aws

관리 설명서

아마존 WorkSpaces

아마존 WorkSpaces: 관리 설명서

Table of Contents

아마존이란 WorkSpaces 무엇입니까?

Amazon을 WorkSpaces 사용하면 사용자에게 가상의 클라우드 기반 Microsoft Windows, Amazon Linux 또는 Ubuntu Linux 데스크톱 (일명) 을 프로비저닝할 수 있습니다. WorkSpaces WorkSpaces 하드웨어를 조달 및 배포하거나 복잡한 소프트웨어를 설치할 필요가 없습니다. 필요에 따라 신속하게 사용자를 추가 또는 제거할 수 있습니다. 사용자는 여러 디바이스 또는 웹 브라우저에서 가상 데스크톱에 액세스할 수 있습니다.

자세한 내용은 Amazon을 참조하십시오 WorkSpaces.

특성

- 운영 체제(Windows, Amazon Linux, Ubuntu Linux)를 선택하고 다양한 하드웨어 구성, 소프트웨어 구성 및 AWS 리전 중에서 선택합니다. 자세한 내용은 Amazon WorkSpaces 번들 및 the section called “사용자 지정 이미지 및 번들 생성” 을 참조하십시오.
- 프로토콜 선택: PCoIP 또는 WorkSpaces 스트리밍 프로토콜 (WSP). 자세한 설명은 아마존용 프로토콜 WorkSpaces 섹션을 참조하세요.
- 에 WorkSpace 연결하고 중단한 부분부터 다시 시작할 수 있습니다. WorkSpaces지속적인 데스크톱 환경을 제공합니다.
- WorkSpaces 월별 또는 시간별 청구의 유연성을 제공합니다 WorkSpaces. 자세한 내용은 WorkSpaces 요금을 참조하십시오.
- Windows 데스크톱의 경우 기존 보유 라이선스 및 애플리케이션을 사용하거나 데스크톱 앱용 AWS Marketplace에서 구매합니다.
- 사용자를 위한 독립형 관리형 디렉터리를 만들거나 온-프레미스 디렉터리에 연결하여 사용자가 기존 자격 증명을 사용하여 회사 리소스에 원활하게 액세스할 수 있도록 하세요. WorkSpaces 자세한 설명은 디렉터리 섹션을 참조하세요.
- 온프레미스 데스크톱을 관리하는 WorkSpaces 데 사용하는 것과 동일한 도구를 사용하여 관리하세요.
- 강화된 보안을 위해 멀티 팩터 인증(MFA)을 사용합니다.
- AWS Key Management Service(AWS KMS)을(를) 사용하여 저장 시 데이터, 디스크 I/O 및 볼륨 스냅샷을 암호화합니다.
- 사용자가 액세스할 수 있는 IP 주소를 제어합니다. WorkSpaces

아키텍처

Windows 및 WorkSpaces Linux의 경우 WorkSpace 각각은 가상 사설 클라우드 (VPC) 및 사용자 및 사용자에 대한 정보를 저장하고 관리하는 WorkSpaces 디렉토리와 연결됩니다. 자세한 설명은 the section called “VPC 요구 사항” 섹션을 참조하세요. 디렉터리는 AWS Directory Service을(를) 통해 관리되는데, 이는 Simple AD, AD Connector 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service 등의 옵션을 제공합니다. 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요.

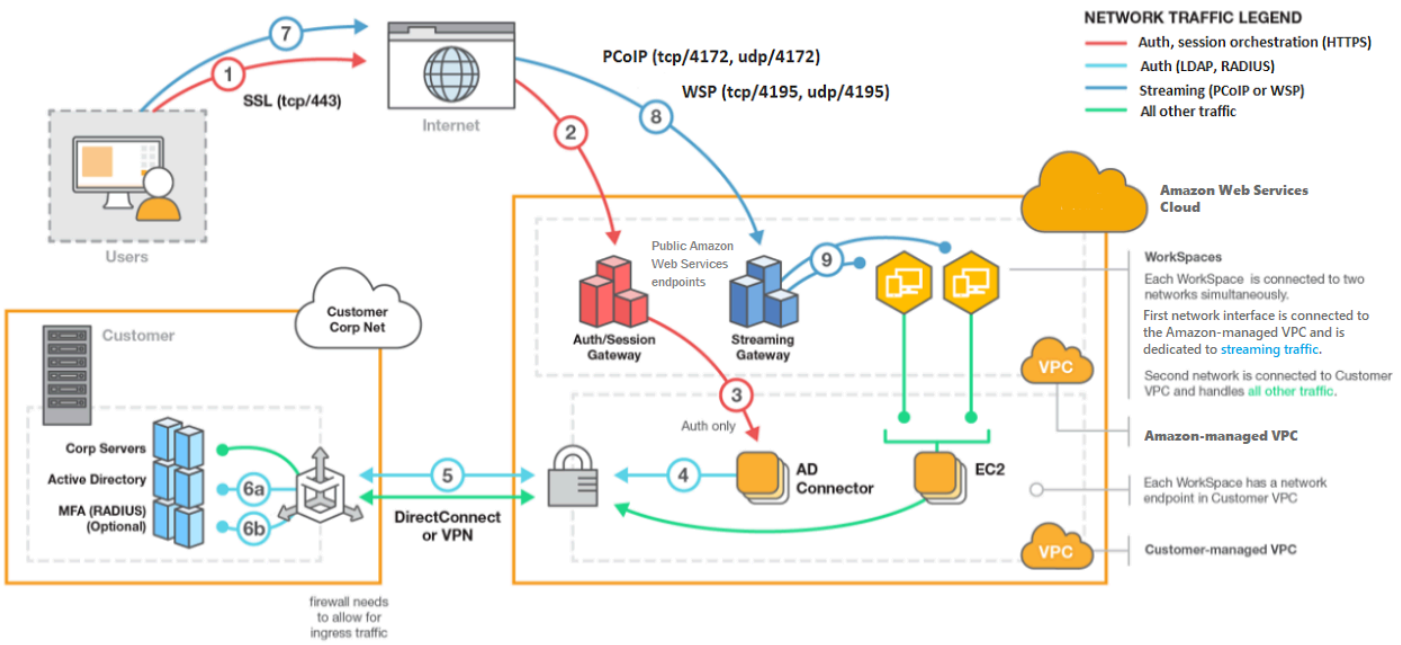
WorkSpaces Simple AD, AD Connector 또는 AWS 관리형 Microsoft AD 디렉터리를 사용하여 사용자를 인증합니다. 사용자는 지원되는 장치에서 클라이언트 애플리케이션을 사용하거나 WorkSpaces Windows의 경우 웹 브라우저를 사용하여 해당 WorkSpaces 디바이스에 액세스하고 디렉터리 자격 증명을 사용하여 로그인합니다. 로그인 정보는 인증 게이트웨이로 전송되며, 인증 게이트웨이는 트래픽을 의 디렉터리로 전달합니다. WorkSpace 사용자가 인증되면 스트리밍 게이트웨이를 통해 스트리밍 트래픽이 시작됩니다.

클라이언트 애플리케이션은 모든 인증 및 세션 관련 정보에 포트 443을 통해 HTTPS를 사용합니다. 클라이언트 애플리케이션은 포트 4172 (PCoIP) 와 포트 4195 (WSP) 를 사용하여 픽셀 스트리밍을 하고, 포트 4172 WorkSpace 및 4195를 사용하여 네트워크 상태를 확인합니다. 자세한 설명은 클라이언트 애플리케이션을 위한 포트 섹션을 참조하세요.

각 WorkSpace 인터페이스에는 관리 및 스트리밍을 위한 네트워크 인터페이스 (eth0) 와 기본 네트워크 인터페이스 (eth1) 라는 두 개의 탄력적 네트워크 인터페이스가 연결되어 있습니다. 기본 네트워크 인터페이스에는 디렉터리에서 사용하는 서브넷으로부터의 IP 주소가 VPC에 의해 제공됩니다. 이렇게 하면 사용자의 트래픽이 디렉터리에 쉽게 WorkSpace 도달할 수 있습니다. VPC 내 리소스에 대한 액세스는 기본 네트워크 인터페이스에 할당된 보안 그룹을 통해 제어됩니다. 자세한 설명은 네트워크 인터페이스 섹션을 참조하세요.

다음 다이어그램은 의 아키텍처를 보여줍니다 WorkSpaces.

Amazon WorkSpaces Architectural Diagram



액세스 WorkSpace

지원되는 운영 체제에서 지원되는 웹 브라우저를 사용하여 지원되는 장치의 클라이언트 애플리케이션을 사용하여 서버에 연결할 수 있습니다. WorkSpaces

> **Note**
>
> 웹 브라우저를 사용하여 Amazon Linux에 연결할 수는 없습니다 WorkSpaces.

다음 디바이스의 클라이언트 애플리케이션이 지원됩니다.

- Windows 컴퓨터
- macOS 컴퓨터
- Ubuntu Linux 18.04 컴퓨터
- Chromebook
- iPad
- Android 디바이스
- Fire 태블릿

- 제로 클라이언트 디바이스(Teradici 제로 클라이언트 디바이스는 PCoIP에서만 지원됨)

Windows, macOS 및 Linux PC에서는 다음 웹 브라우저를 사용하여 Windows 및 Ubuntu Linux에 연결할 수 있습니다. WorkSpaces

- Chrome 53 이상(Windows 및 macOS만 해당)
- Firefox 49 이상

자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces 클라이언트를 참조하십시오.

요금

가입한 후에는 프리 티어 혜택을 사용하여 WorkSpaces 무료로 시작할 수 있습니다. AWS WorkSpaces 자세한 내용은 WorkSpaces 요금을 참조하십시오.

WorkSpaces를 사용하면 사용한 만큼만 비용을 지불하면 됩니다. 번들 및 출시한 번들 수에 WorkSpaces 따라 요금이 부과됩니다. WorkSpaces 요금에는 단순 AD 및 AD 커넥터 사용이 포함되지만 AWS 관리형 Microsoft AD 사용은 포함되지 않습니다.

WorkSpaces 에 대한 월별 또는 시간별 청구를 제공합니다 WorkSpaces. 월별 청구의 경우 무제한 사용에 대해 고정 요금을 지불하는데, 이는 WorkSpaces 풀타임으로 사용하는 사용자에게 가장 적합합니다. 시간당 청구의 경우 소액의 고정 월별 요금과 실행 시간별로 저렴한 시간당 요금을 지불합니다. WorkSpace WorkSpace 자세한 내용은 WorkSpaces 요금을 참조하십시오.

지원되는 지역에 대한 자세한 내용은 WorkSpaces 요금을 참조하십시오.

시작하는 방법

생성하려면 다음 튜토리얼 중 하나를 시도해 보세요. WorkSpace

- WorkSpaces 빠른 설정 시작하기
- AWS Managed Microsoft AD를 사용하여 WorkSpace 시작
- Simple AD를 사용하여 WorkSpaces 시작
- AD Connector를 사용하여 WorkSpaces 시작
- 신뢰할 수 있는 도메인을 사용하여 WorkSpace 시작

다음 리소스를 탐색하여 Amazon에 대해 자세히 알아볼 수도 있습니다 WorkSpaces.

- Provision Desktops in the Cloud
- Amazon 배포를 위한 모범 사례 WorkSpaces
- Amazon WorkSpaces 리소스 — 백서, 블로그 게시물, 웨비나, re:Invent 세션 포함
- 아마존 WorkSpaces 자주 묻는 질문

WorkSpaces 빠른 설정 시작하기

이 자습서에서는 WorkSpaces 및 AWS Directory Service를 사용하여 WorkSpace라고 하는, 가상의 클라우드 기반 Microsoft Windows, Amazon Linux 또는 Ubuntu Linux 데스크톱을 프로비저닝하는 방법을 배웁니다.

이 자습서에서는 빠른 설정 옵션을 사용하여 WorkSpaces를 시작합니다. WorkSpaces를 시작한 적이 없는 경우 이 옵션을 사용할 수 있습니다. 또는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

> **Note**
>
> 빠른 설정은 다음 AWS 리전에서 지원됩니다.
>
> - 미국 동부(버지니아 북부)
> - 미국 서부(오레건)
> - 유럽(아일랜드)
> - 아시아 태평양(싱가포르)
> - 아시아 태평양(시드니)
> - 아시아 태평양(도쿄)
>
> 리전을 변경하려면 리전 선택을 참조하세요.

작업

시작하기 전에

시작하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- WorkSpaces를 생성 또는 관리하려면 AWS 계정이 있어야 합니다. 사용자가 WorkSpaces에 연결하고 사용하는 데는 AWS 계정이 필요하지 않습니다.
- 일부 리전에서는 WorkSpaces를 사용할 수 없습니다. 지원되는 리전을 확인한 후 WorkSpaces용 리전을 선택합니다. 지원되는 리전에 대한 자세한 내용은 AWS 리전별 WorkSpaces 요금을 참조하세요.

진행하기 전에 다음 사항을 검토하고 이해하는 것도 도움이 됩니다.

- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 자세한 내용은 Amazon WorkSpaces 번들 및 Amazon WorkSpaces 요금을 참조하세요.
- WorkSpaces를 시작할 때 번들과 함께 사용할 프로토콜(PCoIP 또는 WorkSpaces 스트리밍 프로토콜(WSP))을 선택해야 합니다. 자세한 내용은 아마존용 프로토콜 WorkSpaces 섹션을 참조하세요.
- WorkSpaces를 시작할 때 사용자 이름 및 이메일 주소를 포함하여 사용자의 프로필 정보를 지정해야 합니다. 사용자는 암호를 지정하여 본인의 프로필을 완성합니다. WorkSpaces 및 사용자의 정보는 디렉터리에 저장됩니다. 자세한 내용은 디렉터리 섹션을 참조하세요.

빠른 설정의 기능

빠른 설정이 사용자를 대신하여 다음 작업을 완료합니다.

- WorkSpaces 서비스에서 탄력적 네트워크 인터페이스를 생성하고 WorkSpaces 디렉터리를 나열하도록 허용하는 IAM 역할을 생성합니다. 이 역할의 이름은 `workspaces_DefaultRole`입니다.
- Virtual Private Cloud(VPC)를 생성합니다. 기존 VPC를 대신 사용하려면 VPC가 다음에 대해 VPC를 구성합니다. WorkSpaces 에 명시된 요구 사항을 충족하는지 확인한 다음 WorkSpaces를 사용하여 가상 데스크톱 시작에 나열된 자습서 중 하나의 단계를 따르세요. 사용할 Active Directory 유형에 해당하는 자습서를 선택하세요.
- VPC에 Simple AD 디렉터리를 설정하고 Amazon WorkDocs에 이 디렉터리를 활성화합니다. 이 Simple AD 디렉터리는 사용자 및 WorkSpace 정보를 저장하는 데 사용됩니다. 빠른 설정을 통해 가장 먼저 생성되는 AWS 계정은 관리자(admin) AWS 계정입니다. † 디렉터리에는 관리자(Administrator) 계정도 있습니다. 자세한 내용은 AWS Directory Service 관리 안내서의 What gets created를 참조하세요.
- 지정된 AWS 계정을 생성하여 디렉터리에 추가합니다.

- WorkSpaces를 생성합니다. 각 WorkSpace에는 인터넷 액세스를 제공하기 위한 퍼블릭 IP 주소가 할당됩니다. 실행 모드는 AlwaysOn입니다. 자세한 내용은 WorkSpace 실행 모드 관리 섹션을 참조하세요.
- 지정된 사용자에게 초대 이메일을 전송합니다. 사용자가 초대 이메일을 받지 못한 경우 초대 이메일 전송 섹션을 참조하세요.

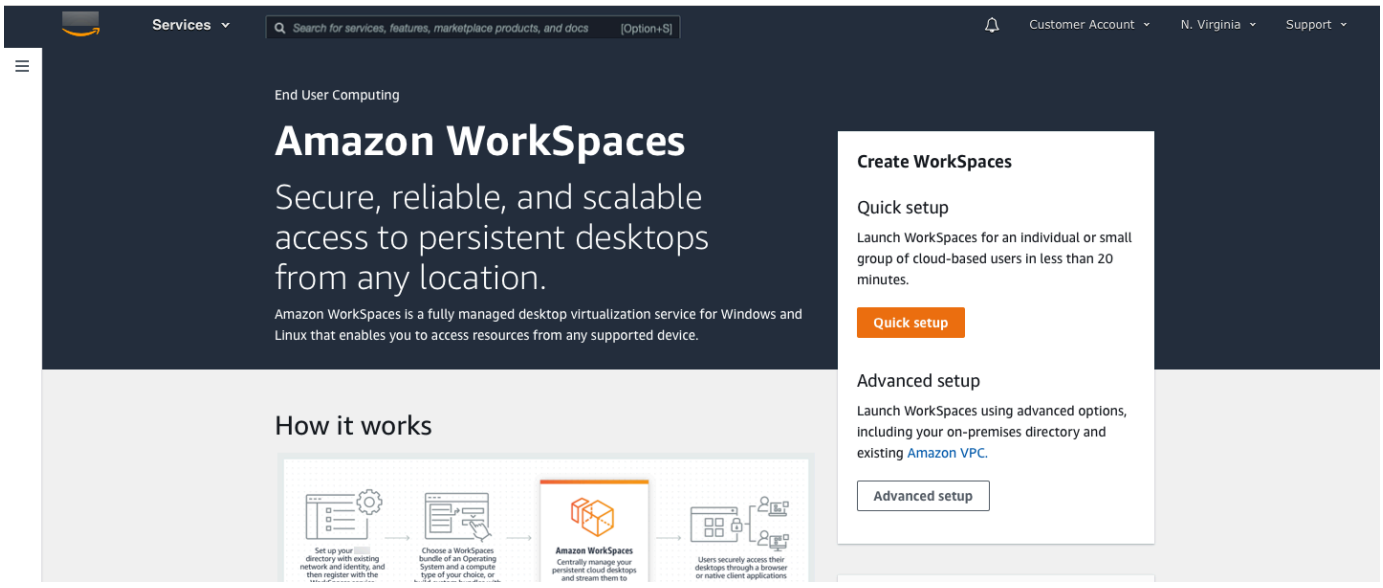
† 빠른 설정을 통해 가장 먼저 생성되는 AWS 계정은 관리자(admin) AWS 계정입니다. WorkSpaces 콘솔에서는 이 AWS 계정을 업데이트할 수 없습니다. 이 계정에 대한 정보를 다른 사람과 공유하지 마세요. 다른 사용자가 WorkSpaces를 사용하도록 초대하려면 해당 사용자를 위해 새 AWS 계정을 생성하세요.

1단계: WorkSpaces 시작

빠른 설정을 사용하여 몇 분이면 첫 번째 WorkSpaces를 시작할 수 있습니다.

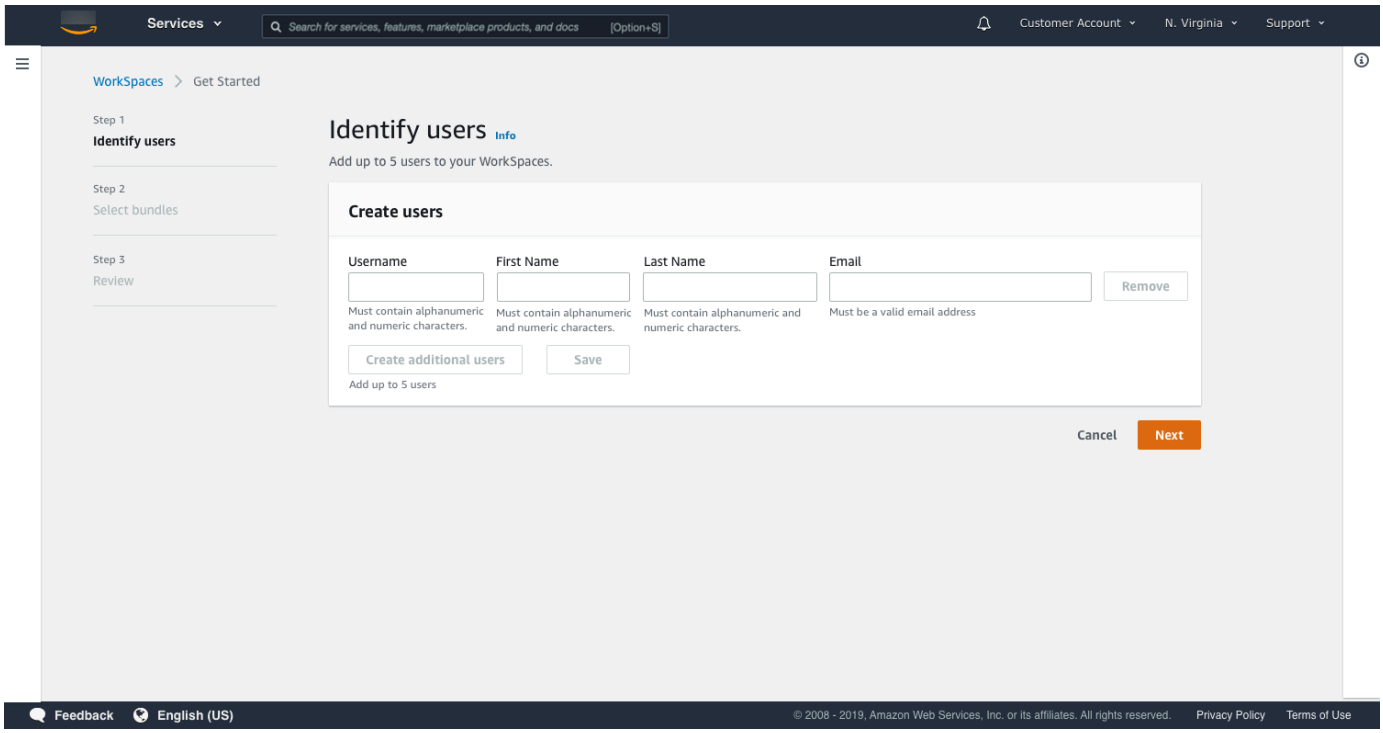
WorkSpaces를 시작하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. Quick setup(빠른 설정)을 선택합니다. 이 버튼이 보이지 않으면 이 리전에서 WorkSpace를 이미 시작했거나, 빠른 설정을 지원하는 리전 중 하나를 사용하고 있지 않는 것입니다. 이 경우 WorkSpaces를 사용하여 가상 데스크톱 시작 섹션을 참조하세요.

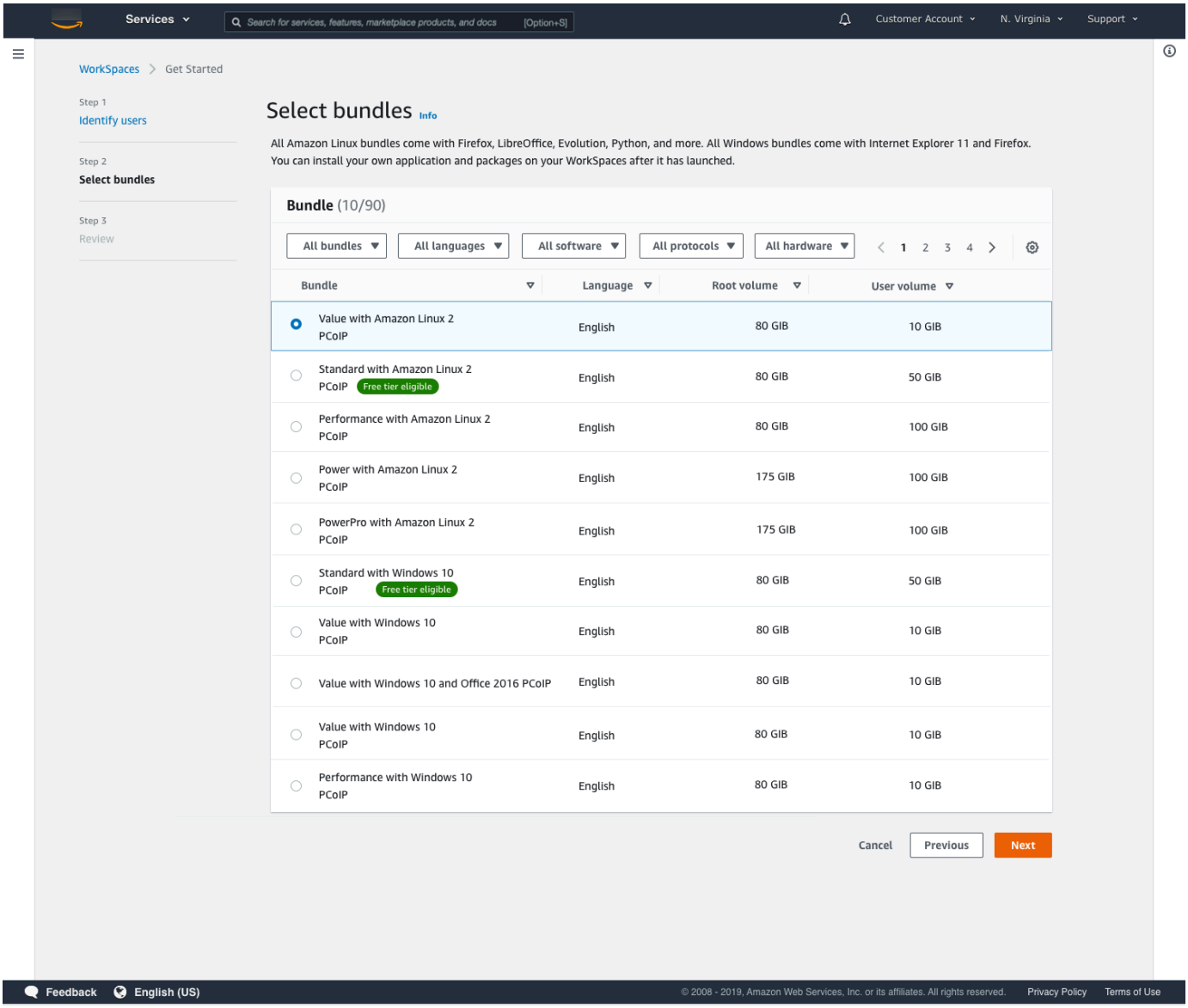


3. 사용자 식별에 사용자 이름, 이름, 성 및 이메일을 입력합니다. 이후 다음을 선택합니다.

> **Note**
>
> WorkSpaces를 처음 사용하는 경우 테스트 목적으로 사용할 사용자를 생성하는 것이 좋습니다.



4. 번들의 경우 적절한 프로토콜(PCoIP 또는 WSP)로 사용자를 위한 번들(하드웨어 및 소프트웨어)을 선택합니다. Amazon WorkSpaces에 사용할 수 있는 다양한 퍼블릭 번들에 대한 자세한 내용은 Amazon WorkSpaces 번들을 참조하세요.



5. 정보를 검토합니다. 그런 다음 WorkSpace 생성을 선택합니다.
6. WorkSpaces를 시작하는 데 약 20분이 소요됩니다. 진행 상황을 모니터링하려면 왼쪽 탐색 창으로 이동하여 디렉터리를 선택합니다. 초기 상태가 `REQUESTED`였다가 `CREATING`이 되고 디렉터리가 생성 중인 것을 볼 수 있습니다.

   디렉터리가 생성되고 상태가 `ACTIVE`이 되면 왼쪽 탐색 창에서 WorkSpaces를 선택하여 WorkSpaces 시작 프로세스의 진행 상황을 모니터링할 수 있습니다. WorkSpaces의 초기 상태는 `PENDING`입니다. 시작이 완료되면 상태가 `AVAILABLE`로 변경되고 각 사용자에 대해 지정한 이메일 주소로 초대가 발송됩니다. 사용자가 초대 이메일을 받지 못한 경우 초대 이메일 전송 섹션을 참조하세요.

2단계: WorkSpaces에 연결

초대 이메일을 수신한 후 원하는 클라이언트를 사용하여 WorkSpaces에 연결할 수 있습니다. 로그인하면 클라이언트에 WorkSpaces 데스크톱이 표시됩니다.

WorkSpaces에 연결하려면

1. 사용자 자격 증명을 아직 설정하지 않은 경우 초대 이메일의 링크를 열고 지침을 따릅니다. WorkSpaces에 연결할 때 필요하므로 이때 지정한 암호를 기억하십시오.

   > **Note**
   >
   > 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 암호는 소문자(a~z), 대문자(A~Z), 숫자(0~9) 및 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/. 세트에서 최소 1자씩 포함해야 합니다.

2. 각 클라이언트의 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients를 검토한 후 다음 중 하나를 수행하세요.

   - 메시지가 표시되면 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작합니다.
   - 메시지가 표시되지 않고 클라이언트 애플리케이션을 아직 설치하지 않은 경우 https://clients.amazonworkspaces.com/ 을 열고 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작하세요.

   > **Note**
   >
   > 웹 브라우저(Web Access)로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

3. 클라이언트를 시작하고 초대 이메일의 등록 코드를 입력한 다음 [Register]를 선택합니다.
4. 로그인하라는 메시지가 표시되면 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.
5. (선택 사항) 자격 증명을 저장하라는 메시지가 표시되면 [Yes]를 선택합니다.

다중 모니터 설정 또는 주변 디바이스 사용과 같은 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

3단계: 정리(선택 사항)

이 자습서에서 생성하여 사용을 마친 WorkSpaces를 삭제할 수 있습니다. 자세한 내용은 the section called “WorkSpace 삭제” 섹션을 참조하세요.

> **Note**
>
> Simple AD는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

다음 단계

계속해서 방금 생성한 WorkSpaces를 사용자 정의할 수 있습니다. 예를 들어 소프트웨어를 설치한 다음 WorkSpaces에서 사용자 지정 번들을 생성할 수 있습니다. 또한 WorkSpaces 및 WorkSpaces 디렉터리에 대해 다양한 관리 작업을 수행할 수 있습니다. 자세한 내용은 다음 문서 섹션을 참조하세요.

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 관리하십시오 WorkSpaces
- WorkSpaces 디렉터리 관리

추가 WorkSpaces를 생성하려면 다음 중 하나를 수행합니다.

- 빠른 설정으로 생성된 VPC와 Simple AD 디렉터리를 계속 사용하려면 'Simple AD를 사용하여 WorkSpaces 시작' 자습서의 2단계: WorkSpaces 생성 섹션에 있는 단계에 따라 추가 사용자를 위한 WorkSpaces를 추가할 수 있습니다.
- 다른 디렉터리 유형을 사용해야 하거나 기존 Active Directory를 사용해야 하는 경우에는 WorkSpaces를 사용하여 가상 데스크톱 시작에서 해당 자습서를 참조하세요.

다중 모니터 설정 또는 주변 디바이스 사용과 같은 WorkSpaces 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

WorkSpaces 고급 설정 시작하기

이 자습서에서는 WorkSpaces 및 AWS Directory Service를 사용하여 WorkSpace라고 하는, 가상의 클라우드 기반 Microsoft Windows 또는 Amazon Linux 데스크톱을 프로비저닝하는 방법을 배웁니다.

이 자습서는 고급 설정 옵션을 사용하여 WorkSpace를 시작합니다.

> **Note**
>
> 고급 설정은 WorkSpaces의 모든 리전에서 지원됩니다.

작업

시작하기 전에

시작하기 전에 WorkSpace를 만들거나 관리하는 데 사용할 수 있는 AWS 계정이 있는지 확인합니다. 사용자가 WorkSpaces에 연결하고 사용하는 데는 AWS 계정이 필요하지 않습니다.

진행하기 전에 다음 개념을 검토하고 이해하세요.

- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 자세한 내용은 Amazon WorkSpaces 번들 단원을 참조하십시오.
- WorkSpaces를 시작할 때 번들과 함께 사용할 프로토콜(PCoIP 또는 WorkSpaces 스트리밍 프로토콜(WSP))을 선택해야 합니다. 자세한 내용은 아마존용 프로토콜 WorkSpaces 섹션을 참조하세요.
- WorkSpaces를 시작할 때 사용자 이름 및 이메일 주소를 포함하여 사용자의 프로필 정보를 지정해야 합니다. 사용자는 암호를 지정하여 본인의 프로필을 완성합니다. WorkSpaces 및 사용자의 정보는 디렉터리에 저장됩니다. 자세한 내용은 디렉터리 섹션을 참조하세요.

고급 설정을 사용하여 WorkSpace 시작

고급 설정을 사용하여 WorkSpace를 시작하는 방법:

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.

2. 다음 디렉터리 유형 중 하나를 선택하고 다음을 선택합니다.

   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector

3. 디렉터리 정보를 입력합니다.
4. 서로 다른 두 개의 가용 영역에 있는 하나의 VPC에서 두 개의 서브넷을 선택합니다. 자세한 내용은 퍼블릭 서브넷이 있는 VPC 구성을 참조하세요.
5. 디렉터리 정보를 검토하고 디렉터리 생성을 선택합니다.

WorkSpaces를 위한 네트워킹 및 액세스

WorkSpace 관리자는 WorkSpaces 네트워킹 및 액세스에 대해 다음 사항을 이해해야 합니다.

목차

아마존용 프로토콜 WorkSpaces

WorkSpaces Amazon은 PCoIP와 WorkSpaces 스트리밍 프로토콜 (WSP) 이라는 두 가지 프로토콜을 지원합니다. 선택하는 프로토콜은 사용자가 액세스하는 디바이스 유형, 사용 중인 운영 체제, 사용자가 직면하게 될 네트워크 조건 WorkSpaces, 사용자에게 양방향 비디오 지원이 필요한지 여부 등 여러 요인에 따라 달라집니다. WorkSpaces

요구 사항

WSP는 다음과 같은 최소 요구 사항에서만 WorkSpaces 지원됩니다.

호스트 에이전트 요구 사항:

- Windows 호스트 에이전트 버전 2.0.0.312 이상
- Ubuntu 호스트 에이전트 버전 2.1.0.501 이상
- Amazon Linux 2 호스트 에이전트 버전 2.0.0.596 이상

클라이언트 요구 사항:

- Windows 네이티브 클라이언트 버전 5.1.0.329 이상
- macOS 네이티브 클라이언트 버전 5.5.0 이상
- 웹 액세스

WorkSpace 클라이언트 버전과 Host Agent 버전을 확인하는 방법에 대한 자세한 내용은 FAQ를 참조하십시오.

