나와 있습니다. 하지만 이 시나리오에서는 온프레미스 부분이 전용 Amazon VPC에 상주합니다.

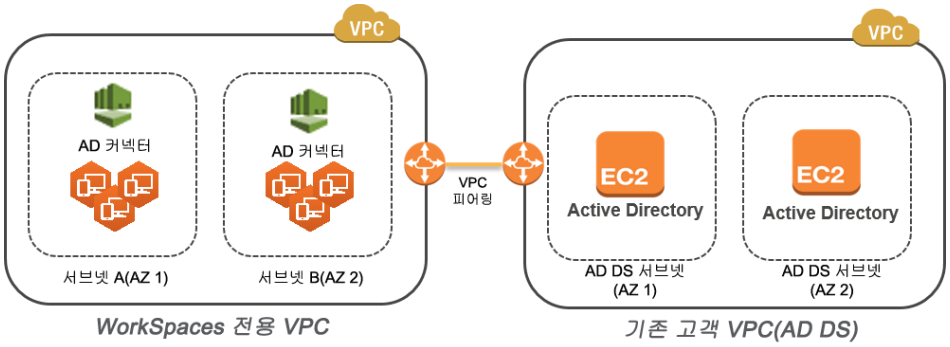

그림 9: 전용 WorkSpaces VPC

참고 기존 AWS 배포에서 AD DS를 사용 중인 고객의 경우, WorkSpaces를 전용 VPC에 배치하고 AD DS 통신에 VPC 피어링을 사용할 것을 권장합니다.

AD DS 전용 프라이빗 서브넷을 생성하는 이외에, 도메인 컨트롤러 및 멤버 서버는 AD DS 복제, 사용자 인증, Windows Time 서비스, 분산 파일 시스템(DFS)과 같은 서비스를 위한 트래픽을 허용하는 보안 그룹 규칙을 필요로 합니다.

참고 모범 사례는 필요한 보안 그룹 규칙을 WorkSpaces 프라이빗 서브넷으로 제한하는 것이고, 시나리오 2의 경우 다음 표에 표시된 대로 온프레미스에서 AWS Cloud와 양방향 AD DS 통신을 허용하는 것입니다.

프로토콜	포트	사용	대상
tcp	53, 88, 135, 139, 389, 445, 464, 636	인증(주)	Active Directory (사설 데이터 센터 또는 EC2)*
tcp	49152 – 65535	RPC High 포트	Active Directory (사설 데이터 센터 또는 EC2)**
tcp	3268-3269	트러스트	Active Directory (사설 데이터 센터 또는 EC2)*
tcp	9389	원격 Microsoft Windows PowerShell (선택 사항)	Active Directory (사설 데이터 센터 또는 EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	인증(주)	Active Directory (사설 데이터 센터 또는 EC2)*
udp	1812	인증(MFA) (선택 사항)	RADIUS (사설 데이터 센터 또는 EC2)*

* Active Directory 및 Active Directory 도메인 서비스 포트 요구 사항 참조

** 서비스 개요 및 Windows용 네트워크 포트 요구 사항 참조

규칙 구현을 위한 단계별 지침은 *Amazon Elastic Compute Cloud 사용 설명서*에서 보안 그룹에 규칙 추가를 참조하십시오.

VPC 설계: DHCP 및 DNS

Amazon VPC에서는 DHCP 서비스가 인스턴스에 대해 기본으로 제공됩니다. 기본적으로, 모든 VPC는 CIDR(Classless Inter-Domain Routing) +2 주소 공간을 통해 액세스할 수 있고 기본 DHCP 옵션 세트를 통해 모든 인스턴스에 할당되는 내부 DNS 서버를 제공합니다.

DHCP 옵션 세트는 Amazon VPC에서 DHCP를 통해 인스턴스로 전달되어야 하는 도메인 이름 또는 이름 서버와 같은 범위 옵션을 정의하는 데 사용됩니다. Windows 서비스가 VPC에서 올바로 기능하기 위해서는 이 DHCP 범위 옵션이 필요하므로 해당 옵션을 정확하게 설정해야 합니다. 앞서 정의된 각 시나리오에서 도메인 이름 및 이름 서버를 정의하는 범위를 설정하고 할당합니다. 그러면 도메인에 조인된 Windows 인스턴스 또는 WorkSpaces가 Active Directory DNS를 사용하도록 구성됩니다. 다음 표는 WorkSpaces 및 AWS 디렉터리 서비스가 올바로 기능하려면 생성되어야 하는 사용자 지정 DHCP 범위 옵션 세트의 예입니다.