WSP을 사용해야 하는 경우

- 최종 사용자 네트워크 조건을 지원하기 위해 더 높은 손실/지연 시간 허용 범위가 필요한 경우 예를 들어 전 세계에서 액세스하거나 신뢰할 수 없는 WorkSpaces 네트워크를 사용하는 사용자가 있을 수 있습니다.
- 사용자가 스마트 카드로 인증하거나 세션 중에 스마트 카드를 사용해야 하는 경우
- 세션 중에 웹캠 지원 기능이 필요한 경우
- Windows Server 2019 WorkSpaces 기반 번들과 함께 웹 액세스를 사용해야 하는 경우
- WorkSpaces우분투를 사용해야 하는 경우
- 윈도우 11 BYOL을 사용해야 하는 경우 WorkSpaces
- 우분투 GPU 기반 번들 (그래픽.G4dn 및 .g4dn) 을 사용해야 하는 경우 GraphicsPro
- 사용자가 세션 중에 또는 Windows Hello와 같은 인증자를 사용하여 인증해야 하는 경우 WebAuthn YubiKey

PCoIP를 사용해야 하는 경우

- iPad 또는 Android Linux 클라이언트를 사용하려는 경우
- Teradici 제로 클라이언트 디바이스를 사용하는 경우

- GPU 기반 번들 (그래픽.G4dn, .g4dn, 그래픽스 등) 을 사용해야 하는 경우 GraphicsPro GraphicsPro
- 스마트 카드가 아닌 사용 사례에 Linux 번들을 사용해야 하는 경우.
-

> **Note**
>
> - 디렉터리에는 PCoIP와 WSP가 혼합되어 있을 수 있습니다. WorkSpaces
> - 사용자는 PCoIP와 WSP를 모두 가질 수 있습니다. 단, PCoIP와 WSP가 서로 WorkSpace WorkSpaces 다른 디렉터리에 있어야 합니다. 동일한 사용자가 동일한 디렉터리에 PCoIP와 WSP를 둘 수 없습니다. WorkSpace 한 사용자에 대해 여러 WorkSpaces 개를 만드는 방법에 대한 자세한 내용은 을 참조하십시오. 한 사용자에 대해 여러 WorkSpaces 만들기
> - 를 다시 빌드해야 하는 WorkSpaces 마이그레이션 기능을 사용하여 두 프로토콜 WorkSpace 간에 a를 마이그레이션할 수 있습니다. WorkSpace 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.
> - PCoIP WorkSpace 번들로 생성한 경우 루트 볼륨을 유지하면서 스트리밍 프로토콜을 수정하여 두 프로토콜 간에 마이그레이션할 수 있습니다. 자세한 내용은 프로토콜 수정을 참조하십시오.
> - 최상의 화상 회의 경험을 위해 Power 또는 PowerPro Bundles만 사용하는 것이 좋습니다.

다음에 대해 VPC를 구성합니다. WorkSpaces

WorkSpaces 가상 사설 클라우드 (VPC) WorkSpaces 에서 실행합니다.

사용자용 프라이빗 서브넷 2개와 퍼블릭 서브넷의 NAT 게이트웨이가 있는 VPC를 만들 수 있습니다 WorkSpaces . 또는 두 개의 퍼블릭 서브넷이 있는 VPC를 생성하고 퍼블릭 IP 주소 또는 엘라스틱 IP 주소를 각각에 연결할 수 WorkSpaces 있습니다. WorkSpace

VPC 설계 고려 사항에 대한 자세한 내용은 Amazon WorkSpaces 배포의 VPC 및 네트워킹 모범 사례 및 배포 모범 사례 - VPC 설계를 참조하십시오. WorkSpaces

내용

- 퍼블릭 서브넷이 있는 VPC 구성

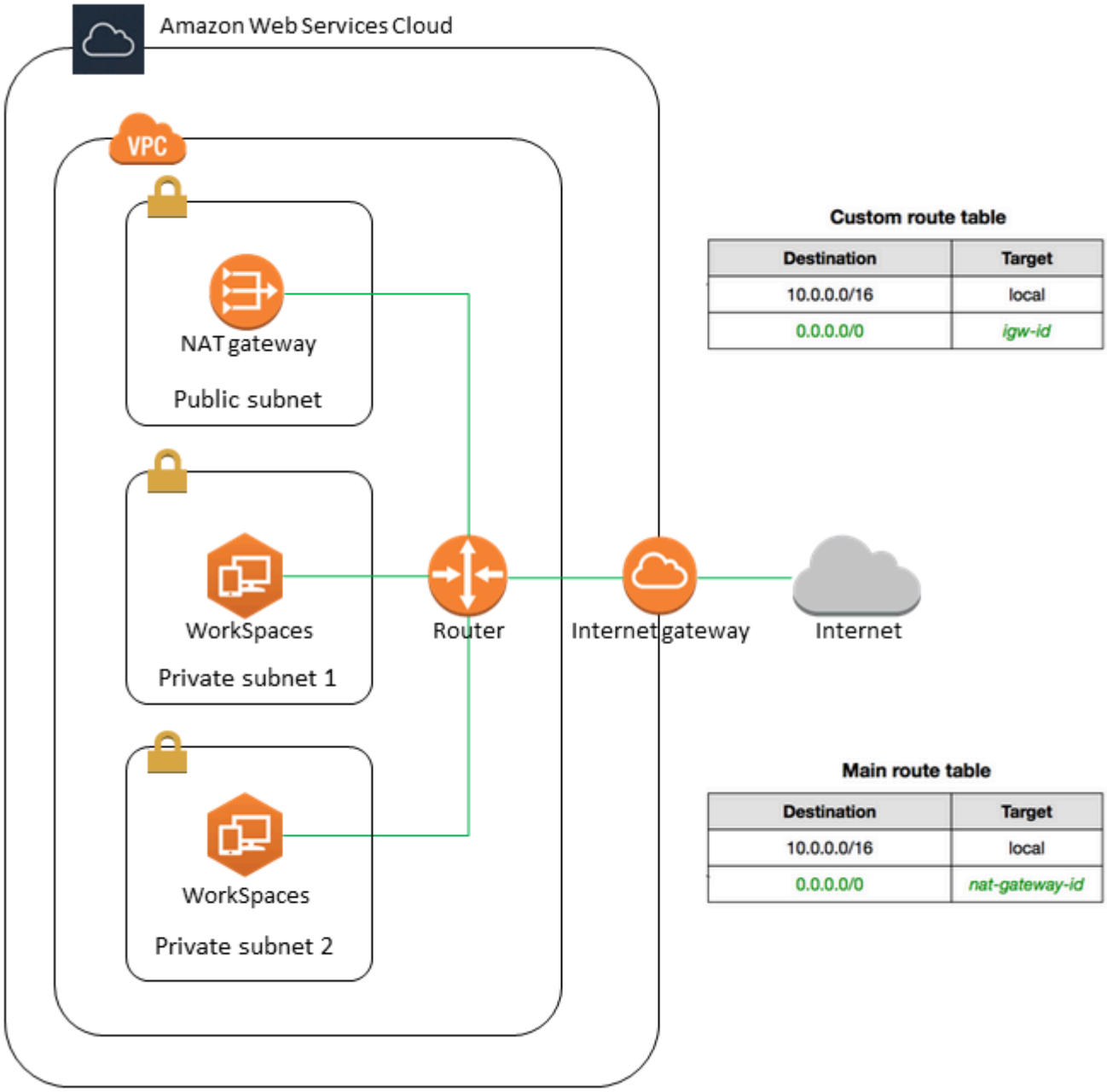
요구 사항

VPC의 서브넷은 출시하려는 지역의 서로 다른 가용 영역에 있어야 합니다. WorkSpaces 각 가용 영역은 다른 가용 영역에서 발생한 장애를 격리시킬 수 있도록 서로 분리된 공간이어야 합니다. 별도의 가용 영역에서 인스턴스를 시작함으로써 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다. 각 서브넷은 단일 가용 영역 내에서만 존재해야 하며, 여러 영역으로 스케일 아웃할 수 없습니다.

> **Note**
>
> WorkSpaces Amazon은 지원되는 각 지역의 일부 가용 영역에서 사용할 수 있습니다. 사용 중인 VPC의 서브넷에 사용할 수 있는 가용 영역을 결정하려면 을 WorkSpaces 참조하십시오. 아마존용 가용 영역 WorkSpaces

프라이빗 서브넷과 NAT 게이트웨이가 있는 VPC 구성

AWS 관리형 Microsoft 또는 Simple AD를 만드는 AWS Directory Service 데 사용하는 경우 VPC를 퍼블릭 서브넷 1개와 프라이빗 서브넷 2개로 구성하는 것이 좋습니다. 프라이빗 WorkSpaces 서브넷에서 실행되도록 디렉터리를 구성하십시오. 프라이빗 WorkSpaces 서브넷에서 인터넷 액세스를 제공하려면 퍼블릭 서브넷에서 NAT 게이트웨이를 구성하십시오.



퍼블릭 서브넷 1개와 프라이빗 서브넷 2개가 있는 VPC를 생성하는 방법

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. VPC 생성을 선택합니다.
3. 생성할 리소스(Resources to create)에서 VPC 등(VPC and more)을 선택합니다.
4. Name tag auto-generation(이름 태그 자동 생성)에 VPC의 이름을 입력합니다.

5. 서브넷을 구성하려면 다음을 수행합니다.

   a. Number of Availability Zones(가용 영역 수)에서 필요에 따라 1 또는 2를 선택합니다.
   b. AZ 사용자 지정을 확장하고 가용 영역을 선택합니다. 그렇지 않으면 AWS 선택해 보세요. 적절하게 선택하는 방법은 아마존용 가용 영역 WorkSpaces 섹션을 참조하세요.
   c. Number of public subnets(퍼블릭 서브넷 수)에서 가용 영역당 하나의 퍼블릭 서브넷이 있는지 확인합니다.
   d. 프라이빗 서브넷 수에서 가용 영역당 하나의 프라이빗 서브넷이 있는지 확인합니다.
   e. 각 서브넷에 대한 CIDR 블록을 입력합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 서브넷 크기를 참조하세요.
6. NAT 게이트웨이는 AZ당 1개를 선택합니다.
7. VPC 생성을 선택합니다.

IPv6 CIDR 블록

IPv6 CIDR 블록을 VPC 및 서브넷에 연결할 수 있습니다. 하지만 서브넷에서 시작된 인스턴스에 자동으로 IPv6 주소를 할당하도록 서브넷을 구성할 경우에는 Graphics 번들을 사용할 수 없습니다. (하지만 그래픽.G4dn, GraphicsPro .g4dn 및 번들은 사용할 수 있습니다.) GraphicsPro 이러한 제한은 IPv6을 지원하지 않는 이전 세대 인스턴스 유형의 하드웨어 제한으로 인해 발생합니다.

이 문제를 해결하려면 그래픽 번들을 시작하기 전에 WorkSpaces 서브넷에서 IPv6 주소 자동 할당 설정을 일시적으로 비활성화하고, 필요한 경우 그래픽 번들을 실행한 후 이 설정을 다시 활성화하여 다른 번들이 원하는 IP 주소를 받도록 할 수 있습니다.

기본적으로 IPv6 주소 자동 할당 설정은 비활성화되어 있습니다. Amazon VPC 콘솔에서 이 설정을 확인하려면 탐색 창에서 서브넷을 선택합니다. 서브넷을 선택하고 Actions(작업), Modify auto-assign IP settings(자동 할당 IP 설정 수정)를 선택합니다.

퍼블릭 서브넷이 있는 VPC 구성

원하는 경우 두 개의 퍼블릭 서브넷이 있는 VPC를 생성할 수 있습니다. 퍼블릭 WorkSpaces 서브넷에서 인터넷 액세스를 제공하려면 엘라스틱 IP 주소를 자동으로 할당하거나 각 주소에 엘라스틱 IP 주소를 수동으로 할당하도록 디렉터리를 구성하십시오. WorkSpace

Tasks

- 1단계: VPC 생성
- 2단계: 퍼블릭 IP 주소를 사용자에게 할당하십시오. WorkSpaces

1단계: VPC 생성

다음과 같이 한 개의 퍼블릭 서브넷이 있는 VPC를 생성합니다.

VPC를 생성하려면

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. VPC 생성을 선택합니다.
3. 생성할 리소스(Resources to create)에서 VPC 등(VPC and more)을 선택합니다.
4. Name tag auto-generation(이름 태그 자동 생성)에 VPC의 이름을 입력합니다.
5. 서브넷을 구성하려면 다음을 수행합니다.
   a. 가용 영역 수에서 2를 선택합니다.
   b. AZ 사용자 지정을 확장하고 가용 영역을 선택합니다. 그렇지 않으면 AWS 해당 주소를 선택해 보세요. 적절하게 선택하는 방법은 아마존용 가용 영역 WorkSpaces 섹션을 참조하세요.
   c. 퍼블릭 서브넷 수는 2를 선택합니다.
   d. 프라이빗 서브넷 수는 0을 선택합니다.
   e. 각 퍼블릭 서브넷에 대한 CIDR 블록을 입력합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 서브넷 크기를 참조하세요.
6. VPC 생성을 선택합니다.

IPv6 CIDR 블록

IPv6 CIDR 블록을 VPC 및 서브넷에 연결할 수 있습니다. 하지만 서브넷에서 시작된 인스턴스에 자동으로 IPv6 주소를 할당하도록 서브넷을 구성할 경우에는 Graphics 번들을 사용할 수 없습니다. (하지만 GraphicsPro 번들은 사용할 수 있습니다.) 이러한 제한은 IPv6을 지원하지 않는 이전 세대 인스턴스 유형의 하드웨어 제한으로 인해 발생합니다.

이 문제를 해결하려면 그래픽 번들을 시작하기 전에 WorkSpaces 서브넷에서 IPv6 주소 자동 할당 설정을 일시적으로 비활성화하고, 필요한 경우 그래픽 번들을 실행한 후 이 설정을 다시 활성화하여 다른 번들이 원하는 IP 주소를 받도록 할 수 있습니다.

기본적으로 IPv6 주소 자동 할당 설정은 비활성화되어 있습니다. Amazon VPC 콘솔에서 이 설정을 확인하려면 탐색 창에서 서브넷을 선택합니다. 서브넷을 선택하고 Actions(작업), Modify auto-assign IP settings(자동 할당 IP 설정 수정)를 선택합니다.

2단계: 퍼블릭 IP 주소를 사용자에게 할당하십시오. WorkSpaces

퍼블릭 IP 주소를 WorkSpaces 자동 또는 수동으로 할당할 수 있습니다. 자동 할당을 사용하려면 the section called “자동 퍼블릭 IP 주소 구성” 단원을 참조하십시오. 퍼블릭 IP 주소를 수동으로 할당하려면 다음 절차를 사용합니다.

퍼블릭 IP 주소를 WorkSpace 수동으로 할당하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 의 행을 펼치고 (화살표 아이콘 선택) WorkSpace IP 값을 기록해 둡니다. WorkSpace 의 기본 사설 IP WorkSpace 주소입니다.
4. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
5. 탐색 창에서 탄력적 IP(Elastic IPs)를 선택합니다. 사용 가능한 탄력적 IP 주소가 없는 경우 탄력적 IP 주소 할당을 선택하고 Amazon의 IPv4 주소 풀 또는 고객이 소유한 IPv4 주소 풀을 선택한 다음 할당을 선택합니다. 새 IP 주소를 기록합니다.
6. 탐색 창에서 네트워크 인터페이스(Network Interfaces)를 선택합니다.
7. 해당 네트워크 인터페이스를 선택합니다 WorkSpace. 해당 네트워크 인터페이스를 찾으려면 WorkSpace 검색 상자에 WorkSpace IP 값 (앞서 적었음) 을 입력한 다음 Enter 키를 누릅니다. WorkSpace IP 값은 네트워크 인터페이스의 기본 프라이빗 IPv4 주소와 일치합니다. 네트워크 인터페이스의 VPC ID는 WorkSpaces VPC의 ID와 일치한다는 점에 유의하십시오.
8. 작업, IP 주소 관리를 선택합니다. Assign new IP(새 IP 할당)을 선택한 다음 Yes, Update(예, 업데이트합니다)를 선택합니다. 새 IP 주소를 기록합니다.
9. [Actions], [Associate Address]를 선택합니다.
10. Associate Elastic IP Address(탄력적 IP 주소 연결) 페이지의 Address(할당)에서 탄력적 IP 주소를 선택합니다. Associate to private IP address(프라이빗 IP 주소에 연결)에서 새 프라이빗 IP 주소를 지정한 다음 Associate Address(주소 연결)를 선택합니다.

아마존용 가용 영역 WorkSpaces

WorkSpacesAmazon에서 사용할 가상 사설 클라우드 (VPC) 를 생성할 때는 VPC의 서브넷이 시작하려는 지역의 서로 다른 가용 영역에 있어야 합니다. WorkSpaces 각 가용 영역은 다른 가용 영역에서 발생한 장애를 격리시킬 수 있도록 서로 분리된 공간이어야 합니다. 별도의 가용 영역에서 인스턴스를 시작함으로써 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다. 각 서브넷은 단일 가용 영역 내에서만 존재해야 하며, 여러 영역으로 스케일 아웃할 수 없습니다.

가용 영역은 리전 코드와 식별 문자의 조합으로 표시됩니다(예: us-east-1a). 리전의 가용 영역에 걸쳐 리소스가 배포될 수 있도록 각 AWS 계정의 이름에 가용 영역을 독립적으로 매핑합니다. 예를 들어 us-east-1a 계정의 AWS 가용 영역은 다른 us-east-1a 계정에 대한 AWS와(과) 위치가 동일하지 않을 수 있습니다.

계정에 대해 가용 영역을 조정하려면 가용 영역에 대한 고유하고 일관된 식별자인 AZ ID를 사용해야 합니다. 예를 들어, use1-az2은(는) us-east-1 리전의 AZ ID이고, 모든 AWS 계정에서 위치가 동일합니다.

AZ ID를 확인하면 다른 계정의 리소스를 기준으로 한 계정의 리소스 위치를 확인할 수 있습니다. 예를 들어, AZ ID가 use1-az2인 가용 영역의 서브넷을 다른 계정과 공유하면 이 서브넷은 AZ ID가 use1-az2인 가용 영역의 계정에서 사용할 수 있습니다. 각 VPC 및 서브넷의 AZ ID가 Amazon VPC 콘솔에 표시됩니다.

WorkSpaces Amazon은 지원되는 각 지역의 가용 영역 중 일부에서만 사용할 수 있습니다. 다음 표에는 각 리전에 사용할 수 있는 AZ ID가 나와 있습니다. AZ ID를 계정의 가용 영역에 매핑하는 방법을 보려면 AWS RAM 사용 설명서의 리소스의 AZ ID를 참조하세요.

지역명	리전 코드	지원되는 AZ ID
미국 동부(버지니아 북부)	us-east-1	use1-az2, use1-az4, use1-az6
미국 서부(오레곤)	us-west-2	usw2-az1, usw2-az2, usw2-az3
아시아 태평양(뭄바이)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
아시아 태평양(서울)	ap-northeast-2	apne2-az1 , apne2-az3
아시아 태평양(싱가포르)	ap-southeast-1	apse1-az1 , apse1-az2
아시아 태평양(시드니)	ap-southeast-2	apse2-az1 , apse2-az3
아시아 태평양(도쿄)	ap-northeast-1	apne1-az1 , apne1-az4
캐나다(중부)	ca-central-1	cac1-az1, cac1-az2
유럽(프랑크푸르트)	eu-central-1	euc1-az2, euc1-az3

지역명	리전 코드	지원되는 AZ ID
유럽(아일랜드)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
유럽(런던)	eu-west-2	euw2-az2, euw2-az3
남아메리카(상파울루)	sa-east-1	sae1-az1, sae1-az3
아프리카(케이프타운)	af-south-1	afs1-az1, afs1-az2, afs1-az3
이스라엘(텔아비브)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (미국 서부)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3
AWS GovCloud (미국 동부)	us-gov-east-1	usge1-az1 , usge1-az2 , usge1-az3

가용 영역 및 AZ ID에 대한 자세한 내용은 Amazon EC2 Linux 인스턴스용 사용 설명서의 리전, 가용 영역 및 로컬 영역을 참조하세요.

IP 주소 및 포트 요구 사항 WorkSpaces

에 연결하려면 WorkSpaces 클라이언트가 연결되는 네트워크에 다양한 AWS 서비스의 IP 주소 범위(하위 집합으로 그룹화) 에 사용할 수 있는 특정 포트가 열려 있어야 합니다. WorkSpaces 이 주소 범위는 AWS 리전에 따라 다릅니다. 또한 클라이언트에서 실행 중인 모든 방화벽에서도 이러한 포트가 개방되어 있어야 합니다. 리전별 AWS IP 주소 범위에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS IP 주소 범위를 참조하세요.

아키텍처 다이어그램은 아키텍처를 참조하십시오WorkSpaces . 추가 아키텍처 다이어그램은 Amazon 배포 모범 사례를 참조하십시오. WorkSpaces

클라이언트 애플리케이션을 위한 포트

WorkSpaces 클라이언트 애플리케이션에는 다음 포트에 대한 아웃바운드 액세스가 필요합니다.

포트 53(UDP)

이 포트는 DNS 서버에 액세스하는 데 사용되며, 클라이언트가 퍼블릭 도메인 이름을 확인할 수 있도록 DNS 서버 IP 주소에 대해 개방되어 있어야 합니다. 도메인 이름 확인에 DNS 서버를 사용하지 않을 경우 이 포트 요구 사항은 선택 사항입니다.

포트 443(TCP)

이 포트는 클라이언트 애플리케이션 업데이트, 등록 및 인증에 사용됩니다. 데스크톱 클라이언트 애플리케이션에서는 포트 443(HTTPS) 트래픽에 대한 프록시 서버 사용을 지원합니다. 프록시 서버 사용을 활성화하려면 클라이언트 애플리케이션을 열고, [Advanced Settings]를 선택하고, [Use Proxy Server]를 선택하고, 프록시 서버의 주소 및 포트를 지정한 다음 [Save]를 선택합니다.

이 포트는 다음 IP 주소 범위에 대해 개방되어 있어야 합니다.

- `GLOBAL` 리전의 `AMAZON` 하위 세트
- 가 `AMAZON` 속해 있는 지역의 서브셋. WorkSpace
- `us-east-1` 리전의 `AMAZON` 하위 세트
- `us-west-2` 리전의 `AMAZON` 하위 세트
- `us-west-2` 리전의 `S3` 하위 세트

포트 4172(UDP 및 TCP)

이 포트는 WorkSpaces PCoIP의 WorkSpace 데스크톱 및 상태 확인을 스트리밍하는 데 사용됩니다. 이 포트는 PCoIP 게이트웨이와 해당 게이트웨이가 위치한 지역의 상태 점검 서버에 개방되어 있어야 합니다. WorkSpace 자세한 내용은 상태 확인 서버 및 PCoIP 게이트웨이 서버 섹션을 참조하세요.

WorkSpacesPCoIP의 경우 데스크톱 클라이언트 애플리케이션은 UDP의 포트 4172 트래픽 (데스크톱 트래픽용) 에 대한 프록시 서버 사용이나 TLS 암호 해독 및 검사를 지원하지 않습니다. 포트 4172에 직접 연결해야 합니다.

포트 4195(UDP 및 TCP)

이 포트는 WorkSpace 데스크톱 스트리밍과 WSP (스트리밍 프로토콜) 의 상태 확인에 사용됩니다. WorkSpaces WorkSpaces 이 포트는 WSP Gateway IP 주소 범위와 해당 지역의 상태 점검 서버에 WorkSpace 개방되어 있어야 합니다. 자세한 내용은 상태 확인 서버 및 WSP 게이트웨이 서버 섹션을 참조하세요.

WSP의 WorkSpaces 경우 WorkSpaces Windows 클라이언트 애플리케이션 (버전 5.1 이상) 및 macOS 클라이언트 애플리케이션 (버전 5.4 이상) 은 포트 4195 TCP 트래픽에 HTTP 프록시 서버 사용을 지원하지만 프록시는 사용하지 않는 것이 좋습니다. TLS 암호 해독 및 검사

는 지원되지 않습니다. 자세한 내용은 Windows WorkSpaces, Amazon Linux WorkSpaces 및 WorkSpacesUbuntu의 인터넷 액세스를 위한 장치 프록시 서버 설정 구성을 참조하십시오.

> **Note**
>
> - 방화벽에서 상태 저장 필터링을 사용하는 경우, 반환 통신을 허용하도록 휘발성 포트(동적 포트라고도 함)가 자동으로 열립니다. 방화벽에서 상태 비저장 필터링을 사용하는 경우 반환 통신을 허용하려면 휘발성 포트를 명시적으로 열어야 합니다. 열어야 하는 필수 휘발성 포트 범위는 구성에 따라 다릅니다.
> - 프록시 서버 기능은 UDP 트래픽에 지원되지 않습니다. 프록시 서버를 사용하는 경우 클라이언트 애플리케이션이 Amazon WorkSpaces 서비스에 보내는 API 호출도 프록시됩니다. API 호출과 데스크톱 트래픽 모두 동일한 프록시 서버를 통과해야 합니다.

웹 액세스를 위한 포트

WorkSpaces 웹 액세스를 위해서는 다음 포트에 대한 아웃바운드 액세스가 필요합니다.

포트 53(UDP)

이 포트는 DNS 서버에 액세스하는 데 사용되며, 클라이언트가 퍼블릭 도메인 이름을 확인할 수 있도록 DNS 서버 IP 주소에 대해 개방되어 있어야 합니다. 도메인 이름 확인에 DNS 서버를 사용하지 않을 경우 이 포트 요구 사항은 선택 사항입니다.

포트 80(UDP 및 TCP)

이 포트는 `https://clients.amazonworkspaces.com`로의 초기 연결에 사용되고, 그런 다음 HTTPS로 전환합니다. 해당 지역의 EC2 하위 집합에 있는 모든 IP 주소 범위에 개방되어 있어야 합니다 WorkSpace .

포트 443(UDP 및 TCP)

이 포트는 HTTPS를 통한 등록 및 인증에 사용되며, 해당 지역의 EC2 하위 집합에 있는 모든 IP 주소 범위에 개방되어야 합니다 WorkSpace .

포트 4195(UDP 및 TCP)

WorkSpaces 스트리밍 프로토콜 (WSP) 용으로 구성된 경우 이 포트는 WorkSpaces 데스크톱 트래픽을 스트리밍하는 데 사용됩니다. WorkSpaces WSP 게이트웨이 IP 주소 범위에 대해 개방되어 있어야 합니다. 자세한 설명은 WSP 게이트웨이 서버 섹션을 참조하세요.

WSP 웹 액세스는 포트 4195 TCP 트래픽에 프록시 서버 사용을 지원하지만 권장되지는 않습니다. 자세한 내용은 Windows WorkSpaces, Amazon Linux WorkSpaces 및 WorkSpacesUbuntu의 인터넷 액세스를 위한 장치 프록시 서버 설정 구성을 참조하십시오.

> **Note**
>
> 방화벽에서 상태 저장 필터링을 사용하는 경우, 반환 통신을 허용하도록 휘발성 포트(동적 포트라고도 함)가 자동으로 열립니다. 방화벽에서 상태 비저장 필터링을 사용하는 경우 반환 통신을 허용하려면 휘발성 포트를 명시적으로 열어야 합니다. 열어야 하는 필수 휘발성 포트 범위는 구성에 따라 다릅니다.

일반적으로 웹 브라우저는 높은 범위의 소스 포트를 임의로 선택하여 스트리밍 트래픽에 사용합니다. WorkSpaces 웹 액세스는 브라우저가 선택하는 포트를 제어할 수 없습니다. 따라서 이 포트에 대한 반송 트래픽이 허용되는지 확인해야 합니다.

허용 목록에 추가할 도메인 및 IP 주소

WorkSpaces 클라이언트 응용 프로그램이 서비스에 액세스할 수 있으려면 클라이언트가 WorkSpaces 서비스에 액세스하려고 하는 네트워크의 허용 목록에 다음 도메인과 IP 주소를 추가해야 합니다.

허용 목록에 추가할 도메인 및 IP 주소

범주	도메인 또는 IP 주소
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	• https://d2td7dqidlhjx7.cloudfront.net/ • AWS GovCloud (미국 서부) 지역: https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ 64.xml WorkSpacesAppCastx
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: • https://.us-east-1.amazonaws.com skylight-client-ds

범주	도메인 또는 IP 주소
	• skylight-client-dshttps://.us-west-2.amazonaws.com • skylight-client-dshttps://.ap-south-1.amazonaws.com • skylight-client-dshttps://.ap-northeast-2.amazonaws.com • skylight-client-dshttps://.ap-southeast-1.amazonaws.com • skylight-client-dshttps://.ap-southeast-2.amazonaws.com • skylight-client-dshttps://.ap-northeast-1.amazonaws.com • skylight-client-dshttps://.ca-central-1.amazonaws.com • skylight-client-dshttps://.eu-central-1.amazonaws.com • skylight-client-dshttps://.eu-west-1.amazonaws.com • skylight-client-dshttps://.eu-west-2.amazonaws.com • skylight-client-dshttps://.sa-east-1.amazonaws.com • skylight-client-dshttps://.af-south-1.amazonaws.com • skylight-client-dshttps://.il-central-1.amazonaws.com • (AWS GovCloud 미국 서부) 지역: https://. skylight-client-ds us-gov-west-1.amazonaws.com • (미국 동부) 지역: AWS GovCloud

범주	도메인 또는 IP 주소
	https://. skylight-client-ds us-gov-east-1.amazonaws.com

범주	도메인 또는 IP 주소
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: • https://.us-east-1.amazonaws.com ws-client-service • ws-client-servicehttps://.us-west-2.amazonaws.com • ws-client-servicehttps://.ap-south-1.amazonaws.com • ws-client-servicehttps://.ap-northeast-2.amazonaws.com • ws-client-servicehttps://.ap-southeast-1.amazonaws.com • ws-client-servicehttps://.ap-southeast-2.amazonaws.com • ws-client-servicehttps://.ap-northeast-1.amazonaws.com • ws-client-servicehttps://.ca-central-1.amazonaws.com • ws-client-servicehttps://.eu-central-1.amazonaws.com • ws-client-servicehttps://.eu-west-1.amazonaws.com • ws-client-servicehttps://.eu-west-2.amazonaws.com • ws-client-servicehttps://.sa-east-1.amazonaws.com • ws-client-servicehttps://.af-south-1.amazonaws.com • ws-client-servicehttps://.il-central-1.amazonaws.com • (AWS GovCloud 미국 서부) 지역:

범주	도메인 또는 IP 주소
	https://. ws-client-service us-gov-west-1.amazonaws.com • (미국 동부) 지역: AWS GovCloud https://. ws-client-service us-gov-east-1.amazonaws.com

범주	도메인 또는 IP 주소
디렉터리 설정	다음에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<##>/<#### ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • 레거시 - https://d1cbg795sa4g1u.cloudfront.net/prod/<리전>/<디렉터리 ID> • 미국 동부(버지니아 북부) - https://d2h1yryv1jxiq.cloudfront.net/ • 미국 서부(오레곤) - https://d1fq42e1gi7rtq.cloudfront.net/ • 아시아 태평양(뭄바이) - https://d1ctsk4u02kky7.cloudfront.net/ • 아시아 태평양(서울) - https://dyoj3cw6iktvg.cloudfront.net • 아시아 태평양(싱가포르) - https://d1525ef92caquk.cloudfront.net/ • 아시아 태평양(시드니) - https://dodwxjr2amr8p.cloudfront.net/

범주	도메인 또는 IP 주소
	• 아시아 태평양(도쿄) - https://d3v7kcib8ir2e1.cloudfront.net/ • 캐나다(중부) - https://d1ebdk07rro1qy.cloudfront.net/ • 유럽(프랑크푸르트) - https://d39q4y7cndearu.cloudfront.net/ • 유럽(아일랜드) - https://d2127w6wvrc6l3.cloudfront.net/ • 유럽(런던) - https://df4ahgpxbxqy2.cloudfront.net/ • 남아메리카(상파울루) - https://d2nezqurrjvain.cloudfront.net/ • 아프리카(케이프타운) - https://dr6ry0pwaoy23.cloudfront.net • 이스라엘 (텔아비브) — https://d2kmf63k5sit88.cloudfront.net 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 미국 동부(버지니아 북부) - https://d32i4gd7pg4909.cloudfront.net/ • 미국 서부(오레곤) - https://d18af777lco7lp.cloudfront.net/ • 아시아 태평양(뭄바이) - https://d78hovzzqqtsb.cloudfront.net/ • 아시아 태평양(서울) - https://dtyv4uwoh7ynt.cloudfront.net/

범주	도메인 또는 IP 주소
	• 아시아 태평양(싱가포르) - https://d3qzmd7y07pz0i.cloudfront.net/ • 아시아 태평양(시드니) - https://dwcpoxuuza83q.cloudfront.net/ • 아시아 태평양(도쿄) - https://d2c2t8mxjhq5z1.cloudfront.net/ • 캐나다(중부) - https://d2wfbsypmqjmog.cloudfront.net/ • 유럽(프랑크푸르트) - https://d1whcm49570jjw.cloudfront.net/ • 유럽(아일랜드) - https://d3pgffbf39h4k4.cloudfront.net/ • 유럽(런던) - https://d16q6638mh01s7.cloudfront.net/ • 남아메리카(상파울루) - https://d2lh2qc5bdoq4b.cloudfront.net/ • 아프리카(케이프타운) - https://di5ygl2cs0mrh.cloudfront.net/ • 이스라엘 (텔아비브) — https://d1a3pnge9on3sx.cloudfront.net (미국 서부) 지역: AWS GovCloud • 고객 디렉터리 설정: https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> • 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: https://.s3- -1.amazonaws.com workspace-client-assets-pdt us-gov-west • 로그인 페이지 스타일 지정을 위한 CSS 파일:

범주	도메인 또는 IP 주소
	workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css • JavaScript 로그인 페이지용 파일: 해당 사항 없음 AWS GovCloud (미국 동부) 지역: • 고객 디렉터리 설정: https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> • 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: https://.s3- -1.amazonaws.com workspace-client-assets-pdt us-gov-east • 로그인 페이지 스타일 지정을 위한 CSS 파일: workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css • JavaScript 로그인 페이지용 파일: 해당 사항 없음
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버

범주	도메인 또는 IP 주소
사전 세션 스마트 카드 인증 엔드포인트	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함) AWS GovCloud (미국 서부) 및 AWS GovCloud (미국 동부) 지역: https://login. us-gov-home<directory id><directory id>.awsapps.com/directory///(고객 도메인은 어디에 있습니까?)

범주	도메인 또는 IP 주소
WS 브로커	도메인: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com • ws-broker-servicehttps://.ap-south-1.amazonaws.com • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com • ws-broker-servicehttps://.ca-central-1.amazonaws.com • ws-broker-servicehttps://.eu-central-1.amazonaws.com • ws-broker-servicehttps://.eu-west-1.amazonaws.com • ws-broker-servicehttps://.eu-west-2.amazonaws.com • ws-broker-servicehttps://.sa-east-1.amazonaws.com • ws-broker-servicehttps://.af-south-1.amazonaws.com

범주	도메인 또는 IP 주소
	• ws-broker-servicehttps://.il-central-1.amazonaws.com • https://ws-broker-service. us-gov-west-1.amazonaws.com • https://. ws-broker-service-fips us-gov-west-1.amazonaws.com • https://. ws-broker-service us-gov-east-1.amazonaws.com • https://. ws-broker-service-fips us-gov-east-1.amazonaws.com

범주	도메인 또는 IP 주소
WorkSpaces API 엔드포인트	도메인: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

범주	도메인 또는 IP 주소
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com

범주	도메인 또는 IP 주소
WorkSpaces SAML 싱글 사인온 (SSO) 용 엔드포인트	도메인: • euc-sso-smhttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-central-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.af-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.il-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm. us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://. euc-sso-sm-fips us-gov-west-1.amazonaws.com/v1/report-heartbeat

범주	도메인 또는 IP 주소
	• https://. euc-sso-sm us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://. euc-sso-sm-fips us-gov-east-1.amazonaws.com/v1/report-heartbeat

PCoIP 허용 목록에 추가할 도메인 및 IP 주소

범주	도메인 또는 IP 주소
PSG(PCoIP Session Gateway)	PCoIP 게이트웨이 서버
세션 브로커(PCM)	도메인: • https://skylight-cm.us-east-1.amazonaws.com • https: //.us-east-1.amazonaws.com skylight-cm-fips • https://skylight-cm.us-west-2.amazonaws.com • skylight-cm-fipshttps://.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

범주	도메인 또는 IP 주소
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm. us-gov-west-1.amazonaws.com • https://. skylight-cm-fips us-gov-west-1.amazonaws.com • https://skylight-cm. us-gov-east-1.amazonaws.com • https://. skylight-cm-fips us-gov-east-1.amazonaws.com

범주	도메인 또는 IP 주소
PCoIP Web Access TURN 서버	서버: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • 현재 아시아 태평양(뭄바이) 리전에서는 Web Access를 사용할 수 없습니다. • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • 현재 아프리카 (케이프타운) 지역에서는 웹 액세스를 사용할 수 없습니다. • 현재 이스라엘 (텔아비브) 지역에서는 웹 액세스를 사용할 수 없습니다.