파라미터	값
Name tag	키 = **name**이고 **value**가 특정 문자열로 설정된 태그를 생성합니다. 예: exampleco. com
Domain name	exampleco. com
Domain name servers	DNS 서버 주소(쉼표로 구분) 예: 10. 0. 0. 10, 10. 0. 1. 10
NTP servers	이 필드는 공란으로 둡니다.
NetBIOS name servers	도메인 이름 서버와 동일한 쉼표로 구분된 IP를 입력합니다. 예: 10. 0. 0. 10, 10. 0. 1. 10
NetBIOS node type	2

사용자 지정 DHCP 옵션 세트를 생성하여 Amazon VPC와 연결하는 방법에 대한 자세한 내용은*Amazon Virtual Private Cloud 사용 설명서*에서 DHCP 옵션 세트를 사용한 작업을 참조하십시오.

시나리오 1에서 DHCP 범위는 온프레미스 DNS 또는 AD DS가 됩니다. 하지만 시나리오 2 또는 3에서는 이 범위가 로컬에 배포된 디렉터리 서비스가 됩니다(Amazon EC2 상의 AD DS 또는 AWS 디렉터리 서비스: Microsoft AD). AWS Cloud에 상주하는 각 도메인 컨트롤러를 글로벌 카탈로그 및 디렉터리 통합 DNS 서버로 만드는 것이 좋습니다.

Active Directory: 사이트 및 서비스

시나리오 2의 경우, 사이트 및 서비스는 AD DS가 올바로 기능하기 위해 중요한 구성 요소입니다. 사이트 토폴로지는 동일한 사이트 내부의 그리고 사이트 경계에 걸친 도메인 컨트롤러 간 Active Directory 복제를 제어합니다. 시나리오 2에서는 온프레미스 및 클라우드 내 AWS WorkSpaces 등 적어도 2개의 사이트가 존재합니다. 올바른 사이트 토폴로지를 정의하면 클라이언트 선호도가 보장됩니다. 즉, 클라이언트(이 경우 WorkSpaces)가 선호하는 로컬 도메인 컨트롤러를 사용합니다.

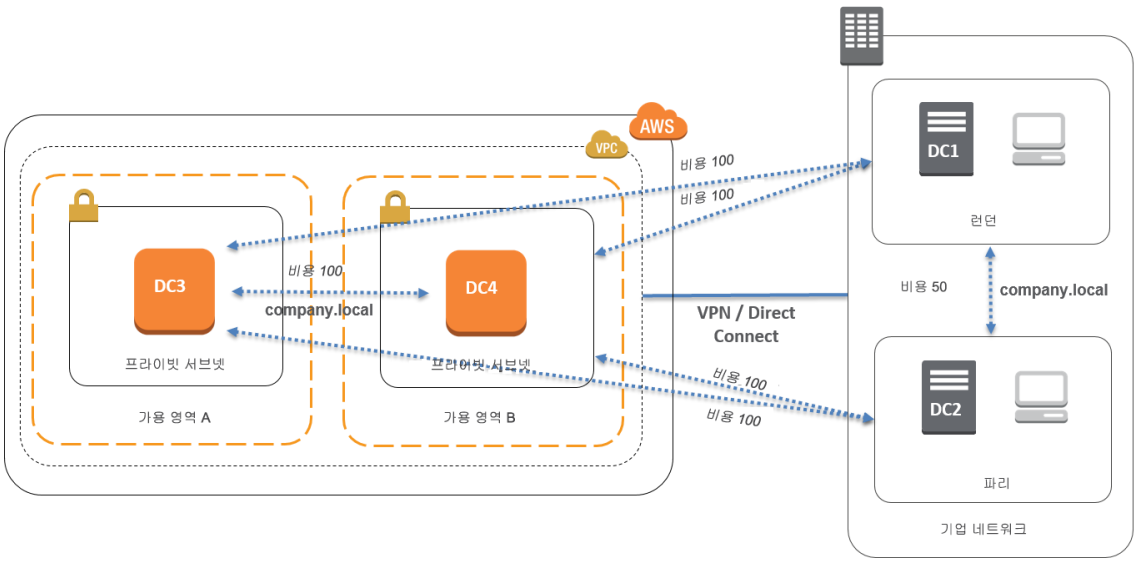

그림 10: Active Directory 사이트 및 서비스: 클라이언트 선호도

모범 사례 온프레미스 AD DS와 AWS Cloud 사이에 높은 비용의 사이트 링크를 정의하십시오. 그림 10은 사이트 독립적 클라이언트 선호도를 보장하기 위해 사이트 링크에 할당해야 하는 비용의 예입니다(비용 100).