WorkSpaces 스트리밍 프로토콜 (WSP) 허용 목록에 추가할 도메인 및 IP 주소

범주	도메인 또는 IP 주소
WSP 세션 게이트웨이(WSG)	WSP 게이트웨이 서버
WSP Web Access TURN 서버	WSP 게이트웨이 서버

상태 확인 서버

WorkSpaces 클라이언트 애플리케이션은 포트 4172 및 4195를 통해 상태 검사를 수행합니다. 이러한 검사는 TCP 또는 UDP 트래픽이 서버에서 클라이언트 애플리케이션으로 스트리밍되는지 여부를 검증합니다 WorkSpaces . 이러한 확인을 성공적으로 완료하려면 방화벽 정책에서 다음과 같은 리전별 상태 확인 서버의 IP 주소에 아웃바운드 트래픽을 허용해야 합니다.

리전	상태 확인 호스트 이름	IP 주소
미국 동부(버지니아 북부)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
미국 서부(오레곤)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
아시아 태평양(뭄바이)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
아시아 태평양(서울)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105 52.78.44.253

리전	상태 확인 호스트 이름	IP 주소
		52.79.54.102
아시아 태평양(싱가포르)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
아시아 태평양(시드니)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
아시아 태평양(도쿄)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
캐나다(중부)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
유럽(프랑크푸르트)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
유럽(아일랜드)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224

리전	상태 확인 호스트 이름	IP 주소
유럽(런던)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
남아메리카(상파울루)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
아프리카(케이프타운)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
이스라엘(텔아비브)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43
AWS GovCloud (미국 서부)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88

리전	상태 확인 호스트 이름	IP 주소
AWS GovCloud (미국 동부)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP 게이트웨이 서버

WorkSpaces PCoIP를 사용하여 포트 4172를 통해 데스크톱 세션을 클라이언트에 스트리밍합니다. PCoIP 게이트웨이 서버의 경우 작은 범위의 Amazon EC2 퍼블릭 IPv4 주소를 WorkSpaces 사용합니다. 따라서 WorkSpaces에 액세스하는 디바이스에 대한 방화벽 정책을 세부적으로 설정할 수 있습니다. 참고로, 현재 WorkSpaces 클라이언트는 IPv6 주소를 연결 옵션으로 지원하지 않습니다.

리전	퍼블릭 IP 주소 범위
미국 동부(버지니아 북부)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
미국 서부(오레곤)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255
아시아 태평양(뭄바이)	13.126.243.0 - 13.126.243.255
아시아 태평양(서울)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
아시아 태평양(싱가포르)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255

리전	퍼블릭 IP 주소 범위
아시아 태평양(시드니)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
아시아 태평양(도쿄)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
캐나다(중부)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
유럽(프랑크푸르트)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
유럽(아일랜드)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
유럽(런던)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
남아메리카(상파울루)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
아프리카(케이프타운)	13.246.120.0 - 13.246.123.255

리전	퍼블릭 IP 주소 범위
이스라엘(텔아비브)	51.17.28.0-51.17.31.255
AWS GovCloud (미국 서부)	52.61.193.0 - 52.61.193.255
AWS GovCloud (미국 동부)	18.254.140.0 - 18.254.143.255

WSP 게이트웨이 서버

> **Important**
>
> 2020년 6월부터 포트 4172 대신 포트 WorkSpaces 4195를 통해 WSP용 데스크톱 세션을 WorkSpaces 클라이언트에 스트리밍합니다. WSP를 WorkSpaces 사용하려면 포트 4195가 트래픽에 개방되어 있어야 합니다.

WorkSpaces 는 WSP 게이트웨이 서버에 소량의 Amazon EC2 퍼블릭 IPv4 주소를 사용합니다. 따라서 WorkSpaces에 액세스하는 디바이스에 대한 방화벽 정책을 세부적으로 설정할 수 있습니다. 참고로, 현재 WorkSpaces 클라이언트는 IPv6 주소를 연결 옵션으로 지원하지 않습니다.

리전	퍼블릭 IP 주소 범위
미국 동부(버지니아 북부)	• 3.227.4.0/22 • 44.209.84.0/22
미국 서부(오레곤)	34.223.96.0/22
아시아 태평양(뭄바이)	65.1.156.0/22
아시아 태평양(서울)	3.35.160.0/22
아시아 태평양(싱가포르)	13.212.132.0/22
아시아 태평양(시드니)	3.25.248.0/22
아시아 태평양(도쿄)	3.114.164.0/22

리전	퍼블릭 IP 주소 범위
캐나다(중부)	3.97.20.0/22
유럽(프랑크푸르트)	18.192.216.0/22
유럽(아일랜드)	3.248.176.0/22
유럽(런던)	18.134.68.0/22
남아메리카(상파울루)	15.228.64.0/22
아프리카(케이프타운)	13.246.108.0/22
이스라엘(텔아비브)	51.17.72.0/22
AWS GovCloud (미국 서부)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (미국 동부)	18.254.148.0/22

WSP 게이트웨이 도메인 이름

다음 표에는 WSP WorkSpace 게이트웨이 도메인 이름이 나열되어 있습니다. WorkSpaces 클라이언트 애플리케이션이 WSP 서비스에 액세스할 수 있으려면 이러한 도메인에 연결할 수 있어야 합니다 WorkSpace .

리전	도메인
미국 동부(버지니아 북부)	*.prod.us-east-1.highlander.aws.a2z.com
미국 서부(오레곤)	*.prod.us-west-2.highlander.aws.a2z.com
아시아 태평양(뭄바이)	*.prod.ap-south-1.highlander.aws.a2z.com
아시아 태평양(서울)	*.prod.ap-northeast-2.highlander.aws.a2z.com
아시아 태평양(싱가포르)	*.prod.ap-southeast-1.highlander.aws.a2z.com

리전	도메인
아시아 태평양(시드니)	*.prod.ap-southeast-2.highlander.aws.a2z.com
아시아 태평양(도쿄)	*.prod.ap-northeast-1.highlander.aws.a2z.com
캐나다(중부)	*.prod.ca-central-1.highlander.aws.a2z.com
유럽(프랑크푸르트)	*.prod.eu-central-1.highlander.aws.a2z.com
유럽(아일랜드)	*.prod.eu-west-1.highlander.aws.a2z.com
유럽(런던)	*.prod.eu-west-2.highlander.aws.a2z.com
남아메리카(상파울루)	*.prod.sa-east-1.highlander.aws.a2z.com
아프리카(케이프타운)	*.prod.af-south-1.highlander.aws.a2z.com
이스라엘(텔아비브)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (미국 서부)	*.prod. us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (미국 동부)	*.prod. us-gov-east-1.highlander.aws.a2z.com

네트워크 인터페이스

각각에는 다음과 같은 네트워크 인터페이스가 있습니다. WorkSpace

- 기본 네트워크 인터페이스 (eth1) 는 VPC와 인터넷 내의 리소스에 대한 연결을 제공하며 디렉터리에 연결하는 WorkSpace 데 사용됩니다.
- 관리 네트워크 인터페이스(eth0)는 보안 WorkSpaces 관리 네트워크에 연결됩니다. WorkSpace데스크톱을 WorkSpaces 클라이언트에 대화형 방식으로 스트리밍하고 관리할 수 있도록 WorkSpaces 하는 데 사용됩니다. WorkSpace

WorkSpaces 관리 네트워크 인터페이스가 생성된 지역에 따라 다양한 주소 범위에서 관리 네트워크 인터페이스의 WorkSpaces IP 주소를 선택합니다. 디렉터리가 등록되면 VPC CIDR과 VPC의 라우팅 테이블을 WorkSpaces 테스트하여 이러한 주소 범위가 충돌을 일으키는지 확인합니다. 리전 내의 사용 가능한 모든 주소 범위에서 충돌이 발생할 경우 오류 메시지가 표시되고 디렉터리는 등록되지 않습니다. 디렉터리를 등록한 이후에 VPC에서 라우팅 테이블을 변경할 경우 충돌이 발생할 수 있습니다.

> **Warning**
>
> a에 연결된 네트워크 인터페이스를 수정하거나 삭제하지 마십시오. WorkSpace 이렇게 하면 접속이 불가능해지거나 인터넷 접속이 WorkSpace 끊길 수 있습니다. 예를 들어 디렉터리 수준에서 엘라스틱 IP 주소 자동 할당을 활성화한 경우, 시작 시 엘라스틱 IP 주소(Amazon 제공 풀) 가 사용자에게 할당됩니다. WorkSpace 하지만 소유한 엘라스틱 IP 주소를 에 연결한 WorkSpace 다음 나중에 해당 엘라스틱 IP 주소를 에서 분리하면 퍼블릭 IP 주소가 WorkSpace 손실되고 Amazon 제공 풀에서 새 주소를 자동으로 가져오지 않습니다. WorkSpace
> Amazon에서 제공한 풀의 새 퍼블릭 IP 주소를 와 연결하려면 를 WorkSpace 재구축해야 합니다. WorkSpace 를 다시 빌드하지 않으려면 소유한 WorkSpace 다른 엘라스틱 IP 주소를 에 연결해야 합니다. WorkSpace

관리 인터페이스 IP 주소 범위

다음 표에서는 관리 네트워크 인터페이스에 사용되는 IP 주소 범위를 보여줍니다.

> **Note**
>
> - BYOL (기존 보유 라이선스 사용) WorkSpaces Windows를 사용하는 경우 다음 표의 IP 주소 범위는 적용되지 않습니다. 대신 PCoIP BYOL은 모든 지역의 관리 인터페이스 트래픽에 54.239.224.0/20 IP 주소 범위를 WorkSpaces 사용합니다. AWS WSP BYOL Windows의 경우 54.239.224.0/20 및 10.0.0.0/8 IP 주소 범위가 모든 지역에 적용됩니다. WorkSpaces AWS (이러한 IP 주소 범위는 BYOL의 관리 트래픽을 위해 선택한 /16 CIDR 블록과 함께 사용됩니다.) WorkSpaces
> - 퍼블릭 번들에서 WorkSpaces 생성된 WSP를 사용하는 경우, 다음 표에 나와 있는 PCoIP/WSP 범위 외에도 모든 AWS 지역의 관리 인터페이스 트래픽에도 10.0.0.0/8의 IP 주소 범위가 적용됩니다.

리전	IP 주소 범위
미국 동부(버지니아 북부)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8

리전	IP 주소 범위
미국 서부(오레곤)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
아시아 태평양(뭄바이)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
아시아 태평양(서울)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
아시아 태평양(싱가포르)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
아시아 태평양(시드니)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
아시아 태평양(도쿄)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
캐나다(중부)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
유럽(프랑크푸르트)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
유럽(아일랜드)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8

리전	IP 주소 범위
유럽(런던)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
남아메리카(상파울루)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
아프리카(케이프타운)	PCoIP/WSP: 172.31.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
이스라엘(텔아비브)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud (미국 서부)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8, 192.169.0.0/16
AWS GovCloud (미국 동부)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

관리 인터페이스 포트

모두의 WorkSpaces 관리 네트워크 인터페이스에서 다음 포트가 열려 있어야 합니다.

- 포트 4172의 인바운드 TCP. PCoIP 프로토콜에서 스트리밍 연결을 설정하는 데 사용됩니다.
- 포트 4172의 인바운드 UDP. PCoIP 프로토콜에서 사용자 입력을 스트리밍하는 데 사용됩니다.
- 포트 4489의 인바운드 TCP. 이것은 웹 클라이언트를 사용한 액세스에 사용됩니다.
- 포트 8200의 인바운드 TCP. 의 관리 및 구성에 사용됩니다 WorkSpace.
- 포트 8201~8250의 인바운드 TCP. 이 포트는 WSP 프로토콜에서 스트리밍 연결을 설정하고 사용자 입력을 스트리밍하는 데 사용됩니다.
- 포트 8220의 인바운드 UDP. 이 포트는 WSP 프로토콜에서 스트리밍 연결을 설정하고 사용자 입력을 스트리밍하는 데 사용됩니다.
- 포트 8443 및 9997의 아웃바운드 TCP. 이것은 웹 클라이언트를 사용한 액세스에 사용됩니다.

- 포트 3478, 4172, 4195의 아웃바운드 UDP. 이것은 웹 클라이언트를 사용한 액세스에 사용됩니다.
- 포트 50002 및 55002의 아웃바운드 UDP. 스트리밍에 사용됩니다. 방화벽에서 상태 저장 필터링을 사용하는 경우 반환 통신을 허용하도록 휘발성 포트 50002 및 55002가 자동으로 열립니다. 방화벽에서 상태 비저장 필터링을 사용하는 경우 반환 통신을 허용하려면 휘발성 포트 49152 – 65535를 열어야 합니다.
- 관리 인터페이스 IP 범위에 정의된 포트 80의 아웃바운드 TCP는 EC2 메타데이터 서비스에 액세스하기 위한 IP 주소 169.254.169.254로 전송됩니다. 사용자에게 할당된 모든 HTTP 프록시는 169.254.169.254도 제외해야 합니다. WorkSpaces
- 포트 1688에서 IP 주소 169.254.169.250 및 169.254.169.251에 대한 아웃바운드 TCP. 퍼블릭 번들 기반 Workspaces에 대한 Microsoft KMS for Windows 정품 인증에 액세스를 허용합니다. BYOL (기존 보유 라이선스 사용) Windows를 사용하는 경우 Windows 정품 인증을 위해 자체 KMS WorkSpaces 서버에 대한 액세스를 허용해야 합니다.
- 포트 1688의 TCP를 IP 주소 54.239.236.220으로 아웃바운드하여 BYOL용 Microsoft KMS 정품 인증에 액세스할 수 있도록 합니다. WorkSpaces

  WorkSpaces 퍼블릭 번들 중 하나를 통해 Office를 사용하는 경우 Office용 Microsoft KMS 정품 인증을 위한 IP 주소가 달라집니다. 해당 IP 주소를 확인하려면 의 관리 인터페이스에 사용할 IP 주소를 찾은 다음 마지막 두 옥텟을 로 바꾸십시오. WorkSpace `64.250` 예를 들어 관리 인터페이스의 IP 주소가 192.168.3.5인 경우 Microsoft KMS Office 정품 인증을 위한 IP 주소는 192.168.64.250입니다.
- WorkSpace 호스트가 프록시 서버를 사용하도록 구성된 경우 WSP의 WorkSpaces IP 주소 127.0.0.2로 TCP를 아웃바운드합니다.
- 루프백 주소 127.0.01에서 시작된 통신.

일반적인 상황에서는 WorkSpaces 서비스가 사용자를 위해 이러한 포트를 구성합니다. WorkSpaces 이러한 포트를 WorkSpace 차단하는 시스템에 보안 또는 방화벽 소프트웨어가 설치되어 있는 경우 제대로 작동하지 않거나 접속이 불가능할 수 있습니다. WorkSpace

기본 인터페이스 포트

어떤 유형의 디렉터리를 사용하든, 모든 디렉터리의 기본 네트워크 인터페이스에서 다음 포트를 열어야 합니다. WorkSpaces

- 인터넷 연결의 경우 다음 포트는 열려 있어야 하며 모든 목적지로 아웃바운드되고 WorkSpaces VPC에서 인바운드되어야 합니다. 인터넷에 액세스할 수 있게 하려면 해당 보안 그룹에 수동으로 추가해야 합니다. WorkSpaces
  - TCP 80(HTTP)

  - TCP 443(HTTPS)
- 디렉터리 컨트롤러와 통신하려면 WorkSpaces VPC와 디렉터리 컨트롤러 사이에 다음 포트가 열려 있어야 합니다. Simple AD 디렉터리의 경우 AWS Directory Service에서 생성되는 보안 그룹에서 이러한 포트가 올바르게 구성됩니다. AD Connector 디렉터리의 경우 이러한 포트를 열도록 VPC의 기본 보안 그룹을 조정해야 할 수 있습니다.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 인증
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP/UDP 636 - LDAPS (TLS/SSL을 통한 LDAP)
  - TCP 1024-65535 - RPC 동적 포트

  이러한 포트를 WorkSpace 차단하는 보안 또는 방화벽 소프트웨어가 설치된 경우 제대로 작동하지 않거나 접속이 불가능할 수 있습니다. WorkSpace

리전별 IP 주소 및 포트 요구 사항

미국 동부(버지니아 북부)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 메트릭 (3.0 WorkSpaces 이상 클라이언트 애플리케이션용)	도메인:

범주	Details
	https://.us-east-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.us-east-1.amazonaws.com ws-client-service

범주	Details
디렉터리 설정	로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 미국 동부(버지니아 북부) - https://d32i4gd7pg4909.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버

범주	Details
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.us-east-1.signin.aws
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: https://workspaces.us-east-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.us-east-1.amazonaws.com • https://.us-east-1.amazonaws.com skylight-cm-fips
PCoIP Web Access TURN 서버	서버: • turn:*.us-east-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-iad.amazonworkspaces.com

범주	Details
상태 확인 IP 주소	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
WSP 게이트웨이 서버 IP 주소 범위	• 3.227.4.0/22 • 44.209.84.0/22
WSP 게이트웨이 도메인 이름	*.prod.us-east-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

미국 서부(오레곤)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인:

범주	Details
	https://.us-west-2.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.us-west-2.amazonaws.com ws-client-service

범주	Details
디렉터리 설정	로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 미국 서부(오레곤) - https://d18af777lco7lp.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버

범주	Details
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.us-west-2.signin.aws
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.us-west-2.amazonaws.com • https://.us-west-2.amazonaws.com skylight-cm-fips
PCoIP Web Access TURN 서버	서버: • turn:*.us-west-2.rdn.amazonaws.com
상태 확인 호스트 이름	drp-pdx.amazonworkspaces.com

범주	Details
상태 확인 IP 주소	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
WSP 게이트웨이 서버 IP 주소 범위	34.223.96.0/22
WSP 게이트웨이 도메인 이름	*.prod.us-west-2.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

아시아 태평양(뭄바이)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-south-1.amazonaws.com skylight-client-ds

범주	Details
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-south-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로 인증합니다. WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아시아 태평양(뭄바이) - https://d78hovzzqqtsb.cloudfront.net/

범주	Details
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.ap-south-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ap-south-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ap-south-1.amazonaws.com
PCoIP Web Access TURN 서버	현재 아시아 태평양(뭄바이) 리전에서는 Web Access를 사용할 수 없습니다.
상태 확인 호스트 이름	drp-bom.amazonworkspaces.com
상태 확인 IP 주소	• 13.127.57.82 • 13.234.250.73
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	13.126.243.0 - 13.126.243.255
WSP 게이트웨이 서버 IP 주소 범위	65.1.156.0/22
WSP 게이트웨이 도메인 이름	*.prod.ap-south-1.highlander.aws.a2z.com

범주	Details
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

아시아 태평양(서울)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
디바이스 메트릭 (1.0+ 및 2.0+ 클라이언트 애플리케이션용) WorkSpaces	https://-2.amazon.com/ device-metrics-us
클라이언트 지표 (3.0 이상 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-northeast-2.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-northeast-2.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증 WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/

범주	Details
	고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아시아 태평양(서울) - https://dtyv4uwoh7ynt.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com

범주	Details
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ap-northeast-2.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ap-northeast-2.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.ap-northeast-2.rdn.amazonaws.com
상태 확인 호스트 이름	drp-icn.amazonworkspaces.com
상태 확인 IP 주소	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
WSP 게이트웨이 서버 IP 주소 범위	3.35.160.0/22
WSP 게이트웨이 도메인 이름	*.prod.ap-northeast-2.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

아시아 태평양(싱가포르)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-southeast-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-southeast-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증 WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID>

범주	Details
	로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아시아 태평양(싱가포르) - https://d3qzmd7y07pz0i.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ap-southeast-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ap-southeast-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.ap-southeast-1.rdn.amazonaws.com

범주	Details
상태 확인 호스트 이름	drp-sin.amazonworkspaces.com
상태 확인 IP 주소	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
WSP 게이트웨이 서버 IP 주소 범위	13.212.132.0/22
WSP 게이트웨이 도메인 이름	*.prod.ap-southeast-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

아시아 태평양(시드니)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-southeast-2.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인:

범주	Details
	https://.ap-southeast-2.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증 WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아시아 태평양(시드니) - https://dwcpoxuuza83q.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/

범주	Details
상태 확인(DRP) 서버	상태 확인 서버
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.ap-southeast-2.signin.aws
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ap-southeast-2.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ap-southeast-2.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.ap-southeast-2.rdn.amazonaws.com
상태 확인 호스트 이름	drp-syd.amazonworkspaces.com
상태 확인 IP 주소	• 3.24.11.127 • 13.237.232.125
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255

범주	Details
WSP 게이트웨이 서버 IP 주소 범위	3.25.248.0/22
WSP 게이트웨이 도메인 이름	*.prod.ap-southeast-2.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

아시아 태평양(도쿄)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-northeast-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ap-northeast-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증 WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결:

범주	Details
	• https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아시아 태평양(도쿄) - https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.ap-northeast-1.signin.aws
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)

범주	Details
WS 브로커	도메인: • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ap-northeast-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ap-northeast-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.ap-northeast-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-nrt.amazonworkspaces.com
상태 확인 IP 주소	• 18.178.102.247 • 54.64.174.128
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
WSP 게이트웨이 서버 IP 주소 범위	3.114.164.0/22
WSP 게이트웨이 도메인 이름	*.prod.ap-northeast-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

캐나다(중부)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ca-central-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.ca-central-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽:

범주	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 캐나다(중부) - https://d2wfbsypmqjmog.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.ca-central-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.ca-central-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.ca-central-1.amazonaws.com

범주	Details
PCoIP Web Access TURN 서버	서버: • turn:*.ca-central-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-yul.amazonworkspaces.com
상태 확인 IP 주소	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
WSP 게이트웨이 서버 IP 주소 범위	3.97.20.0/22
WSP 게이트웨이 도메인 이름	*.prod.ca-central-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

유럽(프랑크푸르트)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인:

범주	Details
	https://.eu-central-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.eu-central-1.amazonaws.com ws-client-service

범주	Details
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증 WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 유럽(프랑크푸르트) - https://d1whcm49570jjw.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버

범주	Details
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.eu-central-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.eu-central-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.eu-central-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.eu-central-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-fra.amazonworkspaces.com
상태 확인 IP 주소	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
WSP 게이트웨이 서버 IP 주소 범위	18.192.216.0/22

범주	Details
WSP 게이트웨이 도메인 이름	*.prod.eu-central-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

유럽(아일랜드)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.eu-west-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.eu-west-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/

범주	Details
	고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 유럽(아일랜드) - https://d3pgffbf39h4k4.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.eu-west-1.signin.aws
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.eu-west-1.amazonaws.com

범주	Details
WorkSpaces API 엔드포인트	도메인: • https://workspaces.eu-west-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.eu-west-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.eu-west-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-dub.amazonworkspaces.com
상태 확인 IP 주소	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
WSP 게이트웨이 서버 IP 주소 범위	3.248.176.0/22
WSP 게이트웨이 도메인 이름	*.prod.eu-west-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

유럽(런던)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.eu-west-2.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.eu-west-2.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽:

범주	Details
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 유럽(런던) - https://d16q6638mh01s7.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.eu-west-2.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.eu-west-2.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.eu-west-2.amazonaws.com

범주	Details
PCoIP Web Access TURN 서버	서버: • turn:*.eu-west-2.rdn.amazonaws.com
상태 확인 호스트 이름	drp-lhr.amazonworkspaces.com
상태 확인 IP 주소	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
WSP 게이트웨이 서버 IP 주소 범위	18.134.68.0/22
WSP 게이트웨이 도메인 이름	*.prod.eu-west-2.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 198.19.0.0/16 • WSP: 10.0.0.0/8

남아메리카(상파울루)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인:

범주	Details
	https://.sa-east-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.sa-east-1.amazonaws.com ws-client-service

범주	Details
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 남아메리카(상파울루) - https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버

범주	Details
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.sa-east-1.amazonaws.com
WorkSpaces API 엔드포인트	도메인: • https://workspaces.sa-east-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.sa-east-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • turn:*.sa-east-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-gru.amazonworkspaces.com
상태 확인 IP 주소	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
WSP 게이트웨이 서버 IP 주소 범위	15.228.64.0/22

범주	Details
WSP 게이트웨이 도메인 이름	*.prod.sa-east-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 198.19.0.0/16 • WSP: 10.0.0.0/8

아프리카(케이프타운)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.af-south-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.af-south-1.amazonaws.com ws-client-service
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로 인증합니다. WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/

범주	Details
	고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 아프리카(케이프타운) - https://di5ygl2cs0mrh.cloudfront.net/
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • ws-broker-servicehttps://.af-south-1.amazonaws.com

범주	Details
WorkSpaces API 엔드포인트	도메인: • https://workspaces.af-south-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.af-south-1.amazonaws.com
상태 확인 호스트 이름	drp-cpt.amazonworkspaces.com
상태 확인 IP 주소	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 13.246.120.0 - 13.246.123.255
WSP 게이트웨이 서버 IP 주소 범위	15.228.64.0/22
WSP 게이트웨이 도메인 이름	*.prod.af-south-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 172.31.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

이스라엘(텔아비브)

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://d2td7dqidlhjx7.cloudfront.net/
연결 점검	https://connectivity.amazonworkspaces.com/

범주	Details
클라이언트 지표 (3.0개 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.il-central-1.amazonaws.com skylight-client-ds
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://.il-central-1.amazonaws.com ws-client-service

범주	Details
디렉터리 설정	다음 사이트에 로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • 로그인 페이지 스타일 지정을 위한 CSS 파일: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 로그인 페이지용 파일: • 이스라엘 (텔아비브); —
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com

범주	Details
사용자 로그인 페이지	https://<디렉터리 ID>.awsapps.com/ (<디렉터리 ID>는 고객의 도메인을 의미함)
WS 브로커	도메인: • https://.il-central-1.amazonaws.com ws-broker-service
WorkSpaces API 엔드포인트	도메인: • https://workspaces.il-central-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm.il-central-1.amazonaws.com
PCoIP Web Access TURN 서버	서버: • 턴: *.il-central-1.rdn.amazonaws.com
상태 확인 호스트 이름	drp-tlv.amazonworkspaces.com
상태 확인 IP 주소	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 51.17.28.0-51.17.31.255
WSP 게이트웨이 서버 IP 주소 범위	51.17.72.0/22
WSP 게이트웨이 도메인 이름	*.prod.il-central-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud (미국 서부) 지역

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://s3.amazonaws.com/ workspaces-client-updates /prod/pdt/windows/ .xml WorkSpaces AppCast
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 지표 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://. skylight-client-ds us-gov-west-1.amazonaws.com
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://. ws-client-service us-gov-west-1.amazonaws.com
디렉터리 설정	로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID>

범주	Details
	고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://s3.amazonaws.com/ workspaces-client-assets /prod/pdt/ <directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css JavaScript 로그인 페이지용 파일: • 해당 사항 없음
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.signin. amazonaws-us-gov.com
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://login. us-gov-home<directory id><directory id>.awsapps.com/directory//(고객 도메인은 어디에 있습니까?)
WS 브로커	도메인: • https:ws-broker-service//. us-gov-west-1.amazonaws.com • https://. ws-broker-service-fips us-gov-west-1.amazonaws.com

범주	Details
WorkSpaces API 엔드포인트	도메인: • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm. us-gov-west-1.amazonaws.com • https://. skylight-cm-fips us-gov-west-1.amazonaws.com
상태 확인 호스트 이름	drp-pdt.amazonworkspaces.com
상태 확인 IP 주소	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 52.61.193.0 - 52.61.193.255
WSP 게이트웨이 서버 IP 주소 범위	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
WSP 게이트웨이 도메인 이름	*.prod. us-gov-west-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 198.19.0.0/16 • WSP: 10.0.0.0/8, 192.169.0.0/16

AWS GovCloud (미국 동부) 지역

허용 목록에 추가할 도메인 및 IP 주소

범주	Details
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
클라이언트 자동 업데이트	https://s3.amazonaws.com/ workspaces-client-updates /prod/osu/windows/ .xml WorkSpaces AppCast
연결 점검	https://connectivity.amazonworkspaces.com/
클라이언트 메트릭 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://. skylight-client-ds us-gov-east-1.amazonaws.com
동적 메시징 서비스 (3.0 이상의 클라이언트 애플리케이션용) WorkSpaces	도메인: https://. ws-client-service us-gov-east-1.amazonaws.com
디렉터리 설정	로그인하기 전에 클라이언트에서 고객 디렉터리로의 인증: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<리전>/<디렉터리 ID> macOS 클라이언트에서의 연결: • https://d32i4gd7pg4909.cloudfront.net/ 고객 디렉터리 설정: • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID>

범주	Details
	고객 디렉터리 수준 협력 브랜드에 대한 로그인 페이지 그래픽: • https://s3.amazonaws.com/ workspaces-client-assets /prod/osu/ <directory ID> 로그인 페이지 스타일 지정을 위한 CSS 파일: • workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css JavaScript 로그인 페이지용 파일: • 해당 사항 없음
Forrester 로그 서비스	https://fls-na.amazon.com/
상태 확인(DRP) 서버	상태 확인 서버
사전 세션 스마트 카드 인증 엔드포인트	https://smartcard.signin. amazonaws-us-gov.com
등록 종속성(웹 액세스 및 Teradici PCoIP 제로 클라이언트용)	https://s3.amazonaws.com
사용자 로그인 페이지	https://login. us-gov-home<directory id><directory id>.awsapps.com/directory//(고객 도메인은 어디에 있습니까?)
WS 브로커	도메인: • https:ws-broker-service//. us-gov-east-1.amazonaws.com • https://. ws-broker-service-fips us-gov-east-1.amazonaws.com

범주	Details
WorkSpaces API 엔드포인트	도메인: • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com
세션 브로커(PCM)	도메인: • https://skylight-cm. us-gov-east-1.amazonaws.com • https://. skylight-cm-fips us-gov-east-1.amazonaws.com
상태 확인 호스트 이름	drp-osu.amazonworkspaces.com
상태 확인 IP 주소	• 18.253.251.70 • 18.254.0.118
PCoIP 게이트웨이 서버 퍼블릭 IP 주소 범위	• 18.254.140.0 - 18.254.143.255
WSP 게이트웨이 서버 IP 주소 범위	18.254.148.0/22
WSP 게이트웨이 도메인 이름	*.prod. us-gov-east-1.highlander.aws.a2z.com
관리 인터페이스 IP 주소 범위	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Amazon WorkSpaces 클라이언트 네트워크 요구 사항

WorkSpaces 사용자는 지원되는 디바이스의 클라이언트 애플리케이션을 사용하여 WorkSpaces에 연결할 수 있습니다. 또한 웹 브라우저를 사용하여 이러한 형식의 액세스를 지원하는 WorkSpaces에 연결할 수도 있습니다. 웹 브라우저 액세스를 지원하는 WorkSpaces의 목록은 클라이언트 액세스, Web Access 및 사용자 환경에서 'Web Access를 지원하는 Amazon WorkSpaces 번들은 무엇인가요?'를 참조하세요.

> **Note**
>
> 웹 브라우저로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

> **Important**
>
> 2020년 10월 1일부터 고객은 더 이상 Amazon WorkSpaces Web Access 클라이언트를 사용하여 Windows 7 사용자 지정 WorkSpaces 또는 Windows 7 기존 보유 라이선스 사용(BYOL) WorkSpaces에 연결할 수 없습니다.

WorkSpaces에 대한 좋은 경험을 사용자에게 제공하려면 클라이언트 디바이스가 다음 네트워크 요구 사항을 충족하는지 확인합니다.

- 클라이언트 디바이스에 광대역 인터넷 연결이 있어야 합니다. 480p 비디오 창을 동시에 시청하는 사용자당 최소 1Mbps를 계획하는 것이 좋습니다. 비디오 해상도에 대한 사용자 품질 요구 사항에 따라 더 많은 대역폭이 필요할 수 있습니다.
- 클라이언트 디바이스가 연결되는 네트워크와 클라이언트 디바이스의 방화벽에서 다양한 AWS 서비스를 위한 IP 주소 범위에 대해 특정 포트가 개방되어 있어야 합니다. 자세한 내용은 IP 주소 및 포트 요구 사항 WorkSpaces 섹션을 참조하세요.
- 최상의 PCoIP 성능을 위해 클라이언트 네트워크에서 WorkSpaces가 속한 리전까지의 왕복 시간(RTT)이 100밀리초보다 짧아야 합니다. RTT가 100~200밀리초일 경우 사용자가 WorkSpaces에 액세스할 수 있지만 성능에 영향이 있습니다. RTT가 200~375밀리초인 경우 성능이 저하됩니다. RTT가 375밀리초를 초과하면 WorkSpaces 클라이언트 연결이 종료됩니다.

  최상의 WorkSpaces 스트리밍 프로토콜(WSP) 성능을 위해 클라이언트 네트워크에서 WorkSpaces가 속한 리전까지의 왕복 시간(RTT)이 250밀리초보다 짧아야 합니다. RTT가 250~400밀리초일 경우 사용자가 WorkSpaces에 액세스할 수 있지만 성능이 저하됩니다.

  현재 위치에서 다양한 AWS 리전까지의 RTT를 확인하려면 Amazon WorkSpaces Connection Health Check을 사용하세요.
- WSP와 함께 웹캠을 사용하려면 초당 1.7메가비트의 최소 업로드 대역폭을 사용하는 것이 좋습니다.
- 사용자가 가상 사설 네트워크(VPN)를 통해 WorkSpaces에 액세스하는 경우 연결에서 1,200바이트 이상의 최대 전송 단위(MTU)를 지원해야 합니다.

> **Note**
>
> Virtual Private Cloud(VPC)에 연결된 VPN을 통해 WorkSpaces에 액세스할 수 없습니다. VPN을 사용하여 WorkSpaces에 액세스하려면 IP 주소 및 포트 요구 사항 WorkSpaces의 설명과 같이 VPN의 퍼블릭 IP 주소를 통한 인터넷 연결이 필요합니다.