이러한 연결은 AD DS 복제, 클라이언트 인증과 같은 트래픽이 도메인 컨트롤러까지 가장 효율적 경로를 사용하도록 해줍니다. 시나리오 2 및 3의 경우, 이는 지연 시간을 더 단축하고 교차 링크 트래픽을 보장합니다.

멀티 팩터 인증(MFA)

MFA를 구현하려면 WorkSpaces 인프라가 AWS 디렉터리 서비스로 AD 커넥터를 사용해야 하고 RADIUS 서버를 포함해야 합니다. 이 백서에서는 RADIUS 서버 배포에 대해 설명하지는 않지만 앞 단원AD DS 배포 시나리오에 시나리오별 RADIUS 배치에 대해 자세히 설명되어 있습니다.

MFA – 2팩터 인증

Amazon WorkSpaces는 AWS 디렉터리 서비스: AD 커넥터 및 *고객 소유* RADIUS 서버를 통한 MFA를 지원합니다. 이 인증이 활성화되면 사용자는 WorkSpaces 데스크톱 인증을 위해 **사용자 이름, 암호** 및 **MFA 코드**를 제공해야 합니다.

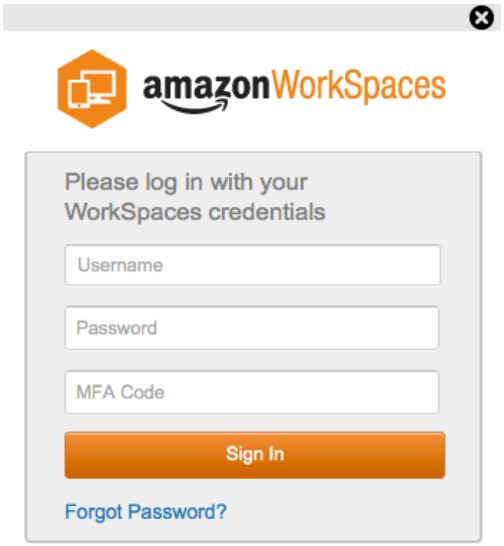

그림 11: MFA를 사용하는 WorkSpaces 클라이언트

필수 규칙 MFA 인증을 구현하려면 AD 커넥터를 사용해야 합니다. AD 커넥터는 선택적 "사용자별" MFA를 지원하지 않습니다. MFA가 전역 AD 커넥터별 설정이기 때문입니다. 선택적 "사용자별" MFA가 필요할 경우 AD 커넥터별로 사용자를 구분해야 합니다.

WorkSpaces MFA는 1대 이상의 RADIUS 서버를 필요로 합니다. 일반적으로 RSA와 같은 기존 솔루션이 있거나, 서버를 VPC 내에서 배포할 수 있습니다(AD DS 배포 시나리오 참조). 새 RADIUS 솔루션을 배포하는 경우 예를 들어 FreeRADIUS, 그리고 Duo Security와 같은 클라우드 서비스 등 다양한 구현이 출시되어 있습니다.

Amazon WorkSpaces에서 MFA를 구현하기 위한 전제 조건의 목록은 *Amazon WorkSpaces Administration Guide*, Preparing Your Network for an AD Connector Directory를 참조하십시오. MFA용 AD 커넥터를 구성하는 프로세스는 *Amazon WorkSpaces Administration Guide*의 Managing an AD Connector Directory: Multi-factor Authentication에 설명되어 있습니다.

보안

이 단원에서는 Amazon WorkSpaces 서비스를 사용할 때 암호화를 통해 데이터를 보호하는 방법을 설명합니다. 전송 시 및 저장 시 암호화, 그리고 보안 그룹을 사용하여 WorkSpaces에 대한 네트워크 액세스 보호를 설명합니다. 인증(MFA 지원 포함)에 대한 자세한 내용은 AWS 디렉터리 서비스 단원에서 확인할 수 있습니다.

전송 시 암호화

Amazon WorkSpaces는 암호화 기법을 사용하여 통신(전송 시)의 각 단계에서 기밀성을 보호하며 저장된 데이터도 보호합니다(암호화된 WorkSpaces). Amazon WorkSpaces가 전송 시 사용하는 각 암호화 단계의 프로세스는 다음 단원에서 설명합니다. 저장 시 암호화에 대한 자세한 내용은 나중에 나오는 암호화된 WorkSpaces 단원을 참조하십시오.

등록 및 업데이트

데스크톱 클라이언트 애플리케이션은 업데이트 및 등록을 위해 https를 사용하여 Amazon과 통신합니다.

인증 단계

데스크톱 클라이언트는 인증 게이트웨이로 자격 증명을 전송하여 인증을 시작합니다. 데스크톱 클라이언트와 인증 게이트웨이 간 통신은 https를 사용합니다. 이 단계의 끝에서 인증이 성공하면 인증 게이트웨이가 동일한 https 연결을 통해 OAuth 2. 0 토큰을 데스크톱 클라이언트로 반환합니다.

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

클라이언트로부터 자격 증명을 수신하면 인증 게이트웨이가 인증 요청을 AWS 디렉터리 서비스로 전송합니다. 인증 게이트웨이에서 AWS 디렉터리 서비스까지 통신은 HTTPS를 통해 이루어지며, 따라서 사용자 자격 증명이 클리어 텍스트로 전송되지 않습니다.

인증 - AD 커넥터

AD 커넥터는 Kerberos를 사용하여 온프레미스 AD와 인증된 통신을 설정하며, 따라서 LDAP로 바인딩하고 이후의 LDAP 쿼리를 실행할 수 있습니다. 이 시점에서는 AWS 디렉터리 서비스는 TLS(LDAPs)를 포함한 LDAP를 지원하지 않습니다. 하지만 어느 시점에도 사용자 자격 증명은 클리어 텍스트로 전송되지 않습니다. 강화된 보안을 위해 VPN 연결을 사용하여 WorkSpaces VPC를 온프레미스 네트워크(AD가 상주하는 위치)에 연결하는 것이 가능합니다. AWS 하드웨어 VPN 연결을 사용할 때 AES-128 또는 AES-256 대칭 암호화 키를 사용하는 표준 IPSEC(IKE 및 IPSEC SAs), 무결성 해시를 위해 SHA-1 또는 SHA-256, 및 PFS를 사용하는 DH 그룹(1단계는 2,14-18, 22, 23 및 24, 2단계는 1,2,5, 14-18, 22, 23 및 24)을 사용하여 전송 중에 암호화를 설정하게 됩니다.

브로커 단계

OAuth 2. 0 토큰을 수신한 후(인증 성공 시 인증 게이트웨이로부터) 데스크톱 클라이언트가 HTTPS를 사용하여 Amazon WorkSpaces 서비스(브로커 연결 관리자)로 쿼리합니다. 데스크톱 클라이언트는 OAuth 2. 0 토큰을 전송하여 자체 인증하고, 그 결과로 클라이언트가 WorkSpaces 스트리밍 게이트웨이의 엔드포인트 정보를 수신합니다.

스트리밍 단계

데스크톱 클라이언트가 스트리밍 게이트웨이에 PCoIP 세션 개설을 요청합니다(OAuth 2. 0 토큰을 사용). 이 세션은 aes256 암호화되고 통신 제어를 위해 PCoIP 포트를 사용합니다(즉 4172/tcp).

OAuth2. 0 토큰을 사용하여 스트리밍 게이트웨이가 https를 통해 WorkSpaces 서비스로부터 사용자별 WorkSpaces 정보를 요청합니다.

또한 스트리밍 게이트웨이는 클라이언트로부터 TGT를 수신하고(클라이언트 사용자 암호를 사용하여 암호화됨) Kerberos TGT 패스스루를 사용하여 게이트웨이가 수신된 사용자 Kerberos TGT를 사용하여 WorkSpace에서 Windows 로그인을 시작합니다.

그러면 WorkSpace가 표준 Kerberos 인증을 사용하여 구성된 AWS 디렉터리 서비스에 인증을 요청합니다.

WorkSpace가 성공적으로 로그인되면 PCoIP 스트리밍이 시작됩니다. 클라이언트가 포트 tcp 4172에서 이 연결을 시작하고 리턴 트래픽은 포트 udp 4172를 사용합니다. 또한, 스트리밍 게이트웨이와 WorkSpaces 데스크톱 사이의 관리 인터페이스를 통한 초기 통신은 UDP 55002를 사용합니다. (Amazon Workspaces 설명서, Amazon WorkSpaces Details를 참조하십시오. 초기 아웃바운드 UDP 포트는 55002입니다.) 포트 4172(tcp 및 udp)를 사용하는 스트리밍 연결은 AES 128비트 및 256비트 암호를 사용하여 암호화되지만 기본값은 128비트입니다. PCoIP 고유 Active Directory GPO를 통해 이 값을 256비트로 변경할 수 있습니다(pcoip. adm).