- 클라이언트가 서비스 및 Amazon Simple Storage Service(S3)에서 호스팅하는 WorkSpaces 리소스에 대한 HTTPS 액세스를 필요로 합니다. 클라이언트는 애플리케이션 수준의 프록시 리디렉션을 지원하지 않습니다. 사용자가 등록을 완료하고 WorkSpaces에 액세스할 수 있도록 HTTPS 액세스가 필요합니다.
- PCoIP 제로 클라이언트 디바이스에서의 액세스를 허용하려면 WorkSpaces에 PCoIP 프로토콜 번들을 사용해야 합니다. 또한 Teradici에 NTP(Network Time Protocol)를 활성화해야 합니다. 자세한 내용은 WorkSpaces용 PCoIP 제로 클라이언트 설정 섹션을 참조하세요.
- 3.0+ 클라이언트의 경우 Amazon WorkDocs에 Single Sign-On(SSO)을 사용하는 경우 AWS Directory Service 관리 안내서의 Single Sign-On에 있는 지침을 따라야 합니다.

클라이언트 디바이스가 네트워킹 요구 사항을 충족하는지 다음과 같이 확인할 수 있습니다.

3.0+ 클라이언트의 네트워킹 요구 사항을 확인하려면

1. WorkSpaces 클라이언트를 엽니다. 이번이 처음 클라이언트를 여는 경우라면 초대 이메일로 받은 등록 코드를 입력하는 메시지가 표시됩니다.
2. 사용 중인 클라이언트에 따라 다음 중 하나를 수행합니다.

운영 체제	조치
Windows 또는 Linux 클라이언트	클라이언트 애플리케이션의 오른쪽 위 모서리에서 네트워크 아이콘을 선택합니다.
macOS 클라이언트	연결, 네트워크를 선택합니다.

클라이언트 애플리케이션에서 네트워크 연결, 포트 및 왕복 시간을 테스트한 후 이러한 테스트 결과를 보고합니다.

3. 네트워크 대화 상자를 닫아서 로그인 페이지로 돌아갑니다.

1.0+ 및 2.0+ 클라이언트의 네트워킹 요구 사항을 확인하려면

1. WorkSpaces 클라이언트를 엽니다. 이번이 처음 클라이언트를 여는 경우라면 초대 이메일로 받은 등록 코드를 입력하는 메시지가 표시됩니다.
2. 클라이언트 애플리케이션의 오른쪽 아래 모서리에서 네트워크를 선택합니다. 클라이언트 애플리케이션에서 네트워크 연결, 포트 및 왕복 시간을 테스트한 후 이러한 테스트 결과를 보고합니다.
3. 로그인 페이지로 돌아가려면 [Dismiss]를 선택합니다.

신뢰할 수 있는 장치에 WorkSpaces 대한 액세스 제한

기본적으로 사용자는 인터넷에 연결된 지원되는 모든 WorkSpaces 장치에서 액세스할 수 있습니다. 회사에서 신뢰할 수 있는 장치 (관리 대상 장치라고도 함) 에 대한 회사 데이터 액세스를 제한하는 경우 유효한 인증서를 사용하여 신뢰할 수 있는 장치에 WorkSpaces 대한 액세스를 제한할 수 있습니다.

이 기능을 사용하도록 설정하면 인증서 기반 인증을 WorkSpaces 사용하여 장치가 신뢰할 수 있는지 여부를 결정합니다. WorkSpaces 클라이언트 애플리케이션이 디바이스를 신뢰할 수 있는지 확인할 수 없는 경우 디바이스에서 로그인하거나 다시 연결하려는 시도를 차단합니다.

각 디렉터리에 대해 최대 2개의 루트 인증서를 가져올 수 있습니다. 두 개의 루트 인증서를 가져오는 경우 이 두 인증서를 모두 클라이언트에 WorkSpaces 제공하고 클라이언트는 루트 인증서 중 하나에 연결된 유효한 일치하는 첫 번째 인증서를 찾습니다.

지원 클라이언트

- Android 또는 Android 호환 Chrome OS 시스템에서 실행되는 Android
- macOS
- Windows

> **Important**
>
> 이 기능은 다음 클라이언트에서 지원되지 않습니다.
>
> - WorkSpaces Linux 또는 iPad용 클라이언트 애플리케이션

- 서드 파트 클라이언트(Teradici PCoIP, RDP 클라이언트 및 원격 데스크톱 애플리케이션을 포함하나 이에 국한되지 않음)

1단계: 인증서 생성

이 기능은 두 가지 유형의 인증서를 요구합니다. 내부 인증 기관(CA)에 의해 생성된 루트 인증서와 루트 인증서로 이어지는 클라이언트 인증서

요구 사항

- 루트 인증서는 CRT, CERT 또는 PEM 형식의 Base64 인코딩된 인증서 파일이어야 합니다.
- 루트 인증서는 다음과 같은 정규 표현식 패턴을 충족해야 합니다. 즉, 마지막 줄을 제외한 모든 인코딩된 줄의 길이는 정확히 64자여야 합니다. `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`
- 디바이스 인증서는 일반 이름을 포함해야 합니다.
- 디바이스 인증서에는 다음과 같은 확장자가 포함되어야 합니다. `Key Usage: Digital Signature`, `Enhanced Key Usage: Client Authentication`
- 디바이스 인증서에서 신뢰할 수 있는 루트 인증 기관으로 연결되는 체인의 모든 인증서를 클라이언트 디바이스에 설치해야 합니다.
- 지원되는 인증서 체인 최대 길이는 4입니다.
- WorkSpaces 클라이언트 인증서에 대한 CRL (인증서 취소 목록) 또는 OCSP (온라인 인증서 상태 프로토콜) 와 같은 장치 취소 메커니즘은 현재 지원하지 않습니다.
- 강력한 암호화 알고리즘을 사용하십시오. SHA256 with RSA, SHA256 with ECDSA, SHA384 with ECDSA, 또는 SHA512 with ECDSA를 권장합니다.
- macOS의 경우 장치 인증서가 시스템 키체인에 있는 경우 WorkSpaces 클라이언트 애플리케이션이 해당 인증서에 액세스할 수 있도록 승인하는 것이 좋습니다. 그렇지 않을 경우 사용자가 로그인 또는 재연결할 때 키 체인 자격 증명을 입력해야 합니다.

2단계: 신뢰할 수 있는 디바이스에 클라이언트 인증서 배포

사용자를 위한 신뢰할 수 있는 디바이스에는 디바이스 인증서에서 신뢰할 수 있는 루트 인증 기관까지 체인에 있는 모든 인증서가 포함된 인증서 번들을 설치해야 합니다. 선호하는 솔루션(System Center

Configuration Manager(SCCM) 또는 모바일 디바이스 관리(MDM))을 사용하여 클라이언트 디바이스 집합에 인증서를 시할 수 있습니다. 참고로 SCCM 및 MDM은 선택적으로 보안 상태 평가를 수행하여 장치가 회사 액세스 정책을 충족하는지 여부를 확인할 수 있습니다. WorkSpaces

WorkSpaces 클라이언트 애플리케이션은 다음과 같이 인증서를 검색합니다.

- Android - Settings으로 이동하여 Security & location, Credentials를 선택하고 Install from SD card를 선택합니다.
- Android 호환 Chrome OS 시스템 - Android 설정을 열고 Security & location, Credentials를 선택하고 Install from SD card를 선택합니다.
- macOS - 키체인에서 클라이언트 인증서를 검색합니다.
- Windows - 사용자 및 루트 인증서 저장소에서 클라이언트 인증서를 검색합니다.

3단계: 제한 구성

신뢰할 수 있는 디바이스에 클라이언트 인증서를 배포한 후 디렉터리 수준에서 제한된 액세스를 활성화할 수 있습니다. 이를 위해서는 WorkSpaces 클라이언트 애플리케이션이 디바이스의 인증서를 검증해야 사용자가 로그인할 수 있도록 허용할 수 WorkSpace 있습니다.

제한을 구성하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. [Access Control Options]를 확장합니다.
5. 각 장치 유형에서 액세스할 WorkSpaces 수 있는 장치를 지정하고 신뢰할 수 있는 장치를 선택합니다.
6. 최대 2개의 루트 인증서를 가져옵니다. 각 루트 인증서에 대해 다음을 수행합니다.
   a. 가져오기를 선택합니다.
   b. 인증서의 본문을 양식에 복사합니다.
   c. 가져오기를 선택합니다.
7. (선택 사항) 다른 유형의 장치가 액세스할 수 있는지 여부를 지정합니다 WorkSpaces.
   a. 아래로 스크롤하여 Other Platforms(기타 플랫폼) 섹션으로 이동합니다. 기본적으로 WorkSpaces Linux 클라이언트는 비활성화되며 사용자는 iOS 디바이스, Android 디바이스,

웹 액세스, 크롬북 및 PCoIP 제로 클라이언트 WorkSpaces 디바이스에서 액세스할 수 있습니다.

b. 활성화할 디바이스 유형을 선택하고, 비활성화할 디바이스 유형을 선택 취소합니다.

c. 선택한 모든 디바이스 유형으로부터 액세스를 차단하려면 [Block]을 선택합니다.

8. [Update and Exit]를 선택합니다.

SAML 2.0과 WorkSpaces 통합

데스크톱 세션 인증을 위해 SAML 2.0을 WorkSpaces와 통합하면 사용자가 기본 웹 브라우저를 통해 기존 SAML 2.0 ID 제공업체(IdP) 보안 인증 정보와 인증 방법을 사용할 수 있습니다. IdP를 사용하여 WorkSpaces에 사용자를 인증하면 다중 인증 및 상황별 액세스 정책과 같은 IdP 기능을 사용하여 WorkSpaces를 보호할 수 있습니다.

인증 워크플로

다음 섹션에서는 WorkSpaces 클라이언트 애플리케이션, WorkSpaces Web Access 및 SAML 2.0 ID 제공업체(IdP)가 시작하는 인증 워크플로에 대해 설명합니다.

- IdP가 흐름을 시작하는 경우. 사용자가 웹 브라우저의 IdP 사용자 포털에서 애플리케이션을 선택하는 경우를 예로 들 수 있습니다.
- WorkSpaces 클라이언트가 흐름을 시작하는 경우. 사용자가 클라이언트 애플리케이션을 열고 로그인하는 경우를 예로 들 수 있습니다.
- WorkSpaces Web Access가 흐름을 시작하는 경우. 사용자가 브라우저에서 Web Access를 열고 로그인하는 경우를 예로 들 수 있습니다.

이 예시에서는 사용자가 IdP에 로그인하기 위해 `user@example.com`을 입력합니다. IdP에는 WorkSpaces 디렉터리용으로 구성된 SAML 2.0 서비스 제공업체 애플리케이션이 있으며 사용자는 WorkSpaces SAML 2.0 애플리케이션에 대한 권한을 부여받습니다. 사용자는 `user`이라는 사용자 이름과 연결된 WorkSpace를 SAML 2.0 인증이 활성화된 디렉터리에 생성합니다. 또한 사용자가 디바이스에 WorkSpaces 클라이언트 애플리케이션을 설치하거나 웹 브라우저에서 Web Access를 사용합니다.

ID 제공업체(IdP)가 클라이언트 애플리케이션을 사용하여 시작한 흐름

IdP가 시작하는 흐름을 통해 사용자는 WorkSpaces 등록 코드를 입력할 필요 없이 디바이스에서 WorkSpaces 클라이언트 애플리케이션을 자동으로 등록할 수 있습니다. 사용자는 IdP가 시작한 흐름

을 사용하여 WorkSpaces에 로그인하지 않습니다. WorkSpaces 인증은 클라이언트 애플리케이션에서 시작해야 합니다.

1. 사용자는 웹 브라우저를 사용하여 IdP에 로그인합니다.
2. IdP에 로그인한 후 사용자는 IdP 사용자 포털에서 WorkSpaces 애플리케이션을 선택합니다.
3. 사용자는 브라우저에서 이 페이지로 리디렉션되고 WorkSpaces 클라이언트 애플리케이션이 자동으로 열립니다.

4. 이제 WorkSpaces 클라이언트 애플리케이션이 등록되었으며 사용자는 계속해서 WorkSpaces에 로그인을 클릭하여 계속해서 로그인할 수 있습니다.

ID 제공업체(IdP)가 Web Access를 사용하여 시작한 흐름

IdP가 시작하는 Web Access 흐름을 통해 사용자는 WorkSpaces 등록 코드를 입력할 필요 없이 웹 브라우저에서 WorkSpaces를 자동으로 등록할 수 있습니다. 사용자는 IdP가 시작한 흐름을 사용하여 WorkSpaces에 로그인하지 않습니다. WorkSpaces 인증은 Web Access에서 시작되어야 합니다.

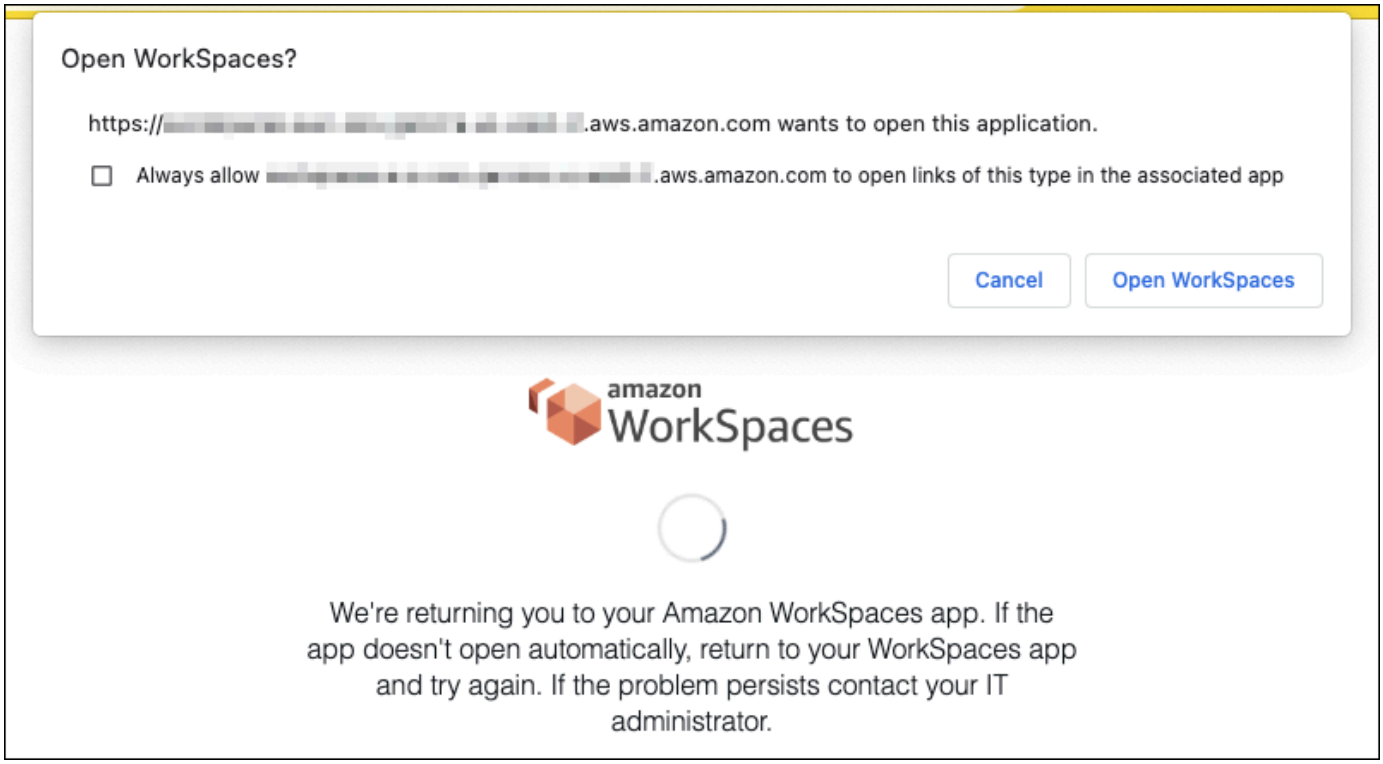
1. 사용자는 웹 브라우저를 사용하여 IdP에 로그인합니다.
2. IdP에 로그인한 후 사용자는 IdP 사용자 포털에서 WorkSpaces 애플리케이션을 클릭합니다.
3. 사용자는 브라우저에서 이 페이지로 리디렉션됩니다. WorkSpaces를 열려면 브라우저에서 Amazon WorkSpaces를 선택합니다.

4. 이제 WorkSpaces 클라이언트 애플리케이션이 등록되었으며 사용자는 WorkSpaces Web Access를 통해 계속해서 로그인할 수 있습니다.

WorkSpaces 클라이언트가 시작한 흐름

클라이언트가 시작하는 흐름을 통해 사용자는 IdP에 로그인한 후 WorkSpaces에 로그인할 수 있습니다.

1. 사용자는 WorkSpaces 클라이언트 애플리케이션이 아직 실행 중이 아닌 경우 애플리케이션을 시작하고 계속해서 WorkSpaces에 로그인을 클릭합니다.
2. 사용자는 기본 웹 브라우저로 리디렉션되어 IdP에 로그인합니다. 사용자가 브라우저에서 이미 IdP에 로그인한 경우 다시 로그인할 필요가 없으며 이 단계를 건너뛰게 됩니다.
3. IdP에 로그인하면 사용자는 팝업으로 리디렉션됩니다. 안내에 따라 웹 브라우저에서 클라이언트 애플리케이션을 열 수 있도록 허용하세요.



4. 사용자는 WorkSpaces 클라이언트 애플리케이션으로 리디렉션되어 WorkSpaces 로그인을 완료합니다. WorkSpaces 사용자 이름은 IdP SAML 2.0 어설션에서 자동으로 채워집니다. 인증서 기반 인증(CBA)을 사용하면 사용자가 자동으로 로그인됩니다.
5. 사용자는 자신의 WorkSpace에 로그인됩니다.

WorkSpaces Web Access가 시작한 흐름

Web Access가 시작하는 흐름을 통해 사용자는 IdP에 로그인한 후 WorkSpaces에 로그인할 수 있습니다.

1. 사용자가 WorkSpaces Web Access를 시작하고 로그인을 선택합니다.
2. 동일한 브라우저 탭에서 사용자는 IdP 포털로 리디렉션됩니다. 사용자가 브라우저에서 이미 IdP에 로그인한 경우 다시 로그인할 필요가 없으며 이 단계를 건너뛸 수 있습니다.
3. IdP에 로그인한 사용자는 브라우저에서 이 페이지로 리디렉션되고 WorkSpaces에 로그인을 클릭합니다.
4. 사용자는 WorkSpaces 클라이언트 애플리케이션으로 리디렉션되어 WorkSpaces 로그인을 완료합니다. WorkSpaces 사용자 이름은 IdP SAML 2.0 어설션에서 자동으로 채워집니다. 인증서 기반 인증(CBA)을 사용하면 사용자가 자동으로 로그인됩니다.
5. 사용자는 자신의 WorkSpace에 로그인됩니다.

SAML 2.0 설정

SAML 2.0을 사용하여 ID 페더레이션을 설정하여 SAML 2.0 ID 공급자 (IdP) 자격 증명과 인증 방법을 사용하여 사용자가 WorkSpaces 클라이언트 애플리케이션을 등록하고 로그인할 수 있도록 합니다. WorkSpaces SAML 2.0을 사용하여 ID 페더레이션을 설정하려면 IAM 역할과 릴레이 상태 URL을 사용하여 IdP를 구성하고 AWS를 활성화합니다. 이렇게 하면 연동 사용자에게 디렉터리 액세스 권한이 부여됩니다. WorkSpaces 릴레이 상태는 로그인에 성공한 사용자가 전달되는 WorkSpaces 디렉터리 엔드포인트입니다. AWS

내용

요구 사항

- SAML 2.0 인증은 다음 리전에서 사용할 수 있습니다.
  - 미국 동부(버지니아 북부) 리전
  - US West (Oregon) Region
  - 아프리카(케이프타운) 리전
  - Asia Pacific (Mumbai) Region
  - Asia Pacific (Seoul) Region
  - 아시아 태평양(싱가포르) 리전
  - 아시아 태평양(시드니) 리전
  - 아시아 태평양(도쿄) 리전
  - 캐나다(중부) 리전
  - Europe (Frankfurt) Region

  - 유럽(아일랜드) 리전
  - Europe (London) Region
  - South America (São Paulo) Region
  - Israel (Tel Aviv) Region
  - AWS GovCloud (미국 서부)
  - AWS GovCloud (미국 동부)
- 에서 SAML 2.0 인증을 사용하려면 IdP가 딥링크 대상 리소스 또는 릴레이 상태 엔드포인트 URL과 WorkSpaces 함께 요청되지 않은 IdP 개시 SSO를 지원해야 합니다. IdPs 예로는 ADFS, Azure AD, 듀오 싱글 사인온, Okta 등이 있습니다. PingFederate PingOne 자세한 내용은 IdP 설명서를 참조하세요.
- SAML 2.0 인증은 Simple AD를 사용하여 WorkSpaces 실행하면 작동하지만 Saml 2.0과 통합되지 않으므로 Saml 2.0 인증은 사용하지 않는 것이 좋습니다. IdPs
- SAML 2.0 인증은 다음 클라이언트에서 지원됩니다. WorkSpaces 다른 클라이언트 버전은 SAML 2.0 인증이 지원되지 않습니다. Amazon WorkSpaces 클라이언트 다운로드를 열어 최신 버전을 찾으십시오.
  - Windows 클라이언트 애플리케이션 버전 5.1.0.3029 이상
  - macOS 클라이언트 버전 5.x 이상
  - 웹 액세스

  폴백이 활성화되지 않는 한 다른 클라이언트 버전에서는 SAML 2.0 인증 WorkSpaces 활성화에 연결할 수 없습니다. 자세한 내용은 디렉터리에서 SAML 2.0 인증 활성화를 참조하십시오. WorkSpaces

ADFS, Azure AD, 듀오 싱글 사인온, Okta 및 PingFederate PingOne 엔터프라이즈용 WorkSpaces 사용과 SAML 2.0을 통합하는 방법에 대한 step-by-step 지침은 Amazon SAML 인증 구현 가이드를 참조하십시오. OneLogin WorkSpaces

필수 조건

디렉터리에 대한 SAML 2.0 ID 공급자 (IdP) 연결을 구성하기 전에 다음 사전 요구 사항을 완료하십시오. WorkSpaces

1. 디렉터리와 함께 사용되는 Microsoft Active Directory의 사용자 ID를 통합하도록 IdP를 구성합니다. WorkSpaces a를 가진 사용자의 경우 WorkSpace Active Directory 사용자의 SaM AccountName 및 이메일 특성과 SAML 클레임 값이 일치해야 사용자가 IdP를 WorkSpaces 사용

하여 로그인할 수 있습니다. Active Directory를 IdP와 통합하는 방법에 대한 자세한 내용은 IdP 설명서를 참조하세요.

2. IdP를 구성하여 와 신뢰 관계를 설정합니다 AWS

   - 페더레이션 구성에 AWS대한 자세한 내용은 타사 SAML 솔루션 공급자 통합을 참조하십시오. AWS 관련 예로는 관리 콘솔에 액세스하기 위한 AWS IAM과의 IdP 통합 등이 있습니다 AWS .
   - IdP를 사용하여 조직을 IdP로 설명하는 페더레이션 메타데이터 문서를 생성하고 다운로드합니다. 이 서명된 XML 문서는 신뢰 당사자 신뢰를 설정하는 데 사용됩니다. 나중에 IAM 콘솔에서 액세스할 수 있는 위치에 이 파일을 저장합니다.

3. WorkSpaces 관리 콘솔을 WorkSpaces 사용하여 디렉토리를 생성하거나 등록하십시오. 자세한 내용은 디렉터리 관리를 참조하십시오. WorkSpaces SAML 2.0 WorkSpaces 인증은 다음 디렉터리 유형에 지원됩니다.

   - AD Connector
   - AWS 관리형 마이크로소프트 AD

4. 지원되는 디렉터리 유형을 사용하여 IdP에 로그인할 수 있는 사용자를 WorkSpace 위한 계정을 생성합니다. WorkSpaces 관리 콘솔 또는 WorkSpaces API를 WorkSpace 사용하여 생성할 수 있습니다. AWS CLI자세한 내용은 를 사용하여 가상 데스크톱 시작을 참조하십시오 WorkSpaces.

1단계: IAM에서 AWS SAML ID 공급자 생성

먼저 IAM에서 SAML IdP를 AWS 생성합니다. 이 IdP는 조직의 IdP 소프트웨어에서 생성한 메타데이터 문서를 사용하여 조직의 IdP와AWS 신뢰 관계를 정의합니다. 자세한 내용은 Creating and managing a SAML identity provider (Amazon Web Services Management Console)를 참조하세요. AWS GovCloud (미국 서부) 및 AWS GovCloud (미국 동부) IdPs 에서 SAML을 사용하는 방법에 대한 자세한 내용은 AWS Identity 및 Access Management를 참조하십시오.

2단계: SAML 2.0 페더레이션 IAM 역할 생성

다음으로 SAML 2.0 페더레이션 IAM 역할을 생성합니다. 이 단계는 IAM과 조직 간에 신뢰 관계를 설정합니다. 이 신뢰 관계에서는 IdP가 페더레이션을 위한 신뢰할 수 있는 엔터티로 식별됩니다.

SAML IdP용 IAM 역할을 생성하는 방법

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할 > 역할 생성을 선택합니다.
3. [Role type]에서 [SAML 2.0 federation]을 선택합니다.

4. SAML 제공업체에서 앞서 생성한 SAML IdP를 선택합니다.

> **Important**
>
> SAML 2.0 액세스 방법으로 프로그래밍 방식 액세스만 허용 또는 프로그래밍 방식 및 Amazon Web Services 관리 콘솔 액세스 허용 중 하나를 선택하지 마세요.

5. [Attribute]에서 [SAML:sub_type]을 선택합니다.
6. 값에 `persistent`를 입력합니다. 이 값은 persistent 값을 갖는 SAML 주체 유형 어설션을 포함하는 SAML 사용자 스트리밍 요청으로 역할 액세스를 제한합니다. SAML:sub_type이 persistent인 경우, IdP는 특정 사용자의 모든 SAML 요청에서 NameID 요소에 대해 동일한 고유한 값을 전송합니다. SAML:sub_type 어설션에 대한 자세한 내용은 API 액세스를 위한 SAML 기반 페더레이션 사용의 SAML 기반 페더레이션에서 사용자 고유 식별 섹션을 참조하십시오. AWS
7. SAML 2.0 신뢰 정보를 검토하여 신뢰할 수 있는 올바른 엔터티와 조건을 확인한 다음 [Next: Permissions]를 선택합니다.
8. Attach permissions policies(권한 정책 연결) 페이지에서 Next: Tags(다음: 태그)를 선택합니다.
9. (선택 사항) 추가할 각 태그의 키와 값을 입력합니다. 자세한 내용은 IAM 사용자 및 역할 태깅을 참조하세요.
10. 완료했으면 Next: Review(다음: 검토)를 선택합니다. 나중에 이 역할의 인라인 정책을 생성하고 포함합니다.
11. 역할 이름에 이 역할의 목적을 나타내는 이름을 입력합니다. 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
12. (선택 사항) Role description(역할 설명)에 새 역할에 대한 설명을 입력합니다.
13. 역할 세부 정보를 검토하고 [Create role]을 선택합니다.
14. 새 IAM 역할의 신뢰 정책에 sts: 권한을 추가합니다. TagSession 자세한 내용은 AWS STS에서 세션 태그 전달을 참조하세요. 새 IAM 역할의 세부 정보에서 신뢰 관계 탭을 선택한 다음 신뢰 관계 편집*을 선택합니다. 신뢰 관계 정책 편집 편집기가 열리면 다음과 같이 sts: TagSession * 권한을 추가합니다.