네트워크 인터페이스

각 Amazon WorkSpace는 주 네트워크 인터페이스 및 관리 네트워크 인터페이스라고 하는 2개 네트워크 인터페이스를 가집니다.

주 네트워크 인터페이스는 AWS 디렉터리 서비스, 인터넷 및 사내 네트워크와 같은 VPC 내부 리소스에 대한 연결을 제공합니다. 이 주 네트워크 인터페이스에 보안 그룹을 연결할 수 있습니다(ENI와 마찬가지). 개념상으로는 배포 범위를 기준으로 이 ENI에 연결된 보안 그룹을 WorkSpaces 보안 그룹과 ENI 보안 그룹으로 구분합니다.

관리 네트워크 인터페이스

관리 네트워크 인터페이스는 보안 그룹을 통해 제어할 수 있습니다. 하지만 WorkSpace에서 호스트 기반 방화벽을 사용하여 포트 또는 제어 액세스를 차단할 수 있습니다. 관리 네트워크 인터페이스에 제한을 적용하는 것은 권장하지 않습니다. 이 인터페이스를 관리하기 위해 호스트 기반 방화벽을 추가하기로 한 경우 WorkSpaces 서비스가 Amazon WorkSpaces Administration Guide에 정의된 대로 상태 및 WorkSpace 접근성을 관리할 수 있도록 몇몇 포트를 개방해두어야 합니다.

WorkSpaces 보안 그룹

기본 보안 그룹은 AWS 디렉터리 서비스별로 생성되며 지정된 디렉터리에 속하는 모든 WorkSpaces에 자동으로 연결됩니다.

다른 보안 그룹과 마찬가지로, WorkSpaces 보안 그룹의 규칙을 수정할 수 있습니다. 변경 사항은 적용 즉시 효력을 발휘합니다.

WorkSpaces 보안 그룹 연결을 변경하여 AWS 디렉터리 서비스에 연결된 기본 WorkSpaces 보안 그룹을 변경할 수 있습니다.

> **참고** 새로 연결된 보안 그룹은 수정 이후 생성 또는 재구축된 WorkSpaces에만 연결됩니다.

ENI 보안 그룹

주 네트워크 인터페이스는 일반 ENI이므로 다른 AWS 관리 도구를 사용하여 그 구성을 관리할 수 있습니다(Elastic Network Interfaces(ENI) 참조). 특히, WorkSpace IP를 조회하여(Amazon WorkSpaces 콘솔의 WorkSpaces 페이지에서) IP 주소를 필터로 사용하여 해당 ENI를 찾습니다(Amazon EC2 콘솔의 네트워크 인터페이스 섹션에서).

ENI를 찾으면 해당 위치에서 직접 보안 그룹을 관리할 수 있습니다. 수동으로 주 네트워크 인터페이스에 보안 그룹을 할당할 때는 Amazon WorkSpaces 세부 정보에 설명된 Amazon WorkSpaces 포트 요구 사항을 고려하십시오.

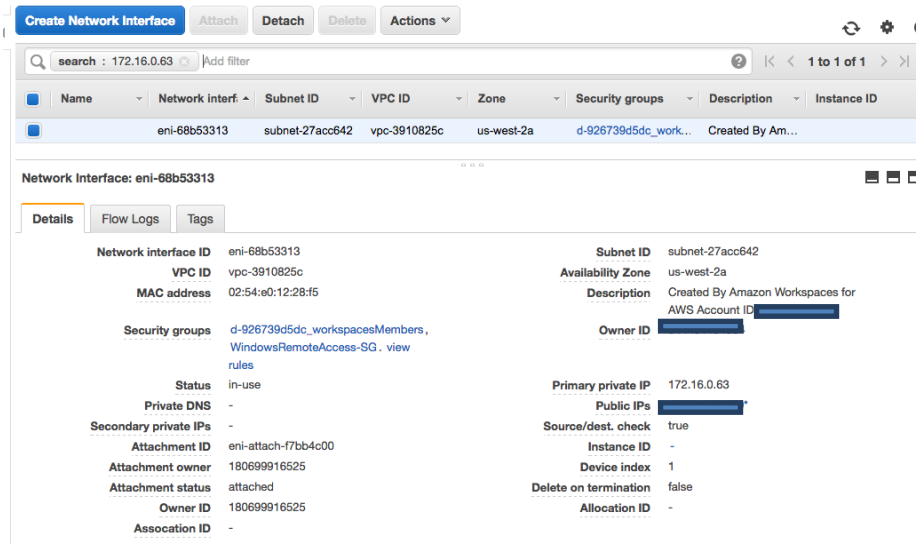

그림 12: 보안 그룹 연결 관리

암호화된 WorkSpaces

각 Amazon WorkSpace는 루트 볼륨(C: 드라이브) 및 사용자 볼륨(D: 드라이브)와 함께 프로비저닝됩니다. 암호화된 WorkSpaces 기능은 한 볼륨 또는 양쪽 볼륨 모두를 암호화할 수 있습니다.

암호화 대상

저장된 데이터, 볼륨과의 디스크 I/O, 암호화된 볼륨에서 생성된 스냅샷이 모두 암호화됩니다.

암호화 시점

WorkSpace를 실행(생성)할 때 WorkSpace 암호화를 지정해야 합니다. WorkSpaces 볼륨은 실행 시에만 암호화될 수 있고 실행 후에는 볼륨의 암호화 상태를 변경할 수 없습니다. 그림 13에는 새 WorkSpace 실행 시 암호화를 선택하기 위한 Amazon WorkSpaces 콘솔 페이지가 나와 있습니다.

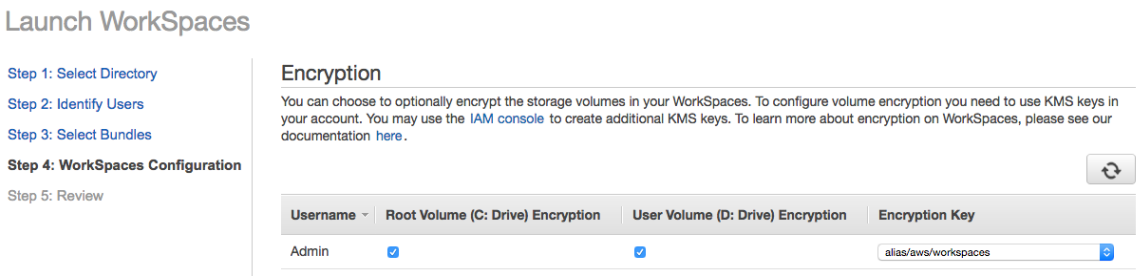

그림 13: WorkSpaces 볼륨 암호화

새 WorkSpace가 암호화되는 방식

새 WorkSpace를 실행하는 시점에 Amazon WorkSpaces 콘솔 또는 AWS CLI로부터 또는 Amazon WorkSpaces API를 사용하여 암호화된 WorkSpaces 옵션을 선택할 수 있습니다.

볼륨을 암호화하기 위해 Amazon WorkSpaces는 AWS Key Management Service(KMS)로부터 고객 마스터 키(CMK)를 사용합니다. 특정 리전에서 WorkSpace가 처음 실행될 때 기본 AWS KMS CMK가 생성됩니다(CMK는 리전 범위를 가짐). 고객 관리형 CMK를 생성하여 암호화된 WorkSpaces에서 사용할 수도 있습니다. CMK는 Amazon WorkSpaces 서비스가 볼륨을 암호화하는 데 사용하는 데이터 키를 암호화하는 데 사용됩니다(엄격한 의미에서는 Amazon Elastic Block Store(Amazon EBS) 서비스가 볼륨을 암호화하는 것임). 각 CMK를 사용하여 최대 30개 WorkSpaces의 키를 암호화합니다.

> **참고** 암호화된 WorkSpaces로부터 사용자 지정 이미지 생성은 현재 지원되지 않습니다. 또한 루트 볼륨 암호화를 설정하여 실행된 WorkSpaces는 프로비저닝까지 최대 1시간이 걸릴 수 있습니다.

WorkSpaces 암호화 프로세스에 대한 자세한 설명은 AWS KMS를 사용한 Amazon WorkSpaces 암호화 개요 단원을 참조하십시오. AWS KMS 고객 마스터 키 및 데이터 키에 대한 자세한 내용은 AWS Key Management Service Concepts를 참조하십시오.

Amazon CloudWatch를 사용한 모니터링 또는 로깅

모니터링은 네트워크, 서버 또는 로그 등 모든 인프라의 핵심 부분입니다. Amazon WorkSpaces를 배포하는 고객은 특히 개별 WorkSpaces의 전반적 상태 및 연결 상태 등 배포를 모니터링해야 합니다.

WorkSpaces용 Amazon CloudWatch 측정치

WorkSpaces용 CloudWatch 측정치는 관리자가 개별 WorkSpaces의 전반적 상태 및 연결 상태를 파악할 수 있게 해줍니다. 측정치는 WorkSpace별로 제공되거나 지정된 디렉터리 내 특정 조직의 모든 WorkSpaces에 대해 집계됩니다(*AD 커넥터, ID 참조*).