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

```
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

IDENTITY-PROVIDER를 1단계에서 생성한 SAML IdP의 이름으로 바꿉니다. 그런 다음 신뢰 정책 업데이트를 선택합니다.

3단계: IAM 역할의 인라인 정책 포함

다음으로 생성한 역할의 인라인 IAM 정책을 포함합니다. 인라인 정책을 포함하면 해당 정책의 권한이 잘못된 보안 주체 엔터티에 실수로 추가되는 일을 예방할 수 있습니다. 인라인 정책은 페더레이션 사용자에게 디렉터리 액세스 권한을 제공합니다. WorkSpaces

> **Important**
>
> 소스 IP를 AWS 기반으로 액세스를 관리하는 IAM 정책은 작업에 지원되지 않습니다. workspaces:Stream 에 대한 WorkSpaces IP 액세스 제어를 관리하려면 IP 액세스 제어 그룹을 사용하십시오. 또한 SAML 2.0 인증을 사용하는 경우 SAML 2.0 IdP에서 사용할 수 있는 경우 IP 액세스 제어 정책을 사용할 수 있습니다.

1. 생성한 IAM 역할의 세부 정보에서 권한 탭을 선택한 다음 역할의 권한 정책에 필요한 권한을 추가합니다. 정책 생성 마법사가 시작됩니다.
2. Create policy(정책 생성)에서 JSON 탭을 선택합니다.
3. 다음 JSON 정책을 복사하여 JSON 창에 붙여넣습니다. 그런 다음 AWS 지역 코드, 계정 ID, 디렉터리 ID를 입력하여 리소스를 수정합니다. 다음 정책에는 WorkSpaces 디렉터리의 데스크톱 세

션에 연결할 수 있는 권한을 WorkSpaces 사용자에게 제공하는 작업이 포함됩니다. `"Action": "workspaces:Stream"`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

WorkSpaces디렉터리가 있는 AWS 지역으로 `REGION-CODE` 바꾸십시오. WorkSpaces 관리 콘솔에서 찾을 수 있는 WorkSpaces 디렉터리 `DIRECTORY-ID` ID로 바꾸십시오. AWS GovCloud (미국 서부) 또는 AWS GovCloud (미국 동부) 리소스의 경우 ARN에 다음 형식을 사용하십시오. `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. 완료했으면 Review policy(정책 검토)를 선택합니다. 정책 검증기가 모든 구문 오류를 보고합니다.

4단계: SAML 2.0 ID 제공업체 구성

다음으로, 사용 중인 SAML 2.0 IdP에 따라 https://signin.aws.amazon.com/static/saml-metadata.xml 파일을 IdP에 `saml-metadata.xml` 업로드하여 서비스 제공업체로서 AWS 신뢰할 수 있도록 IdP를 수동으로 업데이트해야 할 수 있습니다. 이 단계는 IdP의 메타데이터를 업데이트합니다. 일부의 IdPs 경우 업데이트가 이미 구성되어 있을 수 있습니다. 이 경우, 다음 단계로 가십시오.

IdP에서 이 업데이트가 아직 구성되어 있지 않다면 IdP가 제공하는 설명서에서 메타데이터 업데이트 방법에 대한 정보를 검토하세요. 일부 공급자는 URL을 입력할 수 있는 옵션을 제공하며, IdP가 자동으로 해당 파일을 획득하고 설치합니다. 다른 IdP들의 경우에는 URL에서 파일을 내려받은 다음 로컬 파일로 제공해야 합니다.

> **Important**
>
> 이때 IdP의 사용자에게 IdP에서 구성한 애플리케이션에 액세스할 WorkSpaces 수 있는 권한을 부여할 수도 있습니다. 디렉터리의 응용 프로그램에 액세스할 수 있는 권한이 있는 사용자는 해당 WorkSpaces 응용 프로그램을 자동으로 WorkSpace 생성하지 않습니다. 마찬가지로, 자신을 위해 WorkSpace 만든 사용자가 자동으로 WorkSpaces 응용 프로그램에 액세스할 수 있는 권한이 부여되지 않습니다. SAML 2.0 인증을 WorkSpace 사용하여 성공적으로 연결하려면 사용자는 IdP의 인증을 받아야 하며 IdP를 생성해야 WorkSpace 합니다.

5단계: SAML 인증 응답을 위한 어설션 생성

다음으로, 인증 응답에서 IdP가 SAML AWS 속성으로 전송하는 정보를 구성합니다. IdP에 따라 이미 구성되어 있는 경우 이 단계를 건너뛰고 6단계: 페더레이션의 릴레이 상태 구성을 진행하세요.

IdP에서 이 정보가 아직 구성되어 있지 않다면 다음을 제공하세요.

- SAML 주체 이름 ID - 로그인하는 사용자의 고유한 식별자입니다. 값은 WorkSpaces 사용자 이름과 일치해야 하며, 일반적으로 Active Directory 사용자의 AccountNameSaM 속성입니다.
- SAML 주체 유형(값이 `persistent`로 설정됨) - 값을 `persistent`로 설정하면 IdP는 특정 사용자의 모든 SAML 요청에서 `NameID` 요소에 대해 동일한 고유한 값을 전송합니다. 2단계: SAML 2.0 페더레이션 IAM 역할 생성에 설명된 것처럼 IAM 정책에는 SAML sub_type이 `persistent`로 설정된 SAML 요청만 허용하는 조건이 포함되어야 합니다.
- **Name** 속성이 **`https://aws.amazon.com/SAML/Attributes/Role`**로 설정된 **Attribute** 요소 - 이 요소는 IAM 역할과 사용자가 IdP에 의해 매핑되는 SAML IdP를 나열하는 1개 이상의 `AttributeValue` 요소를 포함합니다. 역할과 IdP는 쉼표로 구분된 ARN 쌍으로 지정됩니다. 예상 값의 예는 `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`입니다.
- **AttributeName**속성이 로 설정된 요소 **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** - 이 요소에는 SSO용으로 발급되는 AWS 임시 자격 증명의 식별자를 제공하는 `AttributeValue` 요소가 하나 포함되어 있습니다. `AttributeValue` 요소의 값은 2~64자여야 하며 영숫자, 밑줄 및 _ . : / = + - @만 포함할 수 있고 공백은 포함할 수 없습니다. 이 값은 일반적으로 이메일 주소 또는 사용자 보안 주체 이름(UPN)입니다. 사용자의 표시 이름과 같이 값이 공백을 포함하면 안 됩니다.
- **Name** 속성이 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`**로 설정된 **Attribute** 요소 - 이 요소에는 사용자의 이메일 주소를 제공하는 `AttributeValue` 요소 하나

가 포함되어 있습니다. 값은 WorkSpaces 디렉터리에 정의된 WorkSpaces 사용자 이메일 주소와 일치해야 합니다. 태그 값에는 문자, 숫자, 공백 및 _ . : / = + - @ 기호의 조합이 포함될 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 및 AWS STS의 태그 지정 규칙을 참조하세요.

- **Name** 속성이 **https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName**으로 설정된 **Attribute** 요소(선택 사항) - 이 요소에는 로그인하는 사용자에게 Active Directory `userPrincipalName`을 제공하는 `AttributeValue` 요소 하나가 포함되어 있습니다. 제공하는 값의 형식은 `username@domain.com`이어야 합니다. 이 파라미터는 인증서 기반 인증과 함께 최종 사용자 인증서의 주체 대체 이름으로 사용됩니다. 자세한 내용은 인증서 기반 인증을 참조하세요.
- **Name** 속성이 **https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid**로 설정된 **Attribute** 요소(선택 사항) - 이 요소에는 로그인하는 사용자에게 Active Directory 보안 식별자(SID)를 제공하는 `AttributeValue` 요소 하나가 포함되어 있습니다. 이 파라미터는 Active Directory 사용자에 대한 강력한 매핑을 지원하기 위해 인증서 기반 인증과 함께 사용됩니다. 자세한 내용은 인증서 기반 인증을 참조하세요.
- **Name** 속성이 **https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName**으로 설정된 **Attribute** 요소(선택 사항) - 이 요소에는 대체 사용자 이름 형식을 제공하는 `AttributeValue` 요소 하나가 포함되어 있습니다. `corp\usernamecorp.example.com\username`, 또는 같은 사용자 이름 형식이 필요하거나 WorkSpaces 클라이언트를 사용하여 로그인해야 `username@corp.example.com` 하는 사용 사례가 있는 경우 이 속성을 사용하십시오. 태그 키 및 값은 문자, 숫자, 공백 및 _ : / . + = @ - 기호의 조합을 포함할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 및 AWS STS의 태그 지정 규칙을 참조하세요. `corp\username` 또는 `corp.example.com\username` 형식을 클레임하려면 SAML 어설션에서 \를 /로 바꾸세요.
- **AttributeName**속성이 https://aws.amazon.com/SAML/Attributes/:Domain 으로 설정된 요소 PrincipalTag (선택 사항) - 이 요소에는 `AttributeValue` 로그인하는 사용자에게 Active Directory DNS FQDN (정규화된 도메인 이름) 을 제공하는 요소가 하나 포함되어 있습니다. 이 파라미터는 사용자의 Active Directory `userPrincipalName`에 대체 접미사가 포함된 경우 인증서 기반 인증에 사용됩니다. 값은 모든 하위 도메인을 포함하여 `domain.com`에 제공되어야 합니다.
- **AttributeName**속성이 https://aws.amazon.com/SAML/Attributes/ 으로 설정된 요소 SessionDuration (선택 사항) — 이 요소에는 재인증이 필요하기 전에 사용자의 페더레이션된 스트리밍 세션이 활성 상태를 유지할 수 있는 최대 시간을 지정하는 `AttributeValue` 요소 하나가 포함되어 있습니다. 기본값은 3600초(60분)입니다. 자세한 내용은 SAML `SessionDurationAttribute`를 참조하세요.

> **Note**
>
> `SessionDuration`은 선택적 속성이지만 SAML 응답에 포함시키는 것이 좋습니다. 이 속성을 지정하지 않으면 세션 지속 시간이 기본값인 3600초 (60분) 로 설정됩니다. WorkSpaces 세션 기간이 만료되면 데스크톱 세션의 연결이 끊깁니다.

이러한 요소를 구성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 인증 응답을 위한 SAML 어설션 구성을 참조하세요. IdP의 구체적 구성 요구 사항에 대한 자세한 내용은 IdP의 설명서를 참조하세요.

6단계: 페더레이션의 릴레이 상태 구성

그런 다음 IdP를 사용하여 WorkSpaces 디렉터리 릴레이 상태 URL을 가리키도록 페더레이션의 릴레이 상태를 구성합니다. 의 인증에 AWS성공하면 사용자는 SAML 인증 응답에서 릴레이 상태로 정의된 WorkSpaces 디렉터리 엔드포인트로 이동됩니다.

릴레이 상태 URL 형식은 다음과 같습니다.

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

WorkSpaces 디렉터리 등록 코드 및 디렉터리가 위치한 지역과 연결된 릴레이 상태 엔드포인트를 기반으로 릴레이 상태 URL을 구성하십시오. 등록 코드는 WorkSpaces 관리 콘솔에서 찾을 수 있습니다.

선택적으로, 지역 간 리디렉션을 사용하는 경우 등록 코드를 기본 및 WorkSpaces 장애 조치 지역의 디렉터리에 연결된 FQDN (Fully Qualified Domain Name) 으로 대체할 수 있습니다. 자세한 내용은 Amazon의 지역 간 리디렉션을 참조하십시오. WorkSpaces 리전 간 리디렉션과 SAML 2.0 인증을 사용하는 경우 기본 디렉터리와 장애 조치 디렉터리 모두 SAML 2.0 인증을 활성화하고 각 리전과 연결된 릴레이 상태 엔드포인트를 사용하여 IdP를 독립적으로 구성해야 합니다. 이렇게 하면 사용자가 로그인하기 전에 WorkSpaces 클라이언트 애플리케이션을 등록할 때 FQDN을 올바르게 구성하고 장애 조치 이벤트 중에 사용자가 인증할 수 있습니다.

다음 표에는 WorkSpaces SAML 2.0 인증을 사용할 수 있는 지역의 릴레이 상태 엔드포인트가 나열되어 있습니다.

WorkSpaces SAML 2.0 인증을 사용할 수 있는 지역

지역	릴레이 상태 엔드포인트
미국 동부(버지니아 북부) 리전	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) 워크스페이스. euc-sso-fips.us-east-1.aws.amazon.com
US West (Oregon) Region	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) 워크스페이스. euc-sso-fips.us-west-2.aws.amazon.com
아프리카(케이프타운) 리전	workspaces.euc-sso.af-south-1.aws.amazon.com
Asia Pacific (Mumbai) Region	workspaces.euc-sso.ap-south-1.aws.amazon.com
Asia Pacific (Seoul) Region	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
아시아 태평양(싱가포르) 리전	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
아시아 태평양(시드니) 리전	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
아시아 태평양(도쿄) 리전	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
캐나다(중부) 리전	workspaces.euc-sso.ca-central-1.aws.amazon.com
Europe (Frankfurt) Region	workspaces.euc-sso.eu-central-1.aws.amazon.com

지역	릴레이 상태 엔드포인트
Europe (Ireland) Region	workspaces.euc-sso.eu-west-1.aws.amazon.com
Europe (London) Region	workspaces.euc-sso.eu-west-2.aws.amazon.com
South America (São Paulo) Region	workspaces.euc-sso.sa-east-1.aws.amazon.com
Israel (Tel Aviv) Region	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (미국 서부)	• workspaces.euc-sso. us-gov-west-1. amazonaws-us-gov닷컴 • (FIPS) 워크스페이스. euc-sso-fips. us-gov-west-1. amazonaws-us-gov닷컴 **Note** 에 대한 자세한 내용은 AWS GovCloud (미국) 사용 설명서의 WorkSpaces Amazon을 참조하십시오.
AWS GovCloud (미국 동부)	• workspaces.euc-sso. us-gov-east-1. amazonaws-us-gov닷컴 • (FIPS) 워크스페이스. euc-sso-fips. us-gov-east-1. amazonaws-us-gov닷컴 **Note** 에 대한 자세한 내용은 AWS GovCloud (미국) 사용 설명서의 WorkSpaces Amazon을 참조하십시오.

7단계: 디렉터리의 SAML 2.0과의 통합 활성화 WorkSpaces

WorkSpaces 콘솔을 사용하여 디렉터리에서 SAML 2.0 인증을 활성화할 수 있습니다. WorkSpaces

SAML 2.0과의 통합을 활성화하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 내 디렉터리 ID를 선택하세요 WorkSpaces.
4. 인증에서 편집을 선택합니다.
5. SAML 2.0 ID 제공업체 편집을 선택합니다.
6. SAML 2.0 인증 활성화를 선택합니다.
7. 사용자 액세스 URL 및 IdP 딥링크 파라미터 이름에 1단계에서 구성한 IdP 및 애플리케이션에 적용할 수 있는 값을 입력합니다. 이 매개변수를 생략한 경우 IdP 딥링크 매개변수 이름의 기본값은 RelayState “”입니다. 다음 표에는 애플리케이션의 다양한 ID 제공업체에 고유한 사용자 액세스 URL 및 파라미터 이름이 나와 있습니다.

   허용 목록에 추가할 도메인 및 IP 주소

ID 제공업체	파라미터	사용자 액세스 URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`

ID 제공업체	파라미터	사용자 액세스 URL
Okta	RelayState	https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/<app-id>
Auth0	RelayState	https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>
PingFederate	TargetResource	https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>
PingOne 엔터프라이즈용	TargetResource	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>

사용자 액세스 URL은 일반적으로 요청되지 않고 IdP가 시작한 SSO의 제공업체가 정의합니다. 사용자는 웹 브라우저에 이 URL을 입력하여 SAML 애플리케이션에 직접 페더레이션할 수 있습니다. IdP의 사용자 액세스 URL과 파라미터 값을 테스트하려면 테스트를 선택합니다. 테스트 URL을 복사하여 현재 브라우저 또는 다른 브라우저의 개인 창에 붙여넣으면 현재 AWS 관리 콘솔 세션을 중단하지 않고 SAML 2.0 로그온을 테스트할 수 있습니다. IdP에서 시작한 플로우가 열리면

클라이언트를 등록할 수 있습니다. WorkSpaces 자세한 내용은 ID 제공업체(IdP)가 시작한 흐름을 참조하세요.

8. SAML 2.0을 지원하지 않는 클라이언트의 로그인 허용을 선택하거나 선택 취소하여 대체 설정을 관리합니다. SAML 2.0을 지원하지 않는 클라이언트 유형 또는 버전을 WorkSpaces 사용할 수 있는 액세스 권한을 사용자에게 계속 제공하거나 사용자가 최신 클라이언트 버전으로 업그레이드할 시간이 필요한 경우 이 설정을 활성화합니다.

> **Note**
>
> 이 설정을 통해 사용자는 SAML 2.0을 우회하고 이전 클라이언트 버전을 사용하여 디렉터리 인증으로 로그인할 수 있습니다.

9. 웹 클라이언트에서 SAML을 사용하려면 Web Access를 활성화합니다. 자세한 내용은 Amazon WorkSpaces Web Access 활성화 및 구성을 참조하십시오.

> **Note**
>
> SAML을 사용하는 PCoIP는 Web Access에서 지원되지 않습니다.

10. 저장을 선택합니다. 이제 WorkSpaces 디렉토리가 SAML 2.0 통합으로 활성화되었습니다. IdP에서 시작한 흐름과 클라이언트 응용 프로그램에서 시작한 흐름을 사용하여 클라이언트 응용 프로그램을 WorkSpaces 등록하고 로그인할 수 있습니다. WorkSpaces

인증서 기반 인증

에서 인증서 기반 인증을 사용하여 Active Directory 도메인 암호를 묻는 사용자 WorkSpaces 프롬프트를 제거할 수 있습니다. Active Directory 도메인에서 인증서 기반 인증을 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- SAML 2.0 ID 제공업체를 통해 사용자를 인증하고 Active Directory의 사용자와 매칭하도록 SAML 어설션을 제공할 수 있습니다.
- 사용자 프롬프트 수를 줄여 Single Sign-On 로그온 경험을 구현할 수 있습니다.
- SAML 2.0 ID 제공업체를 사용하여 암호 없는 인증 흐름을 활성화할 수 있습니다.

인증서 기반 인증은 계정의 리소스를 사용합니다. AWS Private CA AWS AWS Private CA 루트 및 하위 CA를 포함한 사설 CA (인증 기관) 계층 구조를 생성할 수 있습니다. 를 사용하면 고유한 CA 계층

구조를 만들고 이를 사용하여 내부 사용자를 인증하는 데 사용할 인증서를 발급할 수 있습니다. AWS Private CA자세한 내용은 AWS Private Certificate Authority 사용 설명서를 참조하십시오.

를 인증서 기반 AWS Private CA 인증에 사용하는 경우 세션 인증 WorkSpaces 중에 자동으로 사용자의 인증서를 요청합니다. 사용자는 인증서로 프로비저닝된 가상 스마트 카드를 사용하여 Active Directory에 인증됩니다.

인증서 기반 인증은 최신 WorkSpaces 웹 액세스, Windows 및 macOS 클라이언트 애플리케이션을 사용하는 Windows WorkSpaces 온 WorkSpaces 스트리밍 프로토콜 (WSP) 번들에서 지원됩니다. Amazon WorkSpaces Client 다운로드를 열어 최신 버전을 찾으십시오.

- Windows 클라이언트 버전 5.5.0 이상
- macOS 클라이언트 버전 5.6.0 이상

Amazon에서 인증서 기반 인증을 구성하는 방법에 대한 자세한 내용은 WorkSpaces Amazon의 인증서 기반 인증을 구성하는 방법 및 규제가 엄격한 2.0 및 인증 기반 인증에 대한 엄격한 규제 환경에서의 설계 고려 사항을 참조하십시오. WorkSpaces AppStream WorkSpaces

필수 조건

인증서 기반 인증을 활성화하기 전에 다음 단계를 완료하세요.

1. 인증서 기반 인증을 사용하도록 SAML WorkSpaces 2.0 통합으로 디렉토리를 구성하십시오. 자세한 내용은 SAML WorkSpaces2.0과의 통합을 참조하십시오.
2. SAML 어설션에서 `userPrincipalName` 속성을 구성합니다. 자세한 내용은 인증 응답을 위한 SAML 어설션 생성을 참조하세요.
3. SAML 어설션에서 `ObjectSid` 속성을 구성합니다. 이는 Active Directory 사용자에 대한 강력한 매핑을 수행하기 위한 선택 사항입니다. 속성이 SAML_Subject `NameID`에 지정된 사용자의 Active Directory 보안 식별자(SID)와 매칭되지 않으면 인증서 기반 인증이 실패합니다. 자세한 내용은 인증 응답을 위한 SAML 어설션 생성을 참조하세요.
4. SAML 2.0 구성에서 사용되는 IAM 역할 신뢰 정책이 아직 없는 경우 sts: TagSession 권한을 추가하십시오. 인증서 기반 인증을 사용하려면 이 권한이 필요합니다. 자세한 내용은 SAML 2.0 페더레이션 IAM 역할 생성을 참조하세요.
5. Active Directory에 사설 인증 기관 (CA) 을 구성하지 않은 AWS Private CA 경우 이를 사용하여 사설 인증 기관 (CA) 을 생성하십시오. AWS Private CA 인증서 기반 인증을 사용하려면 필요합니다. 자세한 내용은 AWS Private CA 배포 계획을 참조하고 지침에 따라 인증서 기반 인증을 위한 CA를 구

성하십시오. 인증서 기반 인증 사용 사례에 가장 일반적으로 사용되는 AWS Private CA 설정은 다음과 같습니다.

a. CA 유형 옵션:

   i. 수명이 짧은 인증서 CA 사용 모드(인증서 기반 인증을 위한 최종 사용자 인증서를 발급하는 데만 CA를 사용하는 경우 권장)

   ii. 루트 CA를 사용한 단일 수준 계층 구조(또는 기존 CA 계층 구조와 통합하려는 경우 하위 CA 선택)

b. 키 알고리즘 옵션: RSA 2048

c. 주체 고유 이름 옵션: Active Directory Trusted Root Certification Authorities 저장소에서 CA를 식별하려면 원하는 옵션을 조합하여 사용하세요.

d. 인증서 취소 옵션: CRL 배포

> **Note**
>
> 인증서 기반 인증을 사용하려면 데스크톱과 도메인 컨트롤러에서 액세스할 수 있는 온라인 CRL 배포 지점이 필요합니다. 이를 위해서는 사설 CA CRL 항목용으로 구성된 Amazon S3 버킷에 대한 인증되지 않은 액세스 또는 퍼블릭 액세스를 차단하는 경우 S3 버킷에 액세스할 수 있는 CloudFront 배포가 필요합니다. 옵션에 대한 자세한 내용은 Planning a certificate revocation list (CRL)를 참조하세요.

6. EUC 인증서 기반 인증에 사용할 CA를 지정할 `euc-private-ca` 키로 프라이빗 CA에 태그를 지정하세요. 이 키에는 값이 필요하지 않습니다. 자세한 내용은 Managing tags for your private CA를 참조하세요.

7. 인증서 기반 인증은 로그온에 가상 스마트 카드를 사용합니다. Active Directory에서 Guidelines for enabling smart card logon with third-party certification authorities를 따라 다음 단계를 수행하세요.

   - 도메인 컨트롤러 인증서를 사용하여 도메인 컨트롤러를 구성하여 스마트 카드 사용자를 인증합니다. Active Directory에 Active Directory Certificate Services 엔터프라이즈 CA가 구성되어 있는 경우 스마트 카드 로그온을 활성화하기 위해 인증서가 도메인 컨트롤러에 자동으로 등록됩니다. Active Directory Certificate Services가 없는 경우 Requirements for domain controller certificates from a third-party CA를 참조하세요. AWS Private CA를 사용하여 도메인 컨트롤러 인증서를 만들 수 있습니다. 이렇게 하는 경우 수명이 짧은 인증서용으로 구성된 프라이빗 CA를 사용하지 마세요.

> **Note**
>
> 를 사용하는 AWS Managed Microsoft AD경우 도메인 컨트롤러 인증서 요구 사항을 충족하도록 EC2 인스턴스에서 인증서 서비스를 구성할 수 있습니다. AWS Launch Wizard예를 들어 Active Directory 인증서 서비스를 사용하여 AWS Managed Microsoft AD 구성된 배포의 예를 참조하십시오. AWS 사설 CA는 Active Directory 인증서 서비스 CA의 하위 CA로 구성하거나 사용 시 자체 루트로 구성할 수 있습니다. AWS Managed Microsoft AD Active Directory 인증서 서비스를 통한 AWS Managed Microsoft AD 추가 구성 작업은 컨트롤러 VPC 보안 그룹에서 인증서 서비스를 실행하는 EC2 인스턴스로 아웃바운드 규칙을 생성하여 TCP 포트 135 및 49152-65535가 인증서 자동 등록을 활성화할 수 있도록 하는 것입니다. 또한 실행 중인 EC2 인스턴스는 도메인 컨트롤러를 포함한 도메인 인스턴스로부터 동일한 포트에 대한 인바운드 액세스를 허용해야 합니다. 보안 그룹을 찾는 방법에 대한 자세한 내용은 VPC 서브넷 및 보안 그룹 구성을 AWS Managed Microsoft AD 참조하십시오.

- AWS Private CA 콘솔에서 또는 SDK 또는 CLI를 사용하여 CA를 선택하고 CA 인증서 아래에서 CA 사설 인증서를 내보냅니다. 자세한 내용은 프라이빗 인증서 내보내기를 참조하세요.
- CA를 Active Directory에 게시합니다. 도메인 컨트롤러 또는 도메인에 조인된 시스템에 로그온합니다. CA 프라이빗 인증서를 원하는 `<path>\<file>`에 복사하고 도메인 관리자로 다음 명령을 실행합니다. 또는 그룹 정책 및 Microsoft PKI Health Tool(PKiView) 도구를 사용하여 CA를 게시할 수도 있습니다. 자세한 내용은 Configuration instructions를 참조하세요.

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

명령이 성공적으로 완료되었는지 확인한 다음 프라이빗 인증서 파일을 제거합니다. Active Directory 복제 설정에 따라 CA를 도메인 컨트롤러와 데스크톱 인스턴스에 게시하는 데 몇 분 정도 걸릴 수 있습니다.

> **Note**
>
> - WorkSpaces 데스크톱이 도메인에 가입되면 Active Directory에서 신뢰할 수 있는 루트 인증 기관 및 엔터프라이즈 NTAuth 저장소에 CA를 자동으로 배포해야 합니다.
> - 인증서 기반 인증을 지원하려면 Active Directory 도메인 컨트롤러가 강력한 인증서 적용에 대한 호환 모드에 있어야 합니다. 자세한 내용은 Microsoft 지원 설명서에서 KB5014754 - Windows 도메인 컨트롤러의 인증서 기반 인증 변경을 참조하십시오.

AWS 관리형 Microsoft AD를 사용하는 경우 자세한 내용은 디렉터리 보안 설정 구성을 참조하십시오.

인증서 기반 인증 활성화

인증서 기반 인증을 활성화하려면 다음 단계를 완료하세요.

1. 에서 WorkSpaces 콘솔을 엽니다https://console.aws.amazon.com/workspaces.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 내 디렉터리 ID를 선택합니다 WorkSpaces.
4. 인증에서 편집을 클릭합니다.
5. 인증서 기반 인증 편집을 클릭합니다.
6. 인증서 기반 인증 활성화를 선택합니다.
7. 프라이빗 CA ARN이 목록에 연결되어 있는지 확인합니다. 사설 CA는 동일한 AWS 계정에 있어야 AWS 리전하며 목록에 표시될 권한이 있는 키로 태그를 euc-private-ca 지정해야 합니다.
8. 변경 사항 저장을 클릭합니다. 인증서 기반 인증이 이제 활성화됩니다.
9. 변경 사항을 적용하려면 Windows WorkSpaces 온 WorkSpaces 스트리밍 프로토콜 (WSP) 번들을 재부팅하십시오. 자세한 내용은 재부팅 a를 참조하십시오. WorkSpace
10. 재부팅 후 지원되는 클라이언트를 사용하여 SAML 2.0을 통해 인증하면 도메인 암호를 입력하라는 메시지가 더 이상 표시되지 않습니다.

> **Note**
>
> 인증서 기반 인증으로 로그인할 수 있는 경우 디렉터리에 MFA (멀티 팩터 인증) 를 WorkSpaces 사용하도록 설정했더라도 사용자에게 MFA (멀티 팩터 인증) 를 입력하라는 메시지가 표시되지 않습니다. 인증서 기반 인증을 사용하는 경우 SAML 2.0 ID 제공업체를 통해 MFA를 활성화할 수 있습니다. AWS Directory Service MFA에 대한 자세한 내용은 다단계 인증 (AD Connector) 또는 다단계 인증 활성화를 참조하십시오. AWS Managed Microsoft AD

인증서 기반 인증 관리

CA 인증서

일반적인 구성에서 프라이빗 CA 인증서의 유효 기간은 10년입니다. 만료된 인증서가 포함된 CA를 교체하거나 CA를 새 유효 기간으로 재발급하는 방법에 대한 자세한 내용은 Managing the private CA lifecycle 참조하세요.

최종 사용자 인증서

에서 WorkSpaces 인증서 기반 인증을 AWS Private CA 위해 발급한 최종 사용자 인증서는 갱신이나 해지가 필요하지 않습니다. 이러한 인증서는 수명이 짧습니다. WorkSpaces24시간마다 새 인증서를 자동으로 발급합니다. 이러한 최종 사용자 인증서는 일반적인 AWS Private CA CRL 배포보다 유효 기간이 짧습니다. 따라서 최종 사용자 인증서를 취소할 필요가 없으며 CRL에 표시되지 않습니다.

감사 보고서

프라이빗 CA가 발급 또는 취소한 모든 인증서를 나열하는 감사 보고서를 만들 수 있습니다. 자세한 내용은 프라이빗 CA에서 감사 보고서 사용을 참조하세요.

로깅 및 모니터링

를 사용하여 AWS CloudTrail AWS Private CA WorkSpacesby에 대한 API 호출을 기록할 수 있습니다. 자세한 내용은 사용을 참조하십시오 CloudTrail. CloudTrail이벤트 기록에서 WorkSpaces `EcmAssumeRoleSession` 사용자 이름으로 만든 `IssueCertificate` 이벤트 소스의 `acm-pca.amazonaws.com` 이벤트 이름을 볼 `GetCertificate` 수 있습니다. 이러한 이벤트는 모든 EUC 인증서 기반 인증 요청에 대해 기록됩니다.

계정 간 PCA 공유를 활성화합니다.

사설 CA 계정 간 공유를 사용하는 경우 다른 계정에 중앙 집중식 CA를 사용할 수 있는 권한을 부여할 수 있으므로 모든 계정에 사설 CA가 필요하지 않습니다. CA는 AWS Resource Access Manager를 사용하여 권한을 관리함으로써 인증서를 생성하고 발급할 수 있습니다. 사설 CA 계정 간 공유는 동일한 지역 내에서 WorkSpaces 인증서 기반 인증 (CBA) 과 함께 사용할 수 있습니다. AWS

공유 사설 CA 리소스를 CBA와 함께 사용하려면 WorkSpaces

1. 중앙 AWS 계정에서 CBA용 사설 CA를 구성하십시오. 자세한 정보는 인증서 기반 인증을 참조하세요.
2. AWS RAM을 사용하여 ACM 사설 CA 교차 AWS 계정을 공유하는 방법의 단계에 따라 WorkSpaces 리소스가 CBA를 활용하는 자원 계정과 사설 CA를 공유하십시오. 인증서를 생성하기 위해 3단계를 완료할 필요는 없습니다. 사설 CA를 개별 AWS 계정과 공유하거나 Organizations를 통해 AWS 공유할 수 있습니다. 개별 계정과 공유하려면 Resource

Access Manager (RAM) 콘솔 또는 API를 사용하여 자원 계정의 공유 사설 CA를 수락해야 합니다. 공유를 구성할 때 리소스 계정의 사설 CA에 대한 RAM 리소스 공유가 `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` 관리 권한 템플릿을 사용하고 있는지 확인하십시오. 이 템플릿은 CBA 인증서를 발급할 때 WorkSpaces 서비스 역할이 사용하는 PCA 템플릿과 일치합니다.

3. 공유에 성공하면 자원 계정의 사설 CA 콘솔을 사용하여 공유 사설 CA를 볼 수 있어야 합니다.
4. API 또는 CLI를 사용하여 디렉터리 속성에서 사설 CA ARN을 CBA와 연결합니다. WorkSpaces 현재 WorkSpaces 콘솔에서는 공유 사설 CA ARN 선택을 지원하지 않습니다. CLI 명령의 예:

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

인증에 스마트 카드 사용

Windows 및 Linux WorkSpaces 온 WorkSpaces 스트리밍 프로토콜 (WSP) 번들을 사용하면 CAC (공용 액세스 카드) 및 PIV (개인 신원 확인) 스마트 카드를 인증에 사용할 수 있습니다.

Amazon은 세션 전 인증과 세션 내 인증 모두에 스마트 카드 사용을 WorkSpaces 지원합니다. 사전 세션 인증은 사용자가 로그인하는 동안 수행되는 스마트 카드 인증을 말합니다. WorkSpaces 세션 내 인증은 로그인 후 수행되는 인증을 말합니다.

예를 들어 사용자는 웹 브라우저 및 애플리케이션으로 작업하는 동안 세션 내 인증에 스마트 카드를 사용할 수 있습니다. 또한 관리자 권한이 필요한 작업에 스마트 카드를 사용할 수도 있습니다. 예를 들어 WorkSpace Linux에 대한 관리자 권한이 있는 사용자는 스마트 카드를 사용하여 명령을 `sudo` 실행하고 `sudo -i` 실행할 때 자신을 인증할 수 있습니다.

내용

요구 사항

- 세션 전 인증에는 Active Directory Connector(AD Connector) 디렉터리가 필요합니다. AD Connector는 인증서 기반 상호 전송 계층 보안(상호 TLS) 인증을 사용하여 하드웨어 또는 소프트웨어 기반 스마트 카드 인증서를 사용하여 Active Directory에 사용자를 인증합니다. AD Connector 및 온프레미스 디렉터리를 구성하는 방법에 대한 자세한 내용은 디렉터리 구성 섹션을 참조하세요.
- Windows 또는 WorkSpace Linux에서 스마트 카드를 사용하려면 사용자는 Amazon WorkSpaces Windows 클라이언트 버전 3.1.1 이상 또는 WorkSpaces macOS 클라이언트 버전 3.1.5 이상을 사용해야 합니다. Windows 및 macOS 클라이언트에서 스마트 카드를 사용하는 방법에 대한 자세한 내용은 Amazon 사용 WorkSpaces 설명서의 스마트 카드 지원을 참조하십시오.
- 루트 CA 및 스마트 카드 인증서는 특정 요구 사항을 충족해야 합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 스마트 카드와 함께 사용할 수 있도록 TLS 인증 활성화) 및 Microsoft 설명서의 Certificate Requirements를 참조하세요.

  이러한 요구 사항 외에도 Amazon에 대한 스마트 카드 인증에 사용되는 사용자 인증서에는 다음 속성이 WorkSpaces 포함되어야 합니다.

  - 인증서의 userPrincipalName (SAN) 필드에 있는 AD 사용자 subjectAltName (UPN) 사용자의 기본 UPN에 대해 스마트 카드 인증서를 발급하는 것이 좋습니다.
  - 클라이언트 인증(1.3.6.1.5.5.7.3.2) 확장 키 사용(EKU) 속성.
  - 스마트 카드 로그온(1.3.6.1.4.1.311.20.2.2) EKU 속성.
- 세션 전 인증의 경우 인증서 해지 검사에 온라인 인증서 상태 프로토콜(OCSP)이 필요합니다. 세션 내 인증의 경우 OCSP가 권장되지만 필수는 아닙니다.

제한 사항

- 현재 스마트 카드 인증에는 WorkSpaces Windows 클라이언트 응용 프로그램 버전 3.1.1 이상 및 macOS 클라이언트 응용 프로그램 버전 3.1.5 이상만 지원됩니다.
- WorkSpaces Windows 클라이언트 응용 프로그램 3.1.1 이상은 클라이언트가 64비트 버전의 Windows에서 실행되는 경우에만 스마트 카드를 지원합니다.
- WorkSpaces Ubuntu는 현재 스마트 카드 인증을 지원하지 않습니다.
- 현재 AD Connector 디렉터리만 스마트 카드 인증에 지원됩니다.
- 세션 내 인증은 WSP가 지원되는 모든 리전에서 사용 가능합니다. 세션 전 인증은 다음 리전에서 사용할 수 있습니다.
  - 아시아 태평양(시드니) 리전

- 아시아 태평양(도쿄) 리전
- Europe (Ireland) Region
- AWS GovCloud (미국 동부) 지역
- AWS GovCloud (미국 서부) 지역
- 미국 동부(버지니아 북부) 리전
- US West (Oregon) Region

- Linux 또는 Windows의 세션 내 인증 및 세션 전 인증의 WorkSpaces 경우 현재 한 번에 하나의 스마트 카드만 허용됩니다.
- 세션 전 인증의 경우 동일한 디렉터리에서 스마트 카드 인증과 로그인 인증을 모두 활성화하는 것은 현재 지원되지 않습니다.
- 현재는 CAC 및 PIV 카드만 지원됩니다. 다른 유형의 하드웨어 또는 소프트웨어 기반 스마트 카드는 작동할 수 있지만, WSP와 함께 사용할 수 있도록 완전히 테스트되지는 않았습니다.

디렉터리 구성

스마트 카드 인증을 사용하려면 다음과 같은 방법으로 AD Connector 디렉터리와 온프레미스 디렉터리를 구성해야 합니다.

AD Connector 디렉터리 구성

시작하기 전에 AWS Directory Service 관리 안내서의 AD Connector 사전 조건에 설명된 대로 AD Connector 디렉터리를 설정했는지 확인하세요. 특히 방화벽에서 필요한 포트를 열었는지 확인하세요.

AD Connector 디렉터리 구성을 완료하려면 AWS Directory Service 관리 안내서에서 스마트 카드와 함께 사용할 수 있도록 AD Connector에서 mTLS 인증 활성화의 지침을 따르세요.

> **Note**
>
> 스마트 카드 인증이 제대로 작동하려면 Kerberos 제한 위임(KCD)이 필요합니다. KCD를 사용하려면 AD Connector 서비스 계정의 사용자 이름 부분이 동일한 사용자의 AccountName SAM과 일치해야 합니다. SaM은 20자를 AccountName 초과할 수 없습니다.

온프레미스 디렉터리 구성

AD Connector 디렉터리를 구성하는 것 외에도 온프레미스 디렉터리의 도메인 컨트롤러에 발급되는 인증서에 'KDC Authentication' 확장 키 사용(EKU)이 설정되어 있는지도 확인해야 합니다. 이렇게 하려

면 Active Directory 도메인 서비스(AD DS)의 기본 Kerberos 인증 인증서 템플릿을 사용하세요. 도메인 컨트롤러 인증서 템플릿이나 도메인 컨트롤러 인증 인증서 템플릿은 스마트 카드 인증에 필요한 설정이 포함되어 있지 않으므로 사용하지 마세요.

Windows용 스마트 카드를 활성화합니다. WorkSpaces

Windows에서 스마트 카드 인증을 활성화하는 방법에 대한 일반적인 지침은 Microsoft 설명서의 Guidelines for enabling smart card logon with third-party certification authorities를 참조하세요.

Windows 잠금 화면을 감지하고 세션 연결을 해제하는 방법

화면이 잠겨 있을 때 스마트 카드 사전 인증이 활성화된 WorkSpaces Windows를 사용자가 잠금 해제할 수 있도록 하려면 사용자 세션에서 Windows 잠금 화면 감지를 사용하도록 설정할 수 있습니다. Windows 잠금 화면이 감지되면 WorkSpace 세션 연결이 끊기고 사용자는 스마트 카드를 사용하여 WorkSpaces 클라이언트에 다시 연결할 수 있습니다.

그룹 정책 설정을 사용하여 Windows 잠금 화면이 감지될 때 세션 연결 해제를 활성화할 수 있습니다. 자세한 설명은 WSP에서 화면 잠금 시 세션 연결 해제 활성화 또는 비활성화 섹션을 참조하세요.

세션 내 또는 세션 전 인증을 활성화하는 방법

기본적으로 WorkSpaces Windows는 사전 세션 또는 세션 내 인증을 위한 스마트 카드 사용을 지원하지 않습니다. 필요한 경우 그룹 정책 설정을 사용하여 WorkSpaces Windows에 대한 세션 내 및 사전 세션 인증을 활성화할 수 있습니다. 자세한 설명은 WSP에서 스마트 카드 리디렉션 활성화 또는 비활성화 섹션을 참조하세요.

세션 전 인증을 사용하려면 그룹 정책 설정을 업데이트하는 것 외에도 AD Connector 디렉터리 설정을 통해 세션 전 인증을 활성화해야 합니다. 자세한 내용은 AWS Directory Service 관리 안내서에서 스마트 카드와 함께 사용할 수 있도록 AD Connector에서 mTLS 인증 활성화의 지침을 따르세요.

사용자가 브라우저에서 스마트 카드를 사용할 수 있게 하는 방법

사용자가 Chrome 브라우저를 사용하는 경우 스마트 카드를 사용하기 위한 특별한 구성이 필요하지 않습니다.

사용자가 Firefox 브라우저를 사용하는 경우 그룹 정책을 통해 사용자가 Firefox에서 스마트 카드를 사용하도록 할 수 있습니다. 에서 이러한 Firefox 그룹 정책 템플릿을 사용할 수 있습니다. GitHub

예를 들어 PKCS #11 지원을 위해 Windows에 OpenSC 64비트 버전을 설치한 후 다음 그룹 정책 설정을 사용할 수 있습니다. 여기서 *NAME_OF_DEVICE*는 PKCS #11 식별에 사용할 값(예: OpenSC) 이고, *PATH_TO_LIBRARY_FOR_DEVICE*는 PKCS #11 모듈의 경로입니다. 이 경로는 확장자가 .DLL

인 라이브러리(예: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`)를 가리켜야 합니다.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

OpenSC를 사용하는 경우 `pkcs11-register.exe` 프로그램을 실행하여 OpenSC `pkcs11` 모듈을 Firefox에 로드할 수도 있습니다. 이 프로그램을 실행하려면 `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe`에서 파일을 두 번 클릭하거나 명령 프롬프트 창을 열고 다음 명령을 실행합니다.

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

OpenSC `pkcs11` 모듈이 Firefox에 로드되었는지 확인하려면 다음을 수행합니다.

1. Firefox가 이미 실행 중이면 종료하세요.
2. Firefox를 엽니다. 오른쪽 상단 모서리의 메뉴 버튼 ( ) 을 선택한 다음 옵션을 선택합니다.
3. about:preferences 페이지의 왼쪽 탐색 창에서 개인 정보 및 보안을 선택합니다.
4. 인증서에서 보안 디바이스를 선택합니다.
5. 디바이스 관리자 대화 상자의 왼쪽 탐색 창에 OpenSC 스마트 카드 프레임워크(0.21)가 표시되며, 이 프레임워크를 선택하면 다음 값이 있을 것입니다.

   모듈: `OpenSC smartcard framework (0.21)`

   경로: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

문제 해결

스마트 카드 문제 해결에 대한 자세한 내용은 Microsoft 설명서의 Certificate and configuration problems를 참조하세요.

문제를 일으킬 수 있는 일반적인 문제는 다음과 같습니다.

- 슬롯을 인증서에 잘못 매핑했습니다.
- 스마트 카드에 사용자와 매칭될 수 있는 인증서가 여러 개입니다. 인증서는 다음 기준을 사용하여 매칭됩니다.
  - 인증서의 루트 CA.
  - 인증서의 <KU> 및 <EKU> 필드.
  - 인증서 주체의 UPN.
- 키 사용에 <EKU>msScLogin이 있는 인증서가 여러 개입니다.

일반적으로 스마트 카드의 첫 번째 슬롯에 매핑되는 스마트 카드 인증용 인증서를 하나만 사용하는 것이 가장 좋습니다.

스마트 카드의 인증서 및 키를 관리(예: 인증서 및 키 제거 또는 재매핑)하는 도구는 제조업체마다 다를 수 있습니다. 자세한 내용은 스마트 카드 제조업체에서 제공하는 설명서를 참조하세요.

Linux용 스마트 카드 활성화 WorkSpaces

> **Note**
>
> WSP WorkSpaces 기반 Linux에는 현재 다음과 같은 제한 사항이 있습니다.
>
> - 클립보드, 오디오 입력, 비디오 입력 및 시간대 리디렉션이 지원되지 않습니다.
> - 다중 모니터가 지원되지 않습니다.
> - WSP에서 WorkSpaces Linux에 연결하려면 WorkSpaces Windows 클라이언트 애플리케이션을 사용해야 합니다.

WorkSpacesLinux에서 스마트 카드를 사용할 수 있게 하려면 이미지에 PEM 형식의 루트 CA 인증서 파일을 포함해야 합니다. WorkSpace

루트 CA 인증서를 받는 방법

여러 가지 방법으로 루트 CA 인증서를 받을 수 있습니다.

- 서드 파티 인증 기관에서 운영하는 루트 CA 인증서를 사용할 수 있습니다.
- 웹 등록 사이트(http://*ip_address*/certsrv 또는 http://*fqdn*/certsrv)를 사용하여 자체 루트 CA 인증서를 내보낼 수 있습니다. *ip_address* 및 *fqdn*은 루트 인증서 CA 서버의 IP 주소와

정규화된 도메인 이름(FQDN)입니다. 웹 등록 사이트 사용에 대한 자세한 내용은 Microsoft 설명서의 How to export a Root Certification Authority Certificate을 참조하세요.

- 다음 절차에 따라 Active Directory Certificate Services(AD CS)를 실행하는 루트 CA 인증 서버에서 루트 CA 인증서를 내보낼 수 있습니다. AD CS 설치에 대한 자세한 내용은 Microsoft 설명서의 Install the Certification Authority를 참조하세요.

  1. 관리자 계정을 사용하여 루트 CA 서버에 로그인합니다.
  2. Windows Start 메뉴에서 명령 프롬프트 창을 엽니다(Start > Windows System > Command Prompt).
  3. 다음 명령을 사용하여 루트 CA 인증서를 새 파일로 내보냅니다. 여기서 *rootca*.cer는 새 파일의 이름입니다.

     ```
     certutil -ca.cert rootca.cer
     ```

     certutil을 실행하는 방법에 대한 자세한 내용은 Microsoft 설명서의 certutil을 참조하세요.
  4. 다음 OpenSSL 명령을 사용하여 내보낸 루트 CA 인증서를 DER 형식에서 PEM 형식으로 변환합니다. 여기서 *rootca*는 인증서 이름입니다. OpenSSL에 대한 자세한 내용은 www.openssl.org를 참조하세요.

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

Linux에 루트 CA 인증서를 추가하려면 WorkSpaces

스마트 카드를 활성화하는 데 도움이 되도록 Amazon Linux WSP 번들에 `enable_smartcard` 스크립트를 추가했습니다. 이 스크립트는 다음 작업을 수행합니다.

- 루트 CA 인증서를 네트워크 보안 서비스(NSS) 데이터베이스로 가져옵니다.
- 플러그 가능 인증 모듈(PAM) 인증을 위한 `pam_pkcs11` 모듈을 설치합니다.
- WorkSpace 프로비저닝 `pkinit` 중에 활성화하는 것을 포함하는 기본 구성을 수행합니다.

다음 절차는 `enable_smartcard` 스크립트를 사용하여 Linux에 루트 CA 인증서를 WorkSpaces 추가하고 Linux용 스마트 카드를 활성화하는 방법을 설명합니다. WorkSpaces

1. WSP 프로토콜이 WorkSpace 활성화된 상태에서 새 Linux를 생성합니다. Amazon WorkSpace WorkSpaces 콘솔에서 실행할 때는 번들 선택 페이지에서 프로토콜로 WSP를 선택한 다음 Amazon Linux 2 퍼블릭 번들 중 하나를 선택해야 합니다.

2. 새 WorkSpace 버전에서는 다음 명령을 root로 실행합니다. 여기서 *pem-path* 는 PEM 형식의 루트 CA 인증서 파일 경로입니다.