모든 CloudWatch 측정치와 마찬가지로 이들 측정치도 CloudWatch API를 통해 액세스하는 AWS Management Console(그림 13)에서 확인하고 CloudWatch 경보 및 타사 도구를 통해 모니터링할 수 있습니다.

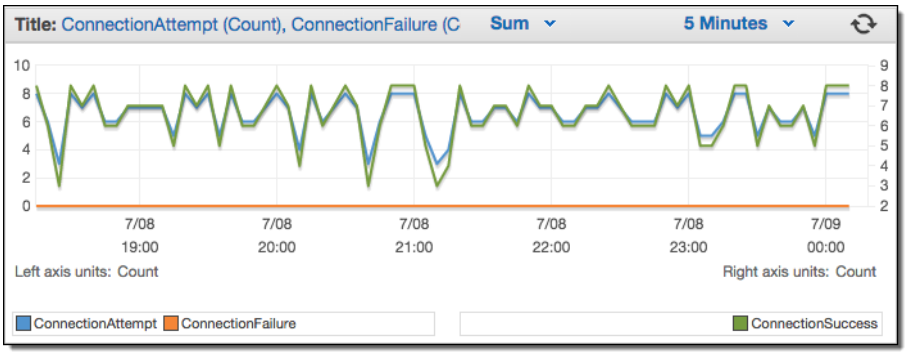

그림 14: CloudWatch 측정치 – ConnectionAttempt/ConnectionFailure

기본적으로 다음 측정치가 활성화되며 추가 비용 없이 제공됩니다.

- **Available**: 상태 검사에 응답하지 않는 WorkSpaces 수.
- **Unhealthy**: 동일한 상태 검사에 응답하지 않는 WorkSpaces 수.
- **ConnectionAttempt**: WorkSpace에 대한 연결 시도 횟수.
- **ConnectionSuccess**: 성공한 연결 시도 횟수.

- **ConnectionFailure**: 실패한 연결 시도 횟수.
- **SessionLaunchTime**: 세션 시작에 소요된 시간(WorkSpaces 클라이언트가 측정).
- **InSessionLatency**: WorkSpaces 클라이언트와 WorkSpaces 간 왕복 시간(클라이언트가 측정 및 보고).
- **SessionDisconnect**: 사용자가 시작하고 자동으로 종료한 세션 수.

또한 그림 15에 표시된 대로 경보를 생성할 수 있습니다.

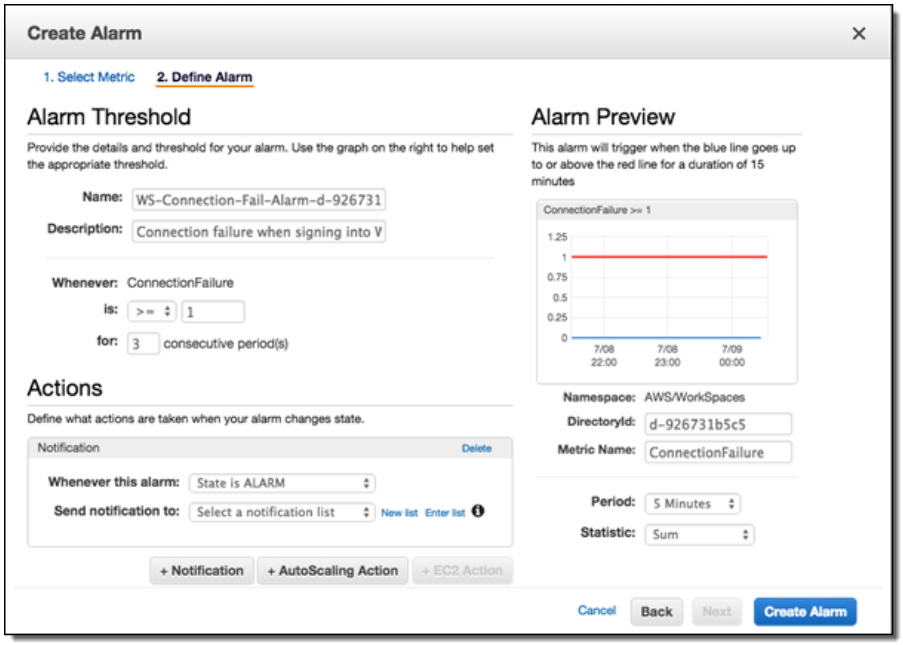

그림 15: WorkSpaces 연결 오류 시 CloudWatch 경보 생성

문제 해결

"Your device is not able to connect to the WorkSpaces Registration service" 또는 "Can't connect to a WorkSpace with an interactive logon banner" 오류 메시지와 같은 일반적인 관리 및 클라이언트 문제는 *Amazon WorkSpaces Administration Guide*의 클라이언트 및 관리 문제 해결 페이지에서 확인할 수 있습니다.

AD 커넥터가 Active Directory에 연결할 수 없음

AD 커넥터가 온프레미스 디렉터리에 연결하려면 온프레미스 네트워크 방화벽이 VPC 내 두 서브넷의 CIDR에 대해 특정 포트를 개방해야 합니다(AD 커넥터 참조). 이러한 조건이 충족되는지 테스트하려면 다음 단계를 수행하십시오.

연결을 확인하려면

1. VPC에서 Windows 인스턴스를 실행하고 RDP를 통해 연결합니다. VPC 인스턴스에서 나머지 단계를 수행합니다.
2. DirectoryServicePortTest 테스트 애플리케이션을 다운로드하여 압축을 해제합니다. 소스 코드 및 Visual Studio 프로젝트 파일이 포함되어 있으므로 원할 경우 테스트 애플리케이션을 수정할 수 있습니다.
3. Windows 명령 프롬프트에서 다음 옵션을 사용하여 DirectoryServicePortTest 테스트 애플리케이션을 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 전체 주소 도메인 이름입니다. 도메인 이름을 제외하면 기능 수준이 테스트되지 않습니다.

<*server_IP_address*>

온프레미스 도메인에 포함된 도메인 컨트롤의 IP 주소입니다. 포트가 이 IP 주소에 대해 테스트됩니다. IP 주소를 제외하면 포트가 테스트되지 않습니다.

이는 필요한 포트가 VPC에서 도메인에 대해 개방되어 있는지 여부를 확인합니다. 또한 테스트 앱은 최소 포리스트 및 도메인 기능 수준도 테스트합니다.

가장 가까운 AWS 리전까지 지연 시간을 점검하는 방법

2015년 10월, Amazon WorkSpaces는 연결 상태 점검 웹 사이트를 개설했습니다. 이 웹사이트는 사용자가 WorkSpaces를 사용하기 위해 필요한 모든 서비스에 액세스할 수 있는지 빠르게 확인합니다. 또한 WorkSpaces가 실행되는 각 AWS 리전에 대해 성능 점검을 수행하고 가장 빠른 리전을 사용자에게 알려줍니다.

결론

기업이 민첩성을 제고하고 데이터 보호를 강화하고 직원 생산성 향상을 지원하기 위해 노력함에 따라 AWS는 최종 사용자 컴퓨팅에서 전략적 변화를 예상하고 있습니다. 이미 클라우드 컴퓨팅으로 실현된 수많은 혜택이 최종 사용자 컴퓨팅에도 적용됩니다. Amazon WorkSpaces를 사용하여 데스크톱을 AWS Cloud로 이전함으로써, 기업은 직원 증가에 따라 신속하게 확장하고 데이터를 디바이스에서 분리함으로써 보안 태세를 강화하고 직원에게 어디에서든 원하는 디바이스에서 액세스할 수 있는 휴대용 데스크톱을 제공할 수 있습니다.

Amazon WorkSpaces는 기존 IT 시스템 및 프로세스와 통합되도록 설계되었으며 이 백서는 이를 위한 모범 사례를 제시합니다. 이 백서에 수록된 지침을 따르면 AWS 글로벌 인프라 상에서 비즈니스와 함께 확장되는 비용 효과적인 클라우드 데스크톱 배포를 구현할 수 있을 것입니다.

기고자

다음은 이 백서의 작성에 도움을 준 개인입니다.

- Justin Bradley, 솔루션 아키텍트, Amazon Web Services

- Mahdi Sajjadpour, 시니어 컨설턴트, AWS Professional Services
- Mauricio Munoz, 솔루션 아키텍트, Amazon Web Services

참고 문헌

자세한 내용은 다음을 참조하십시오.

- Troubleshooting AWS Directory Service Administration Issues
- Troubleshooting Amazon WorkSpaces Administration Issues
- Troubleshooting Amazon WorkSpaces Client Issues
- Amazon WorkSpaces Administration Guide
- Amazon WorkSpaces Developer Guide
- Supported Platforms and Devices
- How Amazon WorkSpaces Uses AWS KMS
- AWS CLI Command Reference – workspaces
- Monitoring Amazon WorkSpaces Metrics