```
/usr/lib/skylight/enable_smartcard --ca-cert pem-path
```

> **Note**
>
> Linux는 스마트 카드의 인증서가 사용자의 기본 UPN (사용자 계정 이름) 에 대해 발급된 것으로 WorkSpaces 가정합니다. 예를 들어*sAMAccountName*@*domain*, 여기서 *domain* 는 FQDN (정규화된 도메인 이름) 입니다.
> 대체 UPN 접미사를 사용하는 방법은 `run /usr/lib/skylight/enable_smartcard --help`에서 자세한 내용을 알아보세요. 대체 UPN 접미사의 매핑은 각 사용자마다 고유합니다. 따라서 매핑은 각 사용자에 대해 개별적으로 수행되어야 합니다. WorkSpace

3. (선택 사항) 기본적으로 모든 서비스는 Linux에서 스마트 카드 인증을 사용하도록 설정되어 WorkSpaces 있습니다. 스마트 카드 인증을 특정 서비스로만 제한하려면 `/etc/pam.d/system-auth`를 편집해야 합니다. 필요한 경우 `pam_succeed_if.so`의 `auth` 줄의 설명을 제거하고 서비스 목록을 편집하세요.

   `auth` 줄의 설명을 제거한 후 서비스가 스마트 카드 인증을 사용할 수 있도록 허용하려면 해당 줄을 목록에 추가해야 합니다. 서비스에서 암호 인증만 사용하도록 하려면 목록에서 제거해야 합니다.

4. 에 대한 추가 사용자 지정을 수행합니다. WorkSpace 예를 들어, 사용자가 Firefox에서 스마트 카드를 사용할 수 있도록 시스템 전체 정책을 추가할 수 있습니다. (Chrome 사용자는 클라이언트에서 직접 스마트 카드를 활성화해야 합니다. 자세한 내용은 Amazon WorkSpaces 사용 설명서의 스마트 카드 지원을 참조하십시오.)
5. 에서 사용자 지정 WorkSpace 이미지와 번들을 생성하십시오 WorkSpace.
6. 새 사용자 지정 번들을 사용하여 사용자를 WorkSpaces 위해 출시하세요.

사용자가 Firefox에서 스마트 카드를 사용할 수 있게 하는 방법

Linux WorkSpace 이미지에 SecurityDevices 정책을 추가하여 사용자가 Firefox에서 스마트 카드를 사용하도록 할 수 있습니다. Firefox에 시스템 전체 정책을 추가하는 방법에 대한 자세한 내용은 Mozilla 정책 템플릿을 참조하십시오. GitHub

1. WorkSpace 이미지를 만들 때 사용하는 파일에 WorkSpace in이라는 이름의 새 파일을 만드십시오. `policies.json /usr/lib64/firefox/distribution/`

2. JSON 파일에 다음 SecurityDevices 정책을 추가합니다. 여기에는 pkcs 모듈을 식별하는 데 사용할 *NAME_OF_DEVICE* 값이 들어 있습니다. 예를 들어, "OpenSC"와 같은 값을 사용할 수 있습니다.

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

문제 해결

문제 해결을 위해 pkcs11-tools 유틸리티를 추가하는 것이 좋습니다. 이 유틸리티를 사용하면 다음 작업을 수행할 수 있습니다.

- 각 스마트 카드를 나열합니다.
- 각 스마트 카드의 슬롯을 나열합니다.
- 각 스마트 카드의 인증서를 나열합니다.

문제를 일으킬 수 있는 일반적인 문제는 다음과 같습니다.

- 슬롯을 인증서에 잘못 매핑했습니다.
- 스마트 카드에 사용자와 매칭될 수 있는 인증서가 여러 개입니다. 인증서는 다음 기준을 사용하여 매칭됩니다.
  - 인증서의 루트 CA.
  - 인증서의 <KU> 및 <EKU> 필드.
  - 인증서 주체의 UPN.
- 키 사용에 <EKU>msScLogin이 있는 인증서가 여러 개입니다.

일반적으로 스마트 카드의 첫 번째 슬롯에 매핑되는 스마트 카드 인증용 인증서를 하나만 사용하는 것이 가장 좋습니다.

스마트 카드의 인증서 및 키를 관리(예: 인증서 및 키 제거 또는 재매핑)하는 도구는 제조업체마다 다를 수 있습니다. 스마트 카드 작업에 사용할 수 있는 추가 도구는 다음과 같습니다.

- opensc-explorer
- opensc-tool
- pkcs11_inspect
- pkcs11_listcerts
- pkcs15-tool

디버그 로깅을 활성화하는 방법

pam_pkcs11 및 pam-krb5 구성 문제를 해결하기 위해 디버그 로깅을 활성화할 수 있습니다.

1. /etc/pam.d/system-auth-ac 파일에서 auth 작업을 편집하고 pam_pksc11.so의 nodebug 파라미터를 debug로 변경합니다.
2. /etc/pam_pkcs11/pam_pkcs11.conf 파일에서 debug = false;를 debug = true;로 변경합니다. 이 debug 옵션은 각 매퍼 모듈에 개별적으로 적용되므로 pam_pkcs11 섹션 바로 아래 및 적절한 매퍼 섹션(기본값: mapper generic)에서 모두 직접 변경해야 할 수도 있습니다.
3. /etc/pam.d/system-auth-ac 파일에서 auth 작업을 편집하고 debug 또는 debug_sensitive 파라미터를 pam_krb5.so에 추가합니다.

디버그 로깅을 활성화한 후 시스템은 활성 터미널에서 직접 pam_pkcs11 디버그 메시지를 출력합니다. pam_krb5의 메시지가 /var/log/secure에 로깅됩니다.

스마트 카드 인증서가 매핑되는 사용자 이름을 확인하려면 다음 pklogin_finder 명령을 사용합니다.

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

메시지가 표시되면 스마트 카드 PIN을 입력합니다. pklogin_finder는 스마트 카드 인증서에 있는 사용자 이름을 *NETBIOS**username* 형식으로 stdout에 출력합니다. 이 사용자 이름은 사용자 이름과 일치해야 합니다. WorkSpace

Active Directory 도메인 서비스(AD DS)에서 NetBIOS 도메인 이름은 Windows 2000 이전 버전의 도메인 이름입니다. 항상 그런 것은 아니지만 일반적으로 NetBIOS 도메인 이름은 도메인 이름 시스템(DNS) 도메인 이름의 하위 도메인입니다. 예를 들어 DNS 도메인 이름이 example.com인 경우 NetBIOS 도메인은 대개 EXAMPLE입니다. DNS 도메인 이름이 corp.example.com인 경우 NetBIOS 도메인은 대개 CORP입니다.

예를 들어, corp.example.com 도메인에 있는 mmajor 사용자의 경우 pklogin_finder의 출력은 CORP\mmajor입니다.

> **Note**
>
> "ERROR:pam_pkcs11.c:504: verify_certificate() failed" 메시지를 수신하는 경우 이 메시지는 pam_pkcs11이 스마트 카드에서 사용자 이름 기준과 매칭되는 인증서를 찾았지만 시스템에서 인식되는 루트 CA 인증서에는 연결되지 않았음을 나타냅니다. 이 경우 pam_pkcs11은 위 메시지를 출력한 후 다음 인증서를 시도합니다. 사용자 이름과 매칭되는 인증서를 찾고 인증서가 인식된 루트 CA 인증서에 연결된 경우에만 인증을 허용합니다.

pam_krb5 구성 문제를 해결하려면 다음 명령을 사용하여 디버그 모드에서 수동으로 kinit를 호출할 수 있습니다.

```
KRB5_TRACE=/dev/stdout kinit -V
```

이 명령은 Kerberos 티켓 허가 티켓(TGT)을 성공적으로 받을 것입니다. 실패할 경우 명령에 올바른 Kerberos 보안 주체 이름을 명시적으로 추가해 보세요. 예를 들어, corp.example.com 도메인에 있는 mmajor 사용자의 경우 다음 명령을 사용하세요.

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

이 명령이 성공하면 사용자 이름을 Kerberos WorkSpace 사용자 이름으로 매핑할 때 문제가 발생할 가능성이 큽니다. /etc/krb5.conf 파일의 [appdefaults]/pam/mappings 섹션을 확인하세요.

이 명령은 성공하지 못했지만 암호 기반 kinit 명령은 성공하면 /etc/krb5.conf 파일에서 pkinit_ 관련 구성을 확인하세요. 예를 들어, 스마트 카드에 둘 이상의 인증서가 들어 있는 경우 pkinit_cert_match를 변경해야 할 수 있습니다.

귀하의 인터넷 액세스 제공 WorkSpace

운영 체제에 업데이트를 설치하고 애플리케이션을 배포하려면 인터넷에 액세스할 수 WorkSpaces 있어야 합니다. 다음 옵션 중 하나를 사용하여 가상 사설 클라우드 (VPC) WorkSpaces 에서 인터넷에 액세스하도록 허용할 수 있습니다.

옵션

- 프라이빗 WorkSpaces 서브넷에서 시작하고 VPC의 퍼블릭 서브넷에서 NAT 게이트웨이를 구성합니다.
- 퍼블릭 WorkSpaces 서브넷에서 시작하고 퍼블릭 IP 주소를 자동 또는 수동으로 할당합니다. WorkSpaces

이러한 옵션에 대한 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 에서 해당하는 섹션을 참조하세요.

이러한 옵션을 사용할 경우 해당 보안 그룹이 포트 80 (HTTP) 및 443 (HTTPS) 을 통해 모든 목적지 () 에 대한 아웃바운드 트래픽을 WorkSpaces 허용하는지 확인해야 합니다. `0.0.0.0/0`

Amazon Linux 엑스트라 라이브러리

Amazon Linux 리포지토리를 사용하는 경우 Amazon WorkSpaces Linux가 인터넷에 액세스할 수 있거나 이 리포지토리와 기본 Amazon Linux 리포지토리에 대한 VPC 엔드포인트를 구성해야 합니다. 자세한 내용은 Amazon S3용 엔드포인트의 예: Amazon Linux AMI 리포지토리 액세스 활성화를 참조하세요. Amazon Linux AMI 리포지토리는 각 리전의 Amazon S3 버킷입니다. VPC의 인스턴스가 엔드포인트를 통해 리포지토리에 액세스하도록 하려면 이러한 버킷에 액세스하게 하는 엔드포인트 정책을 만들 수 있습니다. 다음 정책은 사용자가 Amazon Linux 리포지토리에 읽기 전용 액세스를 할 수 있도록 허용합니다.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

귀사를 위한 보안 그룹 WorkSpaces

에 디렉터리를 등록하면 두 개의 보안 그룹이 생성됩니다. 하나는 디렉터리 컨트롤러용이고 다른 하나는 WorkSpaces 디렉터리에 대한 보안 그룹입니다. WorkSpaces 디렉터리 컨트롤러의 보안 그룹에는 디렉터리 식별자와 _controller로 구성되는 이름이 있습니다(예: d-12345678e1_controller). 의 보안 그룹 이름은 디렉토리 식별자 뒤에 WorkSpaces _WorkspacesMembers가 오는 것으로 구성됩니다 (예: D-123456FC11_WorkspacesMembers).

> **Warning**
>
> _컨트롤러 및 _WorkspacesMembers 보안 그룹을 수정, 삭제 또는 분리하지 마십시오. 이러한 보안 그룹을 수정하거나 삭제할 때는 주의해야 합니다. 수정하거나 삭제한 후에는 이러한 그룹을 다시 생성하여 다시 추가할 수 없기 때문입니다. 자세한 내용은 Linux 인스턴스에 대한 Amazon EC2 Amazon 보안 그룹과 Windows 인스턴스에 대한 Amazon EC2 Amazon 보안 그룹을 참조하세요.

디렉터리에 기본 보안 그룹을 추가할 수 있습니다. WorkSpaces 새 보안 그룹을 WorkSpaces 디렉터리에 연결하면 새로 WorkSpaces 시작하거나 WorkSpaces 재구축한 기존 보안 그룹에 새 보안 그룹이 생깁니다. 이 항목의 뒷부분에서 설명하는 것처럼 이 새 기본 보안 그룹을 WorkSpaces 재구축하지 않고 기존 보안 그룹에 추가할 수도 있습니다.

여러 보안 그룹을 WorkSpaces 디렉터리에 연결하면 각 보안 그룹의 규칙이 효과적으로 집계되어 하나의 규칙 집합이 생성됩니다. 보안 그룹 규칙은 가능한 한 응축하는 것이 좋습니다.

VPC 보안 그룹에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

디렉터리에 보안 그룹을 추가하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. [Security Group]을 확장하여 보안 그룹을 선택합니다.
5. [Update and Exit]를 선택합니다.

보안 그룹을 WorkSpace 재구축하지 않고 기존 보안 그룹에 추가하려면 의 Elastic Network Interface (ENI) 에 새 보안 그룹을 할당합니다. WorkSpace

기존 보안 그룹에 보안 그룹을 추가하려면 WorkSpace

1. 업데이트가 WorkSpace 필요한 각 IP 주소를 찾으십시오.
   a. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
   b. WorkSpace 각각을 펼치고 해당 WorkSpace IP 주소를 기록합니다.
2. 각각의 WorkSpace ENI를 찾아 보안 그룹 할당을 업데이트하십시오.
   a. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
   b. 네트워크 및 보안 아래에서 네트워크 인터페이스를 선택합니다.
   c. 1단계에서 기록한 첫 번째 IP 주소를 검색합니다.
   d. 이 IP 주소와 연결된 ENI를 선택하고 작업을 선택한 다음 보안 그룹 변경을 선택합니다.
   e. 새 보안 그룹을 선택하고 저장을 선택합니다.
   f. 다른 WorkSpaces 프로세스에도 필요에 따라 이 프로세스를 반복합니다.

WorkSpaces의 IP 액세스 제어 그룹

Amazon WorkSpaces를 사용하면 WorkSpaces에 액세스할 수 있는 IP 주소를 제어할 수 있습니다. IP 주소 기반 제어 그룹을 사용하면 신뢰할 수 있는 IP 주소 그룹을 정의 및 관리하고, 사용자가 신뢰할 수 있는 네트워크에 연결된 경우에만 WorkSpaces에 액세스하도록 허용할 수 있습니다.

IP 액세스 제어 그룹은 사용자가 WorkSpaces에 액세스할 수 있는 IP 주소를 제어하는 가상 방화벽의 역할을 합니다. CIDR 주소 범위를 지정하려면 IP 액세스 제어 그룹에 규칙을 추가한 다음 그룹을 디렉터리와 연결합니다. 각 IP 액세스 제어 그룹을 하나 이상의 디렉터리와 연결할 수 있습니다. AWS 계정마다 리전당 최대 100개의 IP 액세스 제어 그룹을 만들 수 있습니다. 하지만 한 개의 디렉터리에는 최대 25개의 IP 액세스 제어 그룹을 연결할 수 있습니다.

기본 IP 액세스 제어 그룹이 각 디렉터리와 연결되어 있습니다. 이 기본 그룹에는 사용자가 어디서나 WorkSpaces에 액세스할 수 있도록 허용하는 기본 규칙이 포함되어 있습니다. 디렉터리의 기본 IP 액세스 제어 그룹은 수정할 수 없습니다. IP 액세스 제어 그룹을 디렉터리에 연결하지 않으면 기본 그룹이 사용됩니다. IP 액세스 제어 그룹을 디렉터리와 연결하면 기본 IP 액세스 제어 그룹이 연결 해제됩니다.

신뢰할 수 있는 네트워크의 퍼블릭 IP 주소 및 IP 주소 범위를 지정하려면 IP 액세스 제어 그룹에 규칙을 추가합니다. 사용자가 NAT 게이트웨이 또는 VPN을 통해 WorkSpaces에 액세스하는 경우 NAT 게이트웨이 또는 VPN에 대한 퍼블릭 IP 주소에서 트래픽을 허용하는 규칙을 생성해야 합니다.

> **Note**
>
> - IP 액세스 제어 그룹은 NAT에 동적 IP 주소를 사용할 수 없습니다. NAT를 사용하는 경우 동적 IP 주소 대신 고정 IP 주소를 사용하도록 구성합니다. NAT가 WorkSpaces 세션 동안 동일한 고정 IP 주소를 통해 모든 UDP 트래픽을 라우팅해야 합니다.
> - IP 액세스 제어 그룹은 사용자가 스트리밍 세션을 WorkSpaces에 연결할 수 있는 IP 주소를 제어합니다. 사용자는 Amazon WorkSpaces 퍼블릭 API를 사용하여 어떤 IP 주소에서든 재시작, 재구축, 종료와 같은 기능을 계속 실행할 수 있습니다.

Web Access, PCoIP 제제로 클라이언트와 macOS, iPad, Windows, Chromebook 및 Android용 클라이언트 애플리케이션을 통해 이 기능을 사용할 수 있습니다.

IP 액세스 제어 그룹 생성

다음과 같이 IP 액세스 제어 그룹을 생성할 수 있습니다. 각 IP 액세스 제어 그룹에는 최대 10개의 규칙이 포함될 수 있습니다.

IP 액세스 제어 그룹을 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 IP 액세스 제어를 선택합니다.
3. IP 그룹 생성을 선택합니다.
4. IP 그룹 생성 대화 상자에서 그룹의 이름과 설명을 입력하고 생성을 선택합니다.
5. 그룹을 선택하고 편집을 선택합니다.
6. 각 IP 주소에 대해 규칙 추가를 선택합니다. 소스에 IP 주소 또는 IP 주소 범위를 입력합니다. 설명에 설명을 입력합니다. 규칙 추가를 완료하면 저장을 선택합니다.

IP 액세스 제어 그룹을 디렉터리와 연결

IP 액세스 제어 그룹을 디렉터리와 연결하여 신뢰할 수 있는 네트워크에서만 WorkSpaces에 액세스하도록 보장할 수 있습니다.

규칙이 없는 IP 액세스 제어 그룹을 디렉터리와 연결하면 모든 WorkSpaces에 대한 모든 액세스가 차단됩니다.

IP 액세스 제어 그룹을 디렉터리와 연결하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. IP 액세스 제어 그룹을 확장하고 하나 이상의 IP 액세스 제어 그룹을 선택합니다.
5. [Update and Exit]를 선택합니다.

IP 액세스 제어 그룹 복사

기존 IP 액세스 제어 그룹을 기반을 사용하여 새로운 IP 액세스 제어 그룹을 생성할 수 있습니다.

기존 IP 액세스 제어 그룹에서 IP 액세스 제어 그룹을 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 IP 액세스 제어를 선택합니다.
3. 그룹을 선택하고 작업, 새로 복사를 선택합니다.
4. IP 그룹 복사 대화 상자에서 새 그룹의 이름과 설명을 입력하고 그룹 복사를 선택합니다.
5. (선택 사항) 원본 그룹에서 복사된 규칙을 수정하려면 새 그룹을 선택하고 편집을 선택합니다. 필요에 따라 규칙을 추가, 업데이트 또는 제거합니다. Save를 선택합니다.

IP 액세스 제어 그룹 삭제

언제든지 IP 액세스 제어 그룹에서 규칙을 삭제할 수 있습니다. WorkSpace에 연결을 허용하는 데 사용된 규칙을 제거하면 사용자가 WorkSpace에서 연결 해제됩니다.

IP 액세스 제어 그룹을 삭제하려면 먼저 IP 액세스 제어 그룹을 디렉터리에서 연결 해제해야 합니다.

IP 액세스 제어 그룹을 삭제하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. IP 액세스 제어 그룹과 연결된 각 디렉터리에 대해 디렉터리를 선택하고 작업, 세부 정보 업데이트를 선택합니다. IP 액세스 제어 그룹을 확장하고, IP 액세스 제어 그룹의 확인란을 선택 취소한 다음, 업데이트 및 종료를 선택합니다.

4. 탐색 창에서 IP 액세스 제어를 선택합니다.
5. 그룹을 선택하고 작업, IP 그룹 삭제를 선택합니다.

WorkSpaces용 PCoIP 제로 클라이언트 설정

PCoIP 제로 클라이언트는 PCoIP 프로토콜을 사용하는 WorkSpaces 번들과만 호환됩니다.

제로 클라이언트 디바이스에 펌웨어 버전 6.0.0 이상이 설치되어 있으면 사용자는 해당 WorkSpaces에 직접 연결할 수 있습니다. 사용자가 제로 클라이언트 디바이스를 사용하여 WorkSpaces에 직접 연결하는 경우 WorkSpaces 디렉터리에 다중 인증(MFA)을 사용하는 것이 좋습니다. 디렉터리에서 MFA를 사용하는 방법에 대한 자세한 내용은 다음 문서를 참조하세요.

- AWS Managed Microsoft AD - AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD에 다중 인증 사용
- AD 커넥터 - AWS Directory Service 관리 안내서의 AD Connector에 대한 다중 인증 활성화 및 다중 인증(AD Connector)
- 신뢰할 수 있는 도메인 - AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD에 다중 인증 사용
- Simple AD - Simple AD에는 다중 인증을 사용할 수 없습니다.

2021년 4월 13일부터 PCoIP 연결 관리자는 4.6.0에서 6.0.0 사이의 제로 클라이언트 디바이스 펌웨어 버전과 함께 사용할 수 없습니다. 제로 클라이언트 펌웨어가 버전 6.0.0 이상이 아닌 경우 https://www.teradici.com/desktop-access에서 데스크톱 액세스 구독을 통해 최신 펌웨어를 받을 수 있습니다.

> **Important**
>
> - Teradici PCoIP 관리 웹 인터페이스(AWI) 또는 Teradici PCoIP 관리 콘솔(MC)에서 NTP(Network Time Protocol)를 활성화해야 합니다. NTP 호스트 DNS 이름으로 **`pool.ntp.org`**를 사용하고, NTP 호스트 포트를 123으로 설정합니다. NTP가 활성화되지 않으면 PCoIP 제로 클라이언트 사용자에게 “The supplied certificate is invalid due to timestamp.(제공된 인증서가 타임스탬프로 인해 유효하지 않습니다.)“와 같은 인증서 실패 오류가 표시될 수 있습니다.
> - PCoIP 에이전트 버전 20.10.4부터 Amazon WorkSpaces는 Windows 레지스트리를 통해 USB 리디렉션을 기본적으로 비활성화합니다. 이 레지스트리 설정은 사용자가 PCoIP 제로 클라이언트 디바이스를 사용하여 WorkSpaces에 연결할 때 USB 주변 디바이스의 동작에 영

향을 줍니다. 자세한 내용은 USB 프린터 및 기타 USB 주변 디바이스가 PCoIP 제로 클라이언트에서 작동하지 않는 경우 섹션을 참조하세요.

PCoIP 제로 클라이언트 디바이스를 설정하고 연결하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 PCoIP 제로 클라이언트를 참조하세요. 승인된 PCoIP 제로 클라이언트 디바이스 목록은 Teradici 웹 사이트의 PCoIP Zero Clients를 참조하세요.

Chromebook을 위한 Android 설정

버전 2.4.13은 Amazon WorkSpaces 크롬북 클라이언트 애플리케이션의 최종 릴리스입니다. Google이 Chrome 앱에 대한 지원을 단계적으로 중단하고 있기 때문에 WorkSpaces Chromebook 클라이언트 애플리케이션에 대한 추가 업데이트는 없을 것이며 사용도 지원되지 않습니다.

Android 애플리케이션 설치를 지원하는 Chromebook의 경우 Android 클라이언트 애플리케이션을 대신 사용하는 것이 좋습니다. WorkSpaces

2019년 이전에 출시된 일부 크롬북은 Android 앱을 설치할 수 있도록 설정해야 사용자가 Amazon WorkSpaces Android 클라이언트 애플리케이션을 설치할 수 있습니다. 자세한 내용은 Android 앱을 지원하는 Chrome OS 시스템을 참조하십시오.

사용자의 Chromebook이 Android 앱을 설치할 수 있도록 원격으로 관리하려면 Chrome 디바이스에서 Android 설정을 참조하십시오.

Amazon WorkSpaces 웹 액세스 활성화 및 구성

대부분의 WorkSpaces 번들은 Amazon WorkSpaces 웹 액세스를 지원합니다. 웹 브라우저 액세스를 WorkSpaces 지원하는 목록은 “웹 액세스를 지원하는 Amazon WorkSpaces 번들은 무엇입니까?”를 참조하십시오. 클라이언트 액세스, Web Access 및 사용자 환경에서 'Web Access를 지원하는 Amazon WorkSpaces 번들은 무엇인가요?'를 참조하세요.

> **Note**
>
> - Windows 및 Ubuntu용 WSP를 사용한 웹 WorkSpaces 액세스는 WSP를 사용할 수 있는 모든 지역에서 지원됩니다. WorkSpaces Amazon WorkSpaces Linux용 WSP는 AWS GovCloud (미국 서부) 에서만 사용할 수 있습니다.

- 최상의 스트리밍 품질과 사용자 경험을 WorkSpaces 위해 WSP와 함께 웹 액세스를 사용하는 것이 좋습니다. 다음은 WorkSpaces PCoIP와 함께 웹 액세스를 사용할 때의 제한 사항입니다.
  - PCoIP를 통한 웹 액세스는 아시아 태평양 (뭄바이) AWS GovCloud (US) Regions, 아프리카 (케이프타운) 및 이스라엘 (텔아비브) 에서 지원되지 않습니다.
  - PCoIP를 사용한 웹 액세스는 Windows에서만 지원되며 Amazon WorkSpaces Linux에서는 지원되지 않습니다. WorkSpaces
  - PCoIP 프로토콜을 사용하는 일부 Windows WorkSpaces 10에서는 웹 액세스를 사용할 수 없습니다. WorkSpaces PCoIP가 윈도우 서버 2019 또는 2022에서 구동되는 경우 웹 액세스를 사용할 수 없습니다.
- 웹 브라우저를 사용하여 GPU 지원 서비스에 연결할 수 없습니다. WorkSpaces
- VPN에서 macOS를 사용하고 Firefox 웹 브라우저를 사용하는 경우, 웹 브라우저는 웹 액세스를 사용한 WorkSpaces PCoIP 스트리밍을 지원하지 않습니다. WorkSpaces 이는 WebRTC 프로토콜의 Firefox 구현에 제한이 있기 때문입니다.

Important

2020년 10월 1일부터 고객은 더 이상 Amazon WorkSpaces Web Access 클라이언트를 사용하여 Windows 7 커스텀 WorkSpaces 또는 Windows 7 사용자 지정 라이선스 사용 (BYOL) 에 연결할 수 없습니다. WorkSpaces

1단계: 사용자 컴퓨터에 대한 웹 액세스 활성화 WorkSpaces

디렉터리 수준에서 사용자에 대한 웹 액세스를 제어할 WorkSpaces 수 있습니다. 웹 액세스 클라이언트를 통해 사용자가 액세스할 수 있도록 허용하려는 각 디렉터리에 대해 다음 단계를 수행하십시오. WorkSpaces

웹 액세스를 활성화하려면 다음과 같이 하십시오. WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리 ID 열에서 Web Access를 활성화하려는 디렉터리의 디렉터리 ID를 선택합니다.
4. 디렉터리 세부 정보 페이지에서 기타 플랫폼 섹션으로 스크롤하여 편집을 선택합니다.

5. 웹 액세스를 선택합니다.
6. 저장을 선택합니다.

> **Note**
> 웹 액세스를 활성화한 후 재부팅하여 변경 사항을 적용하십시오 WorkSpace .

2단계: Web Access를 위해 포트에 대한 인바운드 및 아웃바운드 액세스 구성

Amazon WorkSpaces Web Access에는 특정 포트에 대한 인바운드 및 아웃바운드 액세스가 필요합니다. 자세한 정보는 웹 액세스를 위한 포트을 참조하세요.

3단계: 사용자가 로그온할 수 있도록 그룹 정책 및 보안 정책 설정 구성

WorkSpaces Amazon은 사용자가 웹 액세스 클라이언트에서 성공적으로 로그온할 수 있도록 특정 로그온 화면 구성을 사용합니다.

웹 액세스 사용자가 자신의 WorkSpaces 웹 액세스 사용자에 로그온할 수 있도록 하려면 그룹 정책 설정과 세 가지 보안 정책 설정을 구성해야 합니다. 이러한 설정을 올바르게 구성하지 않으면 사용자가 자신의 WorkSpaces 계정에 로그온하려고 할 때 로그온 시간이 길어지거나 화면이 검은색으로 표시될 수 있습니다. 이러한 설정을 구성하려면 다음 절차를 사용하십시오.

GPO (그룹 정책 개체) 를 사용하여 Windows WorkSpaces 또는 Windows 디렉터리에 속한 사용자를 관리하기 위한 설정을 적용할 수 있습니다. WorkSpaces WorkSpaces 컴퓨터 개체에 대한 조직 단위와 WorkSpaces 사용자 개체에 대한 조직 구성 단위를 만드는 것이 좋습니다.

Active Directory 관리 도구를 사용하여 GPO를 처리하는 방법에 대한 내용은 AWS Directory Service 관리 안내서의 Active Directory 관리 도구 설치를 참조하세요.

WorkSpaces 로그온 에이전트가 사용자를 전환할 수 있도록 하려면

대부분의 경우 사용자가 로그온을 시도하면 사용자 이름 필드에 해당 사용자의 이름이 미리 채워집니다. WorkSpace 그러나 관리자가 유지 관리 작업을 수행하기 WorkSpace 위해 에 RDP 연결을 설정한 경우에는 사용자 이름 필드에 관리자 이름이 대신 채워집니다.

이 문제를 해결하려면 Hide entry points for Fast User Switching(빠른 사용자 전환을 위해 입력 요소 숨기기) 그룹 정책 설정을 비활성화하십시오. 이 설정을 사용하지 않도록 설정하면 WorkSpaces 로그온 에이전트가 사용자 전환 버튼을 사용하여 사용자 이름 필드를 올바른 이름으로 채울 수 있습니다.

1. 그룹 정책 관리 도구 (gpmc.msc) 를 열고 사용 중인 디렉터리의 도메인 또는 도메인 컨트롤러 수준에서 GPO를 찾아 선택합니다. WorkSpaces (도메인에 WorkSpaces 그룹 정책 관리 템플릿이 설치되어 있는 경우 WorkSpaces 컴퓨터 계정에 WorkSpaces GPO를 사용할 수 있습니다.)
2. 주 메뉴에서 [Action], [Edit]를 선택합니다.
3. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, 시스템 및 로그인을 선택합니다.
4. Hide entry points for Fast User Switching(빠른 사용자 전환을 위해 입력 요소 숨기기) 설정을 엽니다.
5. Hide entry points for Fast User Switching(빠른 사용자 전환을 위해 입력 요소 숨기기) 대화 상자에서 비활성을 선택하고 확인을 선택합니다.

마지막으로 로그인한 사용자 이름을 숨기려면

기본적으로 사용자 전환 버튼 대신 마지막으로 로그인한 사용자 목록이 표시됩니다. 의 WorkSpace 구성에 따라 목록에 기타 사용자 타일이 표시되지 않을 수도 있습니다. 이 경우 미리 채워진 사용자 이름이 올바르지 않으면 WorkSpaces 로그온 에이전트가 필드를 올바른 이름으로 채울 수 없습니다.

이 문제를 방지하려면 사용 중인 Windows 버전에 따라 보안 정책 설정인 Interactive logon: Don't display last signed-in(대화형 로그인: 마지막으로 로그인한 사용자를 표시하지 않음) 또는 Interactive logon: Do not display last user name(대화형 로그인: 마지막 사용자 이름을 표시하지 않음) 설정을 비활성화합니다.

1. 그룹 정책 관리 도구 (gpmc.msc) 를 열고 사용 중인 디렉터리의 도메인 또는 도메인 컨트롤러 수준에서 GPO를 찾아 선택합니다. WorkSpaces (도메인에 WorkSpaces 그룹 정책 관리 템플릿이 설치되어 있는 경우 WorkSpaces 컴퓨터 계정에 WorkSpaces GPO를 사용할 수 있습니다.)
2. 주 메뉴에서 [Action], [Edit]를 선택합니다.
3. 그룹 정책 관리 편집기에서 컴퓨터 구성, Windows 설정, 보안 설정, 로컬 정책 및 보안 옵션을 선택합니다.
4. 다음 설정 중 하나를 엽니다.
   - Windows 7 - Interactive logon: Don't display last signed-in
   - Windows 10 - Interactive logon: Do not display last user name
5. 설정의 속성 대화 상자에서 활성을 선택하고 확인을 선택합니다.

사용자가 Ctrl+ALT+DEL을 누른 후에 로그인하도록 하려면

WorkSpaces 웹 액세스의 경우 사용자가 로그온하려면 먼저 Ctrl+Alt+DEL을 눌러야 합니다. 사용자가 Ctrl+ALT+DEL을 누른 후에 로그인하도록 하면 사용자가 암호를 입력할 때 신뢰할 수 있는 경로를 사용하게 됩니다.

1. 그룹 정책 관리 도구 (gpmc.msc) 를 열고 사용 중인 디렉터리의 도메인 또는 도메인 컨트롤러 수준에서 GPO를 찾아 선택합니다. WorkSpaces (도메인에 WorkSpaces 그룹 정책 관리 템플릿이 설치되어 있는 경우 WorkSpaces 컴퓨터 계정에 WorkSpaces GPO를 사용할 수 있습니다.)
2. 주 메뉴에서 [Action], [Edit]를 선택합니다.
3. 그룹 정책 관리 편집기에서 컴퓨터 구성, Windows 설정, 보안 설정, 로컬 정책 및 보안 옵션을 선택합니다.
4. Interactive logon: Do not require CTRL+ALT+DEL(대화형 로그인: Ctrl+ALT+DEL이 필요하지 않음) 설정을 엽니다.
5. 로컬 보안 설정 탭에서 비활성을 선택하고 확인을 선택합니다.

세션이 잠겨 있을 때 도메인 및 사용자 정보를 표시하려면

WorkSpaces 로그온 에이전트는 사용자 이름과 도메인을 찾습니다. 이 설정이 구성되면 잠금 화면에 사용자의 전체 이름(Active Directory에 지정된 경우), 도메인 이름 및 사용자 이름이 표시됩니다.

1. 그룹 정책 관리 도구 (gpmc.msc) 를 열고 사용 중인 디렉터리의 도메인 또는 도메인 컨트롤러 수준에서 GPO를 찾아 선택합니다. WorkSpaces (도메인에 WorkSpaces 그룹 정책 관리 템플릿이 설치되어 있는 경우 WorkSpaces 컴퓨터 계정에 WorkSpaces GPO를 사용할 수 있습니다.)
2. 주 메뉴에서 [Action], [Edit]를 선택합니다.
3. 그룹 정책 관리 편집기에서 컴퓨터 구성, Windows 설정, 보안 설정, 로컬 정책 및 보안 옵션을 선택합니다.
4. Interactive logon: Display user information when the session is locked(대화식 로그인: 세션이 잠겨 있을 때 사용자 정보를 표시함) 설정을 엽니다.
5. 로컬 보안 설정 탭에서 사용자 표시 이름, 도메인 이름 및 사용자 이름을 선택하고 확인을 선택합니다.

그룹 정책 및 보안 정책 설정 변경을 적용하려면

그룹 정책 및 보안 정책 설정 변경 내용은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션을 다시 시작한 후에 적용됩니다. 이전 절차에서 그룹 정책 및 보안 정책 변경을 적용하려면 다음 중 하나를 수행하십시오.

- 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
- 관리 명령 프롬프트에서 gpupdate /force를 입력합니다.

FedRAMP 승인 또는 DoD SRG 준수를 위해 Amazon WorkSpaces 설정

연방정부의 위험 및 인증 관리 프로그램(FedRAMP) 또는 미국 국방부(DoD) 클라우드 컴퓨팅 보안 요구 사항 가이드(SRG)를 준수하려면 Amazon WorkSpaces를 구성하여 디렉터리 수준에서 Federal Information Processing Standards(FIPS) 엔드포인트 암호화를 사용해야 합니다. 또한 FedRAMP에서 승인했거나 DoD SRG를 준수하는 US AWS 리전을 사용해야 합니다.

FedRAMP 승인 수준(보통 또는 높음) 또는 DoD SRG 영향 수준(2, 4 또는 5)은 Amazon WorkSpaces가 사용되는 US AWS 리전에 따라 다릅니다. 각 리전에 적용되는 FedRAMP 승인 및 DoD SRG 준수 수준은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요.

> **Note**
>
> FIPS 엔드포인트 암호화를 사용하는 것 외에도 WorkSpaces도 암호화할 수 있습니다. 자세한 내용은 암호화된 WorkSpaces 섹션을 참조하세요.

요구 사항

- FedRAMP에서 승인했거나 DoD SRG를 준수하는 US AWS 리전에서 WorkSpace를 생성해야 합니다.
- WorkSpaces 디렉터리는 엔드포인트 암호화를 위해 FIPS 140-2 검증 모드를 사용하도록 구성해야 합니다.

> **Note**
>
> FIPS 140-2 검증 모드 설정을 사용하려면 WorkSpaces 디렉터리가 새 디렉터리이거나 디렉터리의 모든 기존 WorkSpace가 엔드포인트 암호화를 위해 FIPS 140-2 검증 모드를 사용해

야 합니다. 그렇지 않으면 이 설정을 사용할 수 없으므로 생성한 WorkSpace가 FedRAMP 또는 DoD 보안 요구 사항을 준수하지 않습니다.

- 사용자는 다음 WorkSpace 클라이언트 애플리케이션 중 하나에서 WorkSpace에 액세스해야 합니다.
  - Windows: 2.4.3 이상
  - macOS: 2.4.3 이상
  - 리눅스: 3.0.0 이상
  - iOS: 2.4.1 이상
  - Android: 2.4.1 이상
  - Fire Tablet: 2.4.1 이상
  - ChromeOS: 2.4.1 이상
  - 웹 액세스

FIPS 엔드포인트 암호화를 사용하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. FedRAMP에서 승인하고 DoD SRG를 준수하는 WorkSpace를 생성할 디렉터리에 연결된 기존 WorkSpace가 없는지 확인합니다. 디렉터리와 연결된 WorkSpace가 있고 디렉터리가 FIPS 140-2 검증 모드를 사용하도록 활성화되지 않은 경우, WorkSpace를 종료하거나 새 디렉터리를 생성합니다.
4. 위의 기준을 충족하는 디렉터리를 생성한 다음 [Actions], [Update Details]를 선택합니다.
5. 디렉터리 세부 정보 업데이트 페이지에서 화살표를 선택하여 [Access Control Options] 섹션을 확장합니다.
6. 엔드포인트 암호화에서 TLS 암호화 모드(표준) 대신 FIPS 140-2 검증 모드를 선택합니다.
7. [Update and Exit]를 선택합니다.
8. 이제 이 디렉터리에서 FedRAMP에서 승인하고 DoD SRG를 준수하는 WorkSpace를 생성할 수 있습니다. 이 WorkSpace에 액세스하려면 [Requirements] 섹션에 나열된 WorkSpace 클라이언트 애플리케이션 중 하나를 사용해야 합니다.

리눅스용 SSH 연결 활성화 WorkSpaces

사용자 또는 사용자가 명령줄을 사용하여 Amazon WorkSpaces Linux에 연결하려는 경우 SSH 연결을 활성화할 수 있습니다. 디렉터리 WorkSpaces 내 모든 사용자 또는 디렉터리 내 WorkSpaces 개인에 대한 SSH 연결을 활성화할 수 있습니다.

SSH 연결을 활성화하려면 새 보안 그룹을 생성하거나 기존 보안 그룹을 업데이트하고 규칙을 추가하여 이 용도로 인바운드 트래픽을 허용합니다. 보안 그룹은 연결된 인스턴스에 대한 방화벽 역할을 하여 인스턴스 수준에서 인바운드 트래픽과 아웃바운드 트래픽을 모두 제어합니다. 보안 그룹을 생성하거나 업데이트하면 사용자 및 다른 사용자가 PuTTY 또는 기타 터미널을 사용하여 디바이스에서 Amazon Linux로 연결할 수 있습니다. WorkSpaces 자세한 설명은 the section called “보안 그룹” 섹션을 참조하세요.

비디오 자습서를 보려면 SSH를 WorkSpaces 사용하여 Linux Amazon에 연결하려면 어떻게 해야 합니까? 를 참조하십시오. AWS 지식 센터에서

내용

Amazon Linux에 대한 SSH 연결을 위한 사전 요구 사항 WorkSpaces

- a로의 인바운드 SSH 트래픽 활성화 WorkSpace - 하나 이상의 Amazon WorkSpaces Linux에 대한 인바운드 SSH 트래픽을 허용하는 규칙을 추가하려면 SSH 연결이 필요한 디바이스의 퍼블릭 또는 프라이빗 IP 주소가 있는지 확인하십시오. WorkSpaces 예를 들어, 가상 사설 클라우드 (VPC) 외부에 있는 디바이스의 퍼블릭 IP 주소 또는 동일한 VPC에 있는 다른 EC2 인스턴스의 프라이빗 IP 주소를 지정할 수 있습니다. WorkSpace

  로컬 WorkSpace 디바이스에서 연결하려는 경우 인터넷 브라우저에서 “내 IP 주소는 무엇입니까?”라는 검색어를 사용하거나 다음 서비스를 사용할 수 있습니다. Check IP.
- 연결 WorkSpace — 디바이스에서 Amazon Linux로 SSH 연결을 시작하려면 다음 정보가 필요합니다. WorkSpace
  - 연결한 Active Directory 도메인의 NetBIOS 이름입니다.

- WorkSpace 사용자 이름.
- WorkSpace 연결하려는 사용자의 공용 또는 사설 IP 주소.

  비공개: VPC가 기업 네트워크에 연결되어 있고 해당 네트워크에 액세스할 수 있는 경우 의 사설 IP 주소를 지정할 수 있습니다. WorkSpace

  퍼블릭: 퍼블릭 IP 주소가 있는 경우 다음 절차에 설명된 대로 WorkSpaces 콘솔을 사용하여 퍼블릭 IP 주소를 찾을 수 있습니다. WorkSpace

WorkSpace 연결하려는 Amazon Linux의 IP 주소와 사용자 이름을 찾으려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 목록에서 SSH 연결을 WorkSpace 활성화하려는 항목을 선택합니다. WorkSpaces
4. 실행 모드 열에서 WorkSpace 상태가 사용 가능으로 표시되는지 확인합니다.
5. WorkSpace 이름 왼쪽에 있는 화살표를 클릭하여 인라인 요약을 표시하고 다음 정보를 기록해 둡니다.

   - WorkSpace IP. 의 사설 IP WorkSpace 주소입니다.

     사설 IP 주소는 와 관련된 Elastic Network 인터페이스를 가져오는 데 필요합니다 WorkSpace. 보안 그룹 또는 관련 공용 IP 주소와 같은 정보를 검색하려면 네트워크 인터페이스가 필요합니다 WorkSpace.
   - WorkSpace 사용자 이름. 연결하기 위해 지정하는 사용자 이름입니다 WorkSpace.
6. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
7. 탐색 창에서 네트워크 인터페이스(Network Interfaces)를 선택합니다.
8. 검색 상자에 5단계에서 기록해 둔 WorkSpace IP를 입력합니다.
9. WorkSpaceIP와 연결된 네트워크 인터페이스를 선택합니다.
10. 퍼블릭 IP WorkSpace 주소가 있는 경우 IPv4 퍼블릭 IP 열에 해당 주소가 표시됩니다. 해당되는 경우 이 주소를 기록해 둡니다.

연결한 Active Directory 도메인의 NetBIOS 이름을 확인하려면

1. https://console.aws.amazon.com/directoryservicev2/ 에서 AWS Directory Service 콘솔을 엽니다.
2. 디렉터리 목록에서 해당 디렉터리의 디렉터리 ID 링크를 클릭합니다. WorkSpace

3. Directory details(디렉터리 세부 정보) 섹션에서 Directory NetBIOS name(디렉터리 NetBIOS 이름)을 기록해 둡니다.

디렉터리의 모든 Amazon WorkSpaces Linux에 대한 SSH 연결 활성화

디렉터리의 모든 Amazon WorkSpaces Linux에 대한 SSH 연결을 활성화하려면 다음과 같이 하십시오.

WorkSpaces 디렉터리의 모든 Amazon Linux에 대한 인바운드 SSH 트래픽을 허용하는 규칙이 포함된 보안 그룹을 생성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 [Security Groups]를 선택합니다.
3. 보안 그룹 생성을 선택합니다.
4. 보안 그룹의 이름을 입력하고 선택적으로 설명을 입력합니다.
5. VPC의 경우 SSH 연결을 활성화하려는 VPC가 들어 WorkSpaces 있는 VPC를 선택합니다.
6. Inbound(인바운드) 탭에서 Add Rule(규칙 추가)을 선택하고 다음을 수행합니다.
   - Type(유형)에서 SSH를 선택합니다.
   - 프로토콜의 경우 SSH를 선택하면 TCP가 자동으로 지정됩니다.
   - 포트 범위의 경우 SSH를 선택하면 22가 자동으로 지정됩니다.
   - 소스의 경우 사용자가 연결하는 데 사용할 컴퓨터의 퍼블릭 IP 주소의 CIDR 범위를 지정합니다. WorkSpaces 회사 네트워크 또는 홈 네트워크를 예로 들 수 있습니다.
   - Description(설명)(선택 사항)에 규칙에 대한 설명을 입력합니다.
7. 생성을 선택하세요.

아마존 리눅스 2에서의 암호 기반 인증 WorkSpaces

2023년 11월 10일 이전에 WorkSpaces 출시된 Amazon Linux 2는 기본적으로 SSH 암호 인증이 활성화되어 있습니다. 아마존 리눅스 2의 경우 11월 10일 이후에 WorkSpaces 출시되었습니다. SSH 암호 인증이 기본적으로 비활성화되어 있습니다.

기존 Amazon Linux 2 WorkSpaces 인스턴스에서 암호 인증을 비활성화하려면

1. WorkSpaces 클라이언트를 시작하고 사용자 클라이언트에 WorkSpace 로그인합니다.
2. 터미널 창을 엽니다(애플리케이션 > 시스템 도구 > MATE 터미널).

3. 터미널 창에서 다음 명령을 실행합니다.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

새로 생성한 Amazon Linux 2 WorkSpaces 인스턴스에서 암호 인증을 활성화하려면

1. WorkSpaces 클라이언트를 시작하고 사용자 클라이언트에 WorkSpace 로그인합니다.
2. 터미널 창을 엽니다(애플리케이션 > 시스템 도구 > MATE 터미널).
3. 터미널 창에서 다음 명령을 실행합니다.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

Ubuntu와 달리 WorkSpaces Amazon Linux 2는 WorkSpaces 기본적으로 사용자 지정 이미지의 SSH 암호 인증 설정을 보존하지 않습니다. 사용자 지정 이미지에서 WorkSpaces 프로비저닝된 Amazon Linux 2에서 기본적으로 SSH 암호 인증을 활성화하려면 암호 인증을 활성화하는 것 외에도 사용자 지정 이미지를 생성할 `ssh_pwauth` 때 포함하는 줄을 제거하도록 `/etc/cloud/cloud.cfg` 파일을 변경해야 합니다. `/etc/cloud/cloud.cfg` 파일을 변경하려면 다음 명령을 실행합니다.

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

특정 아마존 리눅스로의 SSH 연결 활성화 WorkSpace

특정 Amazon Linux에 대한 SSH 연결을 WorkSpace 활성화하려면 다음과 같이 하십시오.

기존 보안 그룹에 규칙을 추가하여 특정 Amazon Linux로의 인바운드 SSH 트래픽을 허용하는 방법 WorkSpace

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 Network & Security(네트워크 및 보안) 아래에서 Network Interfaces(네트워크 인터페이스)를 선택합니다.
3. 검색 창에 SSH 연결을 WorkSpace 활성화하려는 사설 IP 주소를 입력합니다.
4. Security groups(보안 그룹) 열에서 보안 그룹에 대한 링크를 클릭합니다.
5. 인바운드 탭에서 편집을 선택합니다.
6. Add Rule(규칙 추가)를 선택하고 다음을 수행합니다.

   - Type(유형)에서 SSH를 선택합니다.

- 프로토콜의 경우 SSH를 선택하면 TCP가 자동으로 지정됩니다.
- 포트 범위의 경우 SSH를 선택하면 22가 자동으로 지정됩니다.
- Source(소스)에서 My IP(내 IP) 또는 Custom(사용자 지정)을 선택하고 CIDR 표기법으로 단일 IP 주소 또는 IP 주소 범위를 지정합니다. 예를 들어, IPv4 주소가 `203.0.113.25`인 경우 이 단일 IPv4 주소를 CIDR 표기법으로 나열하려면 `203.0.113.25/32`를 지정합니다. 회사에서 주소를 범위로 할당하는 경우 전체 범위(예: `203.0.113.0/24`)를 지정합니다.
- Description(설명)(선택 사항)에 규칙에 대한 설명을 입력합니다.

7. 저장을 선택합니다.

리눅스 또는 WorkSpace PuTTY를 사용하여 아마존 리눅스에 연결

보안 그룹을 만들거나 업데이트하고 필요한 규칙을 추가하면 사용자 및 다른 사용자가 Linux 또는 PuTTY를 사용하여 장치에서 사용자 장치로 연결할 수 있습니다. WorkSpaces

> **Note**
>
> 다음 절차 중 하나를 완료하기 전에 먼저 다음이 있는지 확인합니다.
>
> - 연결한 Active Directory 도메인의 NetBIOS 이름입니다.
> - 연결할 때 사용하는 사용자 이름. WorkSpace
> - WorkSpace 연결하려는 사용자의 공용 또는 사설 IP 주소.
>
> 이 정보를 얻는 방법에 대한 지침은 이 주제 앞부분의 “Amazon WorkSpaces Linux에 대한 SSH 연결 사전 요구 사항”을 참조하십시오.

Linux를 WorkSpace 사용하여 Amazon Linux에 연결하려면

1. 관리자로 명령 프롬프트를 열고 다음 명령을 입력합니다. *NetBIOS ##*, *### ##* 및 *WorkSpace IP#* 해당하는 값을 입력합니다.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   다음은 SSH 명령의 예입니다. 여기서

   - *NetBIOS_NAME*은 anycompany입니다.

- *Username(### ##)*은 janedoe입니다.
- *WorkSpace IP# 203.0.113.25###*.

```
ssh "anycompany\janedoe"@203.0.113.25
```

2. 메시지가 표시되면 WorkSpaces 클라이언트에서 인증할 때 사용하는 것과 동일한 암호 (Active Directory 암호) 를 입력합니다.

PuTTY를 WorkSpace 사용하여 아마존 리눅스에 연결하려면

1. PuTTY를 엽니다.
2. PuTTY Configuration(PuTTY 구성) 대화 상자에서 다음을 수행합니다.
   - Host Name (or IP address)(호스트 이름(또는 IP 주소))으로 다음 명령을 입력합니다. 연결된 Active Directory 도메인의 NetBIOS 이름, 연결할 때 사용하는 사용자 이름 및 연결하려는 IP 주소로 값을 바꿉니다. WorkSpace WorkSpace

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - 포트에서 **22**를 입력합니다.
   - Connection type(연결 유형)에서 SSH를 선택합니다.

   SSH 명령의 예는 이전 절차의 1단계를 참조하십시오.
3. Open을 선택합니다.
4. 메시지가 표시되면 WorkSpaces 클라이언트에서 인증할 때 사용하는 것과 동일한 암호 (Active Directory 암호) 를 입력합니다.

에 대한 필수 구성 및 서비스 구성 요소 WorkSpaces

WorkSpace 관리자는 필수 구성 및 서비스 구성 요소에 대한 다음 사항을 이해해야 합니다.

- the section called “라우팅 테이블 구성”
- the section called “Windows용 구성 요소”
- the section called “Linux용 구성 요소”
- the section called “Ubuntu용 구성 요소”

필수 라우팅 테이블 구성

a에 대한 운영 체제 수준 라우팅 테이블은 수정하지 않는 것이 좋습니다. WorkSpace WorkSpaces 서비스를 이용하려면 이 표에 나와 있는 사전 구성된 경로가 있어야 시스템 상태를 모니터링하고 시스템 구성 요소를 업데이트할 수 있습니다. 조직에 라우팅 테이블을 변경해야 하는 경우 변경 사항을 적용하기 전에 AWS Support 또는 AWS 계정 팀에 문의하세요.

Windows용 필수 서비스 구성 요소

Windows의 WorkSpaces 경우 서비스 구성 요소는 다음 위치에 설치됩니다. 이러한 객체를 삭제하거나, 변경하거나, 차단하거나, 격리하지 마십시오. 이렇게 WorkSpace 하면 가 제대로 작동하지 않습니다.

에 바이러스 백신 소프트웨어가 설치되어 있는 경우 다음 위치에 설치된 서비스 구성 요소를 방해하지 않는지 확인하십시오. WorkSpace

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

32비트 PCoIP 에이전트

2021년 3월 29일부로 PCoIP 에이전트를 32비트에서 64비트로 업데이트했습니다. PCoIP 프로토콜을 사용하는 WorkSpaces Windows의 경우 이는 Teradici 파일의 위치가 에서 로 변경되었음을 의미합니다. `C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici` 정기 유지 관리 기간 중에 PCoIP 에이전트를 업데이트했으므로 전환 중에 일부 사용자가 다른 에이전트보다 32비트 에이전트를 더 오래 WorkSpaces 사용했을 수 있습니다.

방화벽 규칙, 바이러스 백신 소프트웨어 제외(클라이언트 측 및 호스트 측), 그룹 정책 개체(GPO) 설정 또는 Microsoft System Center Configuration Manager(SCCM), Microsoft Endpoint Configuration Manager 또는 32비트 에이전트의 전체 경로를 기반으로 하는 유사한 구성 관리 도구에 대한 설정을 구성한 경우 해당 설정에 64비트 에이전트의 전체 경로를 추가해야 합니다.

32비트 PCoIP 구성 요소의 경로를 필터링하는 경우 구성 요소의 64비트 버전에 경로를 추가해야 합니다. 모든 경로가 동시에 업데이트되지 WorkSpaces 않을 수 있으므로 32비트 경로를 64비트 경로로 바꾸지 마십시오. 그렇지 않으면 일부 경로가 작동하지 않을 수 있습니다. WorkSpaces 예를 들어 `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`에서 제외 또는 통신 필터를 기반으로 하는 경우 `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`도 추가해야 합니다. 마찬가지로, `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`에서 제외 또는 통신 필터를 기반으로 하는 경우 `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`도 추가해야 합니다.

PCoIP 중재자 서비스 변경 — 64비트 에이전트를 사용하도록 업데이트되면 PCoIP 중재자 서비스 (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) 가 제거된다는 점에 유의하십시오. WorkSpaces

PCoIP 제로 클라이언트 및 USB 디바이스 — WorkSpaces Amazon은 PCoIP 에이전트 버전 20.10.4부터 Windows 레지스트리를 통해 USB 리디렉션을 기본적으로 비활성화합니다. 이 레지스트리 설정은 사용자가 PCoIP 제로 클라이언트 디바이스를 사용하여 USB 주변 기기에 연결할 때 USB 주변 기기의 동작에 영향을 줍니다. WorkSpaces 자세한 정보는 USB 프린터 및 기타 USB 주변 디바이스가 PCoIP 제로 클라이언트에서 작동하지 않는 경우을 참조하세요.

Linux용 필수 서비스 구성 요소

Amazon WorkSpaces Linux에서는 서비스 구성 요소가 다음 위치에 설치됩니다. 이러한 객체를 삭제하거나, 변경하거나, 차단하거나, 격리하지 마십시오. 이렇게 WorkSpace 하면 가 제대로 작동하지 않습니다.

> **Note**
>
> 이외의 `/etc/pcoip-agent/pcoip-agent.conf` 파일을 변경하면 작업이 중단되고 파일을 WorkSpaces 다시 빌드해야 할 수도 있습니다. `/etc/pcoip-agent/pcoip-agent.conf` 수정에 대한 자세한 내용은 아마존 리눅스 관리 WorkSpaces 섹션을 참조하세요.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`
- `/etc/os-release`
- `/etc/pam.d/pcoip`

- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent

- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Ubuntu용 필수 서비스 구성 요소

WorkSpacesUbuntu에서는 서비스 구성 요소가 다음 위치에 설치됩니다. 이러한 객체를 삭제하거나, 변경하거나, 차단하거나, 격리하지 마십시오. 이렇게 WorkSpace 하면 가 제대로 작동하지 않습니다.

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service

- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

WorkSpaces 디렉터리 관리

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 다음 옵션 중 하나를 사용할 수 있습니다.

- AD Connector - 기존 온프레미스 Microsoft Active Directory를 사용합니다. 사용자는 온프레미스 자격 증명을 사용하여 WorkSpaces에 로그인하고 WorkSpaces에서 온프레미스 리소스에 액세스할 수 있습니다.
- AWS Managed Microsoft AD - AWS에서 호스팅되는 Microsoft Active Directory를 생성합니다.
- Simple AD - Samba 4를 기반으로 AWS에서 호스팅되는 Microsoft Active Directory 호환 디렉터리를 생성합니다.
- Cross trust - AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 생성합니다.

이러한 디렉터리를 설정하는 WorkSpaces를 시작하는 방법을 예시하는 자습서는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

> **Tip**
>
> 다양한 배포 시나리오에 대한 디렉터리 및 Virtual Private Cloud(VPC) 설계 고려 사항에 대한 자세한 내용은 Best Practices for Deploying Amazon WorkSpaces를 참조하세요.

디렉터리를 생성한 후 WorkSpaces 디렉터리 관리 작업은 대부분 Active Directory 관리 도구와 같은 도구를 사용하여 수행합니다. 일부 디렉터리 관리 작업은 WorkSpaces 콘솔을 사용하고 다른 작업은 그룹 정책을 사용하여 수행할 수 있습니다. 사용자 및 그룹 관리에 대한 자세한 내용은 WorkSpaces 사용자 관리 및 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

> **Note**
>
> - 공유 디렉터리는 현재 WorkSpaces에서 사용이 지원되지 않습니다.
> - 다중 리전 복제를 위해 AWS Managed Microsoft AD 디렉터리를 구성하는 경우 기본 리전의 디렉터리만 Amazon WorkSpaces에서 사용하도록 등록할 수 있습니다. Amazon WorkSpaces에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. AWS Managed Microsoft AD를 사용한 다중 리전 복제는 복제된 리전 내의 Amazon WorkSpaces에서 사용할 수 없습니다.

- Simple AD 및 AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 또는 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.

  빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 또는 AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

목차

WorkSpaces에 디렉터리 등록

WorkSpaces에서 기존 AWS Directory Service 디렉터리를 사용하도록 허용하려면 WorkSpaces에 디렉터리를 등록해야 합니다. 디렉터리를 등록하면 해당 디렉터리에서 WorkSpaces를 시작할 수 있습니다.

요구 사항

WorkSpaces에서 사용할 디렉터리를 등록하려면 다음 요구 사항을 충족해야 합니다.

- AWS Managed Microsoft AD또는 Simple AD를 사용하는 경우 디렉터리가 전용 프라이빗 서브넷에 있을 수 있습니다. 단, 디렉터리가 WorkSpaces가 있는 VPC에 액세스할 수 있어야 합니다.

디렉터리 및 VPC 설계에 대한 자세한 내용은 Best Practices for Deploying Amazon WorkSpaces를 참조하세요.

> **Note**
>
> Simple AD 및 AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 또는 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 또는 AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

디렉터리를 등록하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택합니다.
4. [Actions], [Register]를 선택합니다.

   > **Note**
   >
   > - 공유 디렉터리는 현재 WorkSpaces에서 사용이 지원되지 않습니다.
   > - 다중 리전 복제를 위해 AWS Managed Microsoft AD 디렉터리가 구성된 경우 기본 리전의 디렉터리만 Amazon WorkSpaces에서 사용하도록 등록할 수 있습니다. Amazon WorkSpaces에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. AWS Managed Microsoft AD를 사용한 다중 리전 복제는 복제된 리전 내의 Amazon WorkSpaces에서 사용할 수 없습니다.

5. VPC에서 동일한 가용 영역의 서브넷이 아닌 2개의 서브넷을 선택합니다. 이러한 서브넷은 WorkSpaces를 시작하는 데 사용됩니다. 자세한 내용은 아마존용 가용 영역 WorkSpaces 섹션을 참조하세요.

   > **Note**
   >
   > 어떤 서브넷을 선택해야 할지 모르겠으면 기본 설정 없음을 선택합니다.

6. 셀프 서비스 권한 활성화에서 예를 선택하여 사용자가 WorkSpaces를 다시 빌드하고, 볼륨 크기, 컴퓨팅 유형 및 실행 모드를 변경할 수 있습니다. 활성화하면 Amazon WorkSpaces 요금에 영향을 줄 수 있습니다. 그렇지 않은 경우 아니요를 선택합니다.
7. Amazon WorkDocs 활성화에서 사용할 디렉터리를 등록하려면 예를, 등록하지 않으려면 아니요를 선택합니다.

   > **Note**
   >
   > 이 옵션은 리전에서 Amazon WorkDocs를 사용할 수 있고 AWS Managed Microsoft AD를 사용하지 않는 경우에만 표시됩니다. AWS Managed Microsoft AD를 사용하는 경우 디렉터리 등록을 마친 후 AWS Managed Microsoft AD에 Amazon WorkDocs 활성화 섹션을 참조하세요.

8. 등록(Register)을 선택합니다. 처음에는 [Registered] 값이 `REGISTERING`입니다. 등록이 완료된 후 값은 `Yes`입니다.

WorkSpaces에서 디렉터리 사용을 마쳤으면 디렉터리를 등록 해제할 수 있습니다. 디렉터리를 삭제하려면 먼저 등록을 해제해야 합니다. 디렉터리의 등록을 취소하고 삭제하려면 먼저 디렉터리에 등록된 모든 애플리케이션 및 서비스를 찾아서 제거해야 합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 디렉터리 삭제를 참조하세요.

디렉터리를 등록 해제하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택합니다.
4. 작업(Actions), 등록 취소(Deregister)를 선택합니다.
5. 확인 메시지가 나타나면 [Deregister]를 선택합니다. 등록 해제가 완료된 후 [Registered] 값은 `No`입니다.

내 디렉터리 세부 정보 업데이트 WorkSpaces

WorkSpaces 콘솔을 사용하여 다음 디렉터리 관리 작업을 완료할 수 있습니다.

Tasks

- 조직 단위 선택

- 자동 퍼블릭 IP 주소 구성
- 디바이스 액세스 제어
- 로컬 관리자 권한 관리
- AD Connector 계정 업데이트(AD Connector)
- 다중 인증(AD Connector)

조직 단위 선택

WorkSpace 컴퓨터 계정은 WorkSpaces 디렉터리의 기본 OU (조직 구성 단위) 에 배치됩니다. 처음에는 사용자에 대한 디렉터리 또는 AD Connector가 연결되는 디렉터리의 컴퓨터 OU에 머신 계정이 배치됩니다. 사용자에 대한 디렉터리 또는 연결된 디렉터리에서 다른 OU를 선택할 수도 있고, 별도의 대상 도메인에서 OU를 지정할 수도 있습니다. 디렉터리당 OU를 하나만 선택할 수 있습니다.

새 OU를 선택하면 생성되거나 다시 WorkSpaces 빌드된 모든 컴퓨터 계정이 새로 선택한 OU에 배치됩니다.

조직 구성 단위를 선택하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택합니다.
4. 대상 도메인 및 조직 단위에서 편집을 선택합니다.
5. OU를 찾으려면 대상 및 조직 단위에서 OU 이름 전체 또는 일부를 입력하고 사용할 OU를 선택하면 됩니다.
6. (선택 사항) OU 고유 이름을 선택하여 선택한 OU를 사용자 지정 OU로 덮어씁니다.
7. 저장을 선택합니다.
8. (선택 사항) 기존 WorkSpaces OU를 재구축하여 OU를 업데이트합니다. 자세한 설명은 재구축 a WorkSpace 섹션을 참조하세요.

자동 퍼블릭 IP 주소 구성

퍼블릭 IP 주소 자동 할당을 활성화하면 시작하는 각 WorkSpace 주소에 Amazon에서 제공한 퍼블릭 주소 풀의 퍼블릭 IP 주소가 할당됩니다. 퍼블릭 WorkSpace 서브넷의 A는 퍼블릭 IP 주소가 있는 경우 인터넷 게이트웨이를 통해 인터넷에 액세스할 수 있습니다. WorkSpaces 자동 할당을 활성화하기 전에 이미 존재하는 주소는 다시 구축할 때까지 공용 주소를 받지 않습니다.

프라이빗 서브넷에 WorkSpaces 있고 가상 프라이빗 클라우드 (VPC) 용 NAT 게이트웨이를 구성한 경우 또는 퍼블릭 서브넷에 있고 엘라스틱 IP 주소를 할당한 경우에는 퍼블릭 주소 자동 할당을 활성화하지 않아도 WorkSpaces 됩니다. 자세한 설명은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요.

> **Warning**
>
> 소유한 엘라스틱 IP 주소를 에 연결한 WorkSpace 다음 나중에 해당 엘라스틱 IP 주소를 에서 분리하면 퍼블릭 IP 주소가 WorkSpace 손실되고 Amazon 제공 풀에서 새 주소를 자동으로 가져오지 않습니다. WorkSpace Amazon에서 제공한 풀의 새 퍼블릭 IP 주소를 와 연결하려면 를 WorkSpace 재구축해야 합니다. WorkSpace 를 다시 빌드하지 않으려면 소유한 WorkSpace 다른 엘라스틱 IP 주소를 에 연결해야 합니다. WorkSpace

탄력적 IP 주소를 구성하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 원하는 디렉토리를 선택합니다 WorkSpaces.
4. [Actions], [Update Details]를 선택합니다.
5. [Access to Internet]을 확장하고 [Enable] 또는 [Disable]을 선택합니다.
6. 업데이트를 선택합니다.

디바이스 액세스 제어

에 액세스할 수 있는 장치 유형을 지정할 수 WorkSpaces 있습니다. 또한 신뢰할 수 있는 장치 (관리 대상 장치라고도 함) 에 대한 WorkSpaces 액세스를 제한할 수 있습니다.

장치 액세스를 제어하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택합니다.
4. 액세스 제어 옵션에서 편집을 선택합니다.

5. 신뢰할 수 있는 장치에서 모두 허용, 신뢰할 수 있는 장치 또는 모두 거부를 WorkSpaces 선택하여 액세스할 수 있는 장치 유형을 지정합니다. 자세한 설명은 신뢰할 수 있는 장치에 WorkSpaces 대한 액세스 제한 섹션을 참조하세요.
6. 저장(Save)을 선택합니다.

로컬 관리자 권한 관리

사용자가 로컬 관리자인지 여부를 지정하여 사용자가 자신의 WorkSpaces 응용 프로그램을 설치하고 설정을 수정할 수 있도록 할 수 WorkSpaces 있습니다. 사용자는 기본적으로 로컬 관리자입니다. 이 설정을 수정하면 새로 만드는 모든 설정과 다시 WorkSpaces 빌드하는 모든 WorkSpaces 항목에 변경 내용이 적용됩니다.

로컬 관리자 권한을 수정하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택합니다.
4. 로컬 관리자 설정에서 편집을 선택합니다.
5. 사용자가 로컬 관리자인지 확인하려면 로컬 관리자 설정 활성화를 선택합니다.
6. 저장을 선택합니다.

AD Connector 계정 업데이트(AD Connector)

사용자 및 그룹을 읽고 WorkSpaces 컴퓨터 계정을 AD Connector 디렉터리에 연결하는 데 사용되는 AD Connector 계정을 업데이트할 수 있습니다.

AD Connector 계정을 업데이트하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택한 다음 세부 정보 보기를 선택합니다.
4. AD 커넥터 계정에서 편집을 선택합니다.
5. 새 계정의 로그인 보안 인증 정보를 입력합니다.
6. 저장을 선택합니다.

다중 인증(AD Connector)

AD Connector 디렉터리에서 다중 인증(MFA)을 활성화할 수 있습니다. AWS Directory Service에서 다중 인증을 사용하는 방법에 대한 자세한 내용은 AD Connector에 대한 다중 인증 활성화 및 AD Connector 사전 조건을 참조하세요.

> **Note**
>
> - RADIUS 서버는 AWS에서 호스팅하거나 온프레미스일 수 있습니다.
> - 사용자 이름은 Active Directory와 RADIUS 서버 간에 일치해야 합니다.

멀티 팩터 인증을 활성화하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택한 다음 [Actions], [Update Details]를 선택합니다.
4. [Multi-Factor Authentication]을 확장하여 [Enable Multi-Factor Authentication]을 선택합니다.
5. [RADIUS server IP address(es)]에 RADIUS 서버 엔드포인트의 IP 주소를 쉼표로 구분하여 입력하거나 RADIUS 서버 로드 밸런서의 IP 주소를 입력합니다.
6. [Port]에 통신에 사용하는 RADIUS 서버의 포트를 입력합니다. 온프레미스 네트워크는 AD Connector에서 기본 RADIUS 서버 포트(UDP:1812)로 전송되는 인바운드 트래픽을 허용해야 합니다.
7. [Shared secret code] 및 [Confirm shared secret code]에 RADIUS 서버의 공유 비밀 코드를 입력합니다.
8. [Protocol]에서 RADIUS 서버의 프로토콜을 선택합니다.
9. [Server timeout]에 RADIUS 서버가 응답할 때까지 대기할 시간을 초 단위로 입력합니다. 이 값은 1~50이어야 합니다.
10. [Max retries]에 RADIUS 서버와 통신을 시도하는 횟수를 입력합니다. 이 값은 0~10이어야 합니다.
11. [Update and Exit]를 선택합니다.

[RADIUS status]가 [Enabled]로 변경되면 멀티 팩터 인증을 사용할 수 있습니다. 다단계 인증을 설정하는 동안에는 사용자가 로그인할 수 없습니다. WorkSpaces

Amazon WorkSpaces에 사용되는 DNS 서버 업데이트

WorkSpaces를 시작한 후 Active Directory의 DNS 서버 IP 주소를 업데이트해야 하는 경우 WorkSpaces도 새 DNS 서버 설정으로 업데이트해야 합니다.

다음 방법 중 하나로 WorkSpaces를 새 DNS 설정으로 업데이트할 수 있습니다.

- Active Directory의 DNS 설정을 업데이트하기 전에 WorkSpaces의 DNS 설정을 업데이트합니다.
- Active Directory의 DNS 설정을 업데이트한 후에에 WorkSpaces를 재구축합니다.

Active Directory에서 DNS 설정을 업데이트하기 전에 WorkSpaces에서 DNS 설정을 업데이트하는 것이 좋습니다(다음 절차의 1단계 설명 참조).

WorkSpaces를 재구축하려면 Active Directory의 DNS 서버 IP 주소 중 하나를 업데이트한 다음(2단계) 재구축 a WorkSpace의 절차에 따라 WorkSpaces를 재구축하세요. WorkSpaces를 재구축한 후에는 3단계의 절차에 따라 DNS 서버 업데이트를 테스트하세요. 이 단계를 완료한 후 Active Directory에서 두 번째 DNS 서버의 IP 주소를 업데이트한 다음 WorkSpaces를 재구축하세요. 3단계의 절차에 따라 두 번째 DNS 서버 업데이트를 테스트해야 합니다. 모범 사례 섹션에 설명된 대로 DNS 서버 IP 주소를 한 번에 하나씩 업데이트하는 것이 좋습니다.

모범 사례

DNS 서버 설정을 업데이트할 때 다음과 같은 모범 사례를 적용하는 것이 좋습니다.

- 도메인 리소스 연결이 끊기고 액세스 불가능한 상황을 예방하기 위해 사용량이 적은 시간대나 계획된 유지 관리 기간에 DNS 서버 업데이트를 수행하는 것이 좋습니다.
- DNS 서버 설정을 변경하기 전 15분과 변경 후 15분 동안에는 새 WorkSpaces를 시작하지 마세요.
- DNS 서버 설정을 업데이트할 때는 DNS 서버 IP 주소를 한 번에 하나씩 변경하세요. 두 번째 IP 주소를 업데이트하기 전에 첫 번째 업데이트가 올바른지 확인하세요. 다음 절차(1단계, 2단계, 3단계)를 두 번 수행하여 IP 주소를 한 번에 하나씩 업데이트하는 것이 좋습니다.

1단계: WorkSpaces에서 DNS 서버 설정 업데이트

다음 절차에서는 현재 및 신규 DNS 서버 IP 주소 값이 다음과 같습니다.

- 현재 DNS IP 주소:*OldIP1*, *OldIP2*
- 신규 DNS IP 주소: *NewIP1*, *NewIP2*

> **Note**
>
> 이 절차를 두 번째로 수행하는 경우 *OldIP1*을 *OldIP2*로, *NewIP1*를 *NewIP2*로 바꾸세요.

Windows WorkSpaces의 DNS 서버 설정 업데이트

WorkSpaces가 여러 개인 경우 WorkSpaces의 Active Directory OU에 그룹 정책 개체(GPO)를 적용하여 다음 레지스트리 업데이트를 WorkSpaces에 배포할 수 있습니다. GPO 작업에 대한 자세한 내용은 윈도우 관리하기 WorkSpaces 섹션을 참조하세요.

레지스트리 편집기를 사용하거나 Windows PowerShell을 사용하여 이러한 업데이트를 수행할 수 있습니다. 두 절차 모두 이 섹션에 설명되어 있습니다.

레지스트리 편집기를 사용하여 DNS 레지스트리 설정을 업데이트하는 방법

1. Windows WorkSpace에서 Windows 검색 상자를 열고 **registry editor**를 입력하여 레지스트리 편집기(regedit.exe)를 엽니다.
2. "이 앱이 디바이스를 변경할 수 있도록 허용하시겠습니까?"라고 묻는 메시지가 나타나면 예를 선택합니다.
3. 레지스트리 편집기에서 다음 레지스트리 항목으로 이동합니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight
4. DomainJoinDns 레지스트리 키를 엽니다. *OldIP1*을 *NewIP1*로 업데이트한 다음 확인을 선택합니다.
5. 레지스트리 편집기를 닫습니다.
6. WorkSpace를 재부팅하거나 서비스 SkyLightWorkspaceConfigService를 다시 시작합니다.

   > **Note**
   >
   > 서비스 SkyLightWorkspaceConfigService를 다시 시작한 후 네트워크 어댑터가 변경 사항을 반영하는 데 최대 1분이 걸릴 수 있습니다.
7. 2단계로 진행하여 Active Directory의 DNS 서버 설정을 업데이트하여 *OldIP1*을 *NewIP1*로 바꿉니다.

PowerShell을 사용하여 DNS 레지스트리 설정을 업데이트하는 방법

다음 절차는 PowerShell 명령을 사용하여 레지스트리를 업데이트하고 서비스 SkyLightWorkspaceConfigService를 다시 시작합니다.

1. Windows WorkSpace에서 Windows 검색 상자를 열고 **powershell**을 입력합니다. [Run as Administrator]를 선택합니다.
2. "이 앱이 디바이스를 변경할 수 있도록 허용하시겠습니까?"라고 묻는 메시지가 나타나면 예를 선택합니다.
3. PowerShell 창에서 다음 명령을 실행하여 현재 DNS 서버 IP 주소를 검색합니다.

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

   다음과 같이 출력될 것입니다.

```
DomainJoinDns : OldIP1,OldIP2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon\SkyLight
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon
PSChildName   : SkyLight
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. PowerShell 창에서 다음 명령을 실행하여 *OldIP1*을 *NewIP1*로 변경합니다. 지금은 *OldIP2*를 그대로 두세요.

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. 다음 명령을 실행하여 서비스 SkyLightWorkspaceConfigService를 다시 시작합니다.

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> 서비스 SkyLightWorkspaceConfigService를 다시 시작한 후 네트워크 어댑터가 변경 사항을 반영하는 데 최대 1분이 걸릴 수 있습니다.

6. 2단계로 진행하여 Active Directory의 DNS 서버 설정을 업데이트하여 *OldIP1*을 *NewIP1*로 바꿉니다.

Linux WorkSpaces의 DNS 서버 설정 업데이트

Linux WorkSpaces가 두 개 이상 있다면 구성 관리 솔루션을 사용하여 정책을 배포하고 적용하는 것이 좋습니다. 예를 들어, AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise 또는 Ansible을 사용할 수 있습니다.

Linux WorkSpaces에서 DNS 서버 설정을 업데이트하는 방법

1. Linux WorkSpaces에서 터미널 창을 엽니다(애플리케이션 > 시스템 도구 > MATE 터미널).
2. 다음 Linux 명령을 실행하여 `/etc/dhcp/dhclient.conf` 파일을 편집합니다. 이 파일을 편집하려면 루트 사용자 권한이 있어야 합니다. `sudo -i` 명령을 사용하여 루트가 되거나, 아래처럼 sudo를 사용하여 모든 명령을 실행하세요.

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   `/etc/dhcp/dhclient.conf` 파일에서 다음 `prepend` 명령을 볼 수 있습니다. *OldIP1*과 *OldIP2*는 DNS 서버의 IP 주소입니다.

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. *OldIP1*을 *NewIP1*로 바꾸고 지금은 *OldIP2*를 그대로 둡니다.
4. `/etc/dhcp/dhclient.conf`에 변경 사항을 저장합니다.
5. WorkSpace를 재부팅합니다.
6. 2단계로 진행하여 Active Directory의 DNS 서버 설정을 업데이트하여 *OldIP1*을 *NewIP1*로 바꿉니다.

2단계: Active Directory에 사용되는 DNS 서버 설정 업데이트

이 단계에서는 Active Directory에 사용되는 DNS 서버 설정을 업데이트합니다. 모범 사례 섹션에 설명된 대로 DNS 서버 IP 주소를 한 번에 하나씩 업데이트하는 것이 좋습니다.

Active Directory의 DNS 서버 설정을 업데이트하려면 AWS Directory Service 관리 안내서의 다음 설명서를 참조하세요.

- AD Connector: AD Connector의 DNS 주소 업데이트

- AWS Managed Microsoft AD: 온프레미스 도메인을 위한 DNS 조건부 전달자 구성
- Simple AD: DNS 구성

DNS 서버 설정을 업데이트한 후 3단계로 진행하세요.

3단계: 업데이트된 DNS 서비스 서버 테스트

1단계와 2단계를 완료한 후 다음 절차를 사용하여 업데이트된 DNS 서버 설정이 예상대로 작동하는지 확인합니다.

다음 절차에서는 현재 및 신규 DNS 서버 IP 주소 값이 다음과 같습니다.

- 현재 DNS IP 주소:*OldIP1*, *OldIP2*
- 신규 DNS IP 주소: *NewIP1*, *NewIP2*

> **Note**
>
> 이 절차를 두 번째로 수행하는 경우 *OldIP1*을 *OldIP2*로, *NewIP1*를 *NewIP2*로 바꾸세요.

Windows WorkSpaces의 업데이트된 DNS 서버 설정 테스트

1. *OldIP1* DNS 서버를 종료합니다.
2. Windows WorkSpace에 로그인합니다.
3. Windows 시작 메뉴에서 Windows 시스템을 선택한 다음 명령 프롬프트를 선택합니다.
4. 다음 명령을 실행합니다. 여기서 *AD_Name*은 Active Directory의 이름(예: `corp.example.com`)입니다.

   ```
   nslookup AD_Name
   ```

   `nslookup` 명령은 다음 출력을 반환합니다. (이 절차를 두 번째로 수행하는 경우에는 *OldIP2* 대신 *NewIP2*가 나타납니다.)

   ```
   Server:  Full_AD_Name
   Address:  NewIP1
   ```

```
Name:     AD_Name
Addresses:  OldIP2
            NewIP1
```

5. 출력이 예상한 것과 다르거나 오류가 발생하는 경우 1단계를 반복합니다.
6. 한 시간 정도 기다린 후 보고된 문제가 없는지 확인합니다. *NewIP1*이 DNS 쿼리를 받고 답변으로 응답하고 있는지 확인하세요.
7. 첫 번째 DNS 서버가 제대로 작동하는지 확인한 후 1단계를 반복하여 두 번째 DNS 서버를 업데이트합니다. 이번에는 *OldIP2*를 *NewIP2*로 교체합니다. 그런 다음 2단계와 3단계를 반복합니다.

Linux WorkSpaces의 업데이트된 DNS 서버 설정 테스트

1. *OldIP1* DNS 서버를 종료합니다.
2. Linux WorkSpace에 로그인합니다.
3. Linux WorkSpaces에서 터미널 창을 엽니다(애플리케이션 > 시스템 도구 > MATE 터미널).
4. DHCP 응답에서 반환된 DNS 서버 IP 주소는 WorkSpace의 로컬 `/etc/resolv.conf` 파일에 기록됩니다. 다음 명령을 실행하여 `/etc/resolv.conf` 파일의 내용을 확인합니다.

```
cat /etc/resolv.conf
```

다음과 같이 출력되어야 합니다. (이 절차를 두 번째로 수행하는 경우에는 *OldIP2* 대신 *NewIP2*가 나타납니다.)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> `/etc/resolv.conf` 파일을 수동으로 수정하는 경우 WorkSpace를 다시 시작하면 해당 변경 사항이 손실됩니다.

5. 출력이 예상한 것과 다르거나 오류가 발생하는 경우 1단계를 반복합니다.

6. 실제 DNS 서버 IP 주소는 `/etc/dhcp/dhclient.conf` 파일에 저장됩니다. 파일의 내용을 확인하려면 다음 명령을 실행합니다.

   ```
   sudo cat /etc/dhcp/dhclient.conf
   ```

   다음과 같이 출력되어야 합니다. (이 절차를 두 번째로 수행하는 경우에는 *OldIP2* 대신 *NewIP2*가 나타납니다.)

   ```
   # This file is generated by Amazon WorkSpaces
   # Modifying it can make your WorkSpace inaccessible until rebuild
   prepend domain-name-servers NewIP1, OldIP2; # skylight
   ```

7. 한 시간 정도 기다린 후 보고된 문제가 없는지 확인합니다. *NewIP1*이 DNS 쿼리를 받고 답변으로 응답하고 있는지 확인하세요.

8. 첫 번째 DNS 서버가 제대로 작동하는지 확인한 후 1단계를 반복하여 두 번째 DNS 서버를 업데이트합니다. 이번에는 *OldIP2*를 *NewIP2*로 교체합니다. 그런 다음 2단계와 3단계를 반복합니다.

WorkSpaces용 디렉터리 삭제

더 이상 다른 WorkSpaces 또는 다른 애플리케이션(예: Amazon WorkDocs, Amazon WorkMail 또는 Amazon Chime)에서 사용하지 않는 경우 WorkSpaces용 디렉터리를 삭제할 수 있습니다. 디렉터리를 삭제하려면 먼저 등록을 해제해야 합니다.

> **Note**
>
> Simple AD 및 AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 또는 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
> Simple AD 또는 AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

디렉터리가 삭제될 경우

Simple AD 또는 AWS Directory Service for Microsoft Active Directory 디렉터리가 삭제되면 모든 디렉터리 데이터와 스냅샷이 삭제되어 복구가 불가능합니다. 디렉터리가 삭제된 후에도 디렉터리에 조인

된 Amazon EC2 인스턴스는 변동 없이 보관됩니다. 그러나 디렉터리 자격 증명을 사용해서 이러한 인스턴스에 로그인할 수 없습니다. 인스턴스에 로컬인 AWS 계정을 통해 이러한 인스턴스에 로그인해야 합니다.

AD Connector 디렉터리가 삭제되어도 온프레미스 디렉터리는 그대로 유지됩니다. 디렉터리에 조인된 모든 Amazon EC2 인스턴스도 변동 없이 보관되며, 온프레미스 디렉터리에 조인된 상태가 유지됩니다. 여전히 디렉터리 자격 증명을 사용해 이러한 인스턴스에 로그인할 수 있습니다.

디렉터리를 삭제하는 방법

1. 디렉터리의 모든 WorkSpaces를 삭제합니다. 자세한 내용은 WorkSpace 삭제 섹션을 참조하세요.
2. 디렉터리에 등록된 모든 애플리케이션 및 서비스를 찾아 제거합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 디렉터리 삭제를 참조하세요.
3. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
4. 탐색 창에서 [Directories]를 선택합니다.
5. 디렉터리를 선택하고 [Actions], [Deregister]를 선택합니다.
6. 확인 메시지가 나타나면 [Deregister]를 선택합니다.
7. 디렉터리를 다시 선택하고 [Actions], [Delete]를 선택합니다.
8. 확인 메시지가 나타나면 Delete(삭제)를 선택합니다.

> **Note**
>
> 애플리케이션 할당을 제거하는 데 예상보다 시간이 오래 걸릴 수 있습니다. 다음 오류 메시지가 나타나면 모든 애플리케이션 할당을 제거했는지 확인한 다음, 디렉터리를 다시 삭제하기 전에 30-60분 정도 기다립니다.
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (선택 사항) 디렉터리의 가상 사설 클라우드(VPC)에서 모든 리소스를 삭제한 후 해당 VPC를 삭제하고 NAT 게이트웨이에 사용된 탄력적 IP 주소를 해제할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 삭제 및 탄력적 IP 주소 작업을 참조하세요.
10. (선택 사항) 사용을 마친 사용자 지정 번들 및 이미지를 삭제하려면 사용자 지정 WorkSpaces 번들 또는 이미지 삭제 단원을 참조하십시오.

AWS Managed Microsoft AD에 Amazon WorkDocs 활성화

Amazon WorkSpaces와 함께 AWS Managed Microsoft AD를 사용하는 경우 Amazon WorkDocs 콘솔 또는 AWS Directory Service 콘솔을 통해 디렉터리에 대해 Amazon WorkDocs를 활성화할 수 있습니다.

> **Note**
>
> Amazon WorkSpaces를 사용할 수 있는 모든 AWS 리전에서 Amazon WorkDocs를 사용할 수 있는 것은 아닙니다. 자세한 내용은 Amazon WorkDocs 요금을 참조하세요.

Amazon WorkDocs 콘솔을 통해 WorkDocs를 활성화하는 방법

1. https://console.aws.amazon.com/zocalo/에서 Amazon WorkDocs 콘솔을 엽니다.
2. [Create a New WorkDocs Site]를 선택합니다.
3. [Standard Setup]에서 [Launch]를 선택합니다.
4. 디렉터리를 선택하고 사이트 이름을 생성합니다.
5. WorkDocs 사이트를 관리할 사용자를 지정합니다. 관리자 또는 디렉터리에서 생성된 사용자를 사용할 수 있습니다.

자세한 내용은 Amazon WorkDocs 관리 안내서의 AWS Managed Microsoft AD 시작하기를 참조하세요.

AWS Directory Service 콘솔을 통해 WorkDocs를 활성화하려면

1. https://console.aws.amazon.com/directoryservicev2/에서 AWS Directory Service 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. [Directories] 페이지에서 디렉터리를 선택합니다.
4. 디렉터리 세부 정보 페이지에서 Application management 탭을 선택합니다.
5. 액세스 URL이 디렉터리에 할당되지 않은 경우 애플리케이션 액세스 URL 섹션에 생성 버튼이 표시됩니다. 디렉터리 별칭을 입력하고 생성을 선택합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 액세스 URL 생성하기를 참조하세요.
6. 애플리케이션 액세스 URL 섹션에서 Enable(활성화)을 선택하여 Amazon WorkDocs에 대한 Single Sign-On을 활성화합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Single Sign-On을 참조하세요.

WorkSpaces용 Active Directory 관리 도구 설정

WorkSpaces 디렉터리 관리 작업은 대부분 Active Directory 관리 도구와 같은 디렉터리 관리 도구를 사용하여 수행합니다. 하지만 일부 디렉터리 관련 작업은 WorkSpaces 콘솔에서 수행합니다. 자세한 내용은 WorkSpaces 디렉터리 관리 섹션을 참조하세요.

5개 이상의 WorkSpaces를 포함하는 AWS Managed Microsoft AD 또는 Simple AD를 사용하여 디렉터리를 생성하는 경우 Amazon EC2 인스턴스에 관리를 중앙 집중화하는 것이 좋습니다. WorkSpaces에 디렉터리 관리 도구를 설치할 수 있지만 Amazon EC2 인스턴스를 사용하는 것이 더 강력한 솔루션입니다.

Active Directory 관리 도구를 설정하려면

1. Amazon EC2 Windows 인스턴스를 시작하고 다음 옵션 중 하나를 사용하여 WorkSpaces 디렉터리에 연결합니다.

   - 기존 Amazon EC2 Windows 인스턴스가 아직 없는 경우, 인스턴스를 시작할 때 디렉터리 도메인에 인스턴스를 조인할 수 있습니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Windows EC2 인스턴스를 원활하게 조인을 참조하세요.
   - 기존 Amazon EC2 Windows 인스턴스가 이미 있는 경우 해당 인스턴스를 디렉터리에 수동으로 조인할 수 있습니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Manually Add a Windows Instance를 참조하세요.
2. Amazon EC2 Windows 인스턴스에 Active Directory 관리 도구를 설치합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Active Directory 관리 도구 설치를 참조하세요.

   > **Note**
   >
   > Active Directory 관리 도구를 설치할 때는 그룹 정책 관리도 선택하여 그룹 정책 관리 편집기(gpmc.msc) 도구를 설치해야 합니다.

   기능 설치가 완료되면 Windows Start 메뉴의 Windows Administrative Tools에서 Active Directory 도구를 사용할 수 있습니다.
3. 다음과 같이 디렉터리 관리자로 도구를 실행합니다.

   a. Windows Start 메뉴에서 Windows Administrative Tools를 엽니다.
   b. Shift 키를 누른 상태에서 도구 바로 가기를 마우스 오른쪽 버튼으로 클릭하고 Run as different user를 선택합니다.

c. 관리자의 로그인 보안 인증 정보를 입력합니다. Simple AD의 경우 사용자 이름이 **Administrator**이고, AWS Managed Microsoft AD의 경우 관리자가 **Admin**입니다.

이제 익숙한 Active Directory 도구를 사용하여 디렉터리 관리 작업을 수행할 수 있습니다. 예를 들어 Active Directory 사용자 및 컴퓨터 도구를 사용하여 사용자를 추가하거나, 사용자를 제거하거나, 사용자를 디렉터리 관리자로 승격하거나, 사용자 암호를 재설정할 수 있습니다. 해당 디렉터리에서 사용자를 관리할 수 있는 권한이 있는 사용자로 Windows 인스턴스에 로그인해야 한다는 점을 유의해야 합니다.

사용자를 디렉터리 관리자로 승격시키려면

> **Note**
>
> 이 절차는 AWS Managed AD가 아닌 Simple AD를 사용하여 만든 디렉터리에만 적용됩니다. AWS Managed AD로 만든 디렉터리의 경우 AWS Directory Service 관리 안내서의 Manage Users and Groups in AWS Managed Microsoft AD를 참조하세요.

1. Active Directory 사용자 및 컴퓨터 도구를 엽니다.
2. 도메인 아래의 [Users] 폴더로 이동하고 승격시킬 사용자를 선택합니다.
3. [Action], [Properties]를 선택합니다.
4. ***username*** 속성 대화 상자에서 Member of를 선택합니다.
5. 다음 그룹에 사용자를 추가하고 [OK]를 선택합니다.
   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

사용자를 추가하거나 제거하려면

WorkSpace를 시작하는 프로세스 동안에만 Amazon WorkSpaces 콘솔에서 새로운 사용자를 생성할 수 있으며, Amazon WorkSpaces 콘솔을 통해 사용자를 삭제할 수는 없습니다. 사용자 그룹 관리를 포함한 대부분의 사용자 관리 작업은 디렉터리를 통해 수행해야 합니다.

> **Important**
>
> 사용자를 제거하려면 먼저 해당 사용자에 할당된 WorkSpaces를 삭제해야 합니다. 자세한 내용은 WorkSpace 삭제 섹션을 참조하세요.

사용자 및 그룹을 관리하는 데 사용하는 프로세스는 사용 중인 디렉터리 유형에 따라 다릅니다.

- AWS Managed Microsoft AD를 사용하는 경우 AWS Directory Service 관리 안내서의 Manage Users and Groups in AWS Managed Microsoft AD를 참조하세요.
- Simple AD를 사용하는 경우 AWS Directory Service 관리 안내서의 Simple AD에서 사용자 및 그룹 관리를 참조하세요.
- AD Connector 또는 신뢰 관계를 통해 Microsoft Active Directory를 사용하는 경우 Active Directory 모듈을 사용하여 사용자 및 그룹을 관리할 수 있습니다.

사용자 암호를 재설정하려면

기존 사용자의 암호를 재설정하는 경우 [User must change password at next logon]을 설정하지 마십시오. 그렇지 않으면 사용자가 본인의 WorkSpaces에 연결할 수 없습니다. 대신 각 사용자에게 안전한 임시 암호를 할당하고 다음에 로그온할 때 WorkSpaces 내에서 암호를 수동으로 변경하도록 요청합니다.

> **Note**
>
> AD Connector를 사용하거나 사용자가 AWS GovCloud(미국 서부) 리전에 있는 경우 사용자는 자신의 암호를 재설정할 수 없습니다. (WorkSpaces 클라이언트 애플리케이션 로그인 화면에서 암호 찾기 옵션을 사용할 수 없습니다.)

WorkSpaces를 사용하여 가상 데스크톱 시작

WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Microsoft Windows, Amazon Linux 또는 Ubuntu Linux 데스크톱을 프로비저닝할 수 있습니다.

> **Note**
>
> Amazon WorkSpaces 콘솔의 WorkSpaces에 표시되는 컴퓨터 이름 값은 시작한 WorkSpace의 유형(Amazon Linux, Ubuntu 또는 Windows)에 따라 달라집니다. WorkSpace의 컴퓨터 이름은 두 가지 형식 중 하나일 수 있습니다.
>
> - Amazon Linux: A-*xxxxxxxxxxxxx*
> - Ubuntu: U-*xxxxxxxxxxxxx*
> - Windows: IP-C*xxxxxx* 또는 WSAMZN-*xxxxxxx* 또는 EC2AMAZ-*xxxxxxx*
>
> Windows WorkSpaces의 경우 컴퓨터 이름 형식은 번들 유형에 따라 결정되며, 퍼블릭 번들 또는 퍼블릭 이미지 기반 사용자 지정 번들로 만든 WorkSpaces의 경우 퍼블릭 이미지가 생성된 시기에 따라 결정됩니다.
> 2020년 6월 22일부터 퍼블릭 번들에서 시작된 Windows WorkSpaces의 컴퓨터 이름에 IP-*xxxxxx* 형식 대신 WSAMZN-*xxxxxxx* 형식이 적용됩니다.
> 퍼블릭 이미지를 기반으로 하는 사용자 지정 번들의 경우, 2020년 6월 22일 이전에 생성된 퍼블릭 이미지의 경우 컴퓨터 이름은 EC2AMAZ-*xxxxxxx* 형식입니다. 퍼블릭 이미지가 2020년 6월 22일 또는 그 이후에 생성된 경우 컴퓨터 이름은 WSAMZN-*xxxxxxx* 형식입니다.
> 기존 보유 라이선스 사용(BYOL) 번들의 경우 기본적으로 DESKTOP-*xxxxxxx* 또는 EC2AMAZ-*xxxxxxx* 형식이 컴퓨터 이름에 사용됩니다.
> 사용자 지정 번들 또는 BYOL 번들에서 컴퓨터 이름에 사용자 지정 형식을 지정한 경우 사용자 지정 형식이 이러한 기본값보다 우선 적용됩니다. 사용자 정의 형식을 지정하려면 사용자 지정 WorkSpaces 이미지 및 번들 생성 섹션을 참조하세요.
> 중요 - Windows 시스템 설정을 통해 WorkSpaces의 컴퓨터 이름을 변경하면 WorkSpaces에 더 이상 액세스할 수 없습니다.

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 다음 중 무엇이든 수행할 수 있습니다.

- Simple AD 디렉터리를 생성합니다.

- AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service를 생성합니다.
- Active Directory Connector를 사용하여 기존 Microsoft Active Directory에 연결합니다.
- AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 생성합니다.

> **Note**
>
> - 공유 디렉터리는 현재 WorkSpaces에서 사용이 지원되지 않습니다.
> - 다중 리전 복제를 위해 AWS Managed Microsoft AD 디렉터리를 구성하는 경우 기본 리전의 디렉터리만 Amazon WorkSpaces에서 사용하도록 등록할 수 있습니다. Amazon WorkSpaces에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. AWS Managed Microsoft AD를 사용한 다중 리전 복제는 복제된 리전 내의 Amazon WorkSpaces에서 사용할 수 없습니다.
> - Simple AD 및 AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 또는 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
>
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 또는 AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

다음 자습서에서는 지원되는 디렉터리 서비스 옵션을 사용하여 WorkSpace를 시작하는 방법을 안내합니다.

자습서

- AWS Managed Microsoft AD를 사용하여 WorkSpace 시작
- Simple AD를 사용하여 WorkSpaces 시작
- AD Connector를 사용하여 WorkSpaces 시작
- 신뢰할 수 있는 도메인을 사용하여 WorkSpace 시작

AWS Managed Microsoft AD를 사용하여 WorkSpace 시작

WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Windows 및 Linux 데스크톱을 프로비저닝할 수 있습니다.

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 디렉터리는 Simple AD, AD Connector, 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service 중에서 선택할 수 있습니다. 또한 AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 설정할 수 있습니다.

이 자습서에서는 AWS Managed Microsoft AD를 사용하는 WorkSpace를 시작합니다. 다른 옵션을 사용하는 자습서는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

작업

시작하기 전에

- 일부 리전에서는 WorkSpaces를 사용할 수 없습니다. 지원되는 리전을 확인한 후 WorkSpaces용 리전을 선택합니다. 지원되는 리전에 대한 자세한 내용은 AWS 리전별 WorkSpaces 요금을 참조하세요.
- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 번들은 운영 체제, 스토리지, 컴퓨팅 및 소프트웨어 리소스의 조합입니다. 자세한 내용은 Amazon WorkSpaces 번들 단원을 참조하십시오.
- AWS Directory Service을(를) 사용하여 디렉터리를 생성하거나 WorkSpace를 시작할 때 퍼블릭 서브넷 1개와 프라이빗 서브넷 2개를 포함하여 구성된 가상 사설 클라우드를 생성하거나 선택해야 합니다. 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요.

1단계: AWS Managed Microsoft AD 디렉터리 생성

먼저 AWS Managed Microsoft AD 디렉터리를 만듭니다. AWS Directory Service이(가) VPC의 각 프라이빗 서브넷에 하나씩 두 개의 디렉터리 서버를 생성합니다. 처음에는 디렉터리에 사용자가 없습니다. 다음 단계에서 WorkSpaces를 시작할 때 사용자를 추가합니다.

> **Note**
>
> - 공유 디렉터리는 현재 WorkSpaces에서 사용이 지원되지 않습니다.
> - 다중 리전 복제를 위해 AWS Managed Microsoft AD 디렉터리가 구성된 경우 기본 리전의 디렉터리만 Amazon WorkSpaces에서 사용하도록 등록할 수 있습니다. Amazon WorkSpaces에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. AWS Managed Microsoft AD를 사용한 다중 리전 복제는 복제된 리전 내의 Amazon WorkSpaces에서 사용할 수 없습니다.

AWS Managed Microsoft AD 디렉터리를 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. [Set up Directory], [Create Microsoft AD]를 선택합니다.
4. 다음과 같이 디렉터리를 구성합니다.

   a. 조직 이름에 디렉터리의 고유한 조직 이름(예: my-demo-directory)을 입력합니다. 이 이름은 길이가 4자 이상이고, 영숫자 및 하이픈(-)만으로 구성되고, 하이픈 이외의 문자로 시작하거나 끝나야 합니다.

   b. 디렉터리 DNS에 디렉터리의 정규화된 이름(예: workspaces.demo.com)을 입력합니다.

   > **Important**
   >
   > WorkSpaces를 시작한 후 DNS 서버를 업데이트해야 하는 경우, Amazon WorkSpaces에 사용되는 DNS 서버 업데이트의 절차에 따라 WorkSpaces가 제대로 업데이트되도록 하세요.

   c. NetBIOS 이름에 디렉터리의 짧은 이름(예: workspaces)을 입력합니다.

d. 관리자 암호 및 암호 확인에 디렉터리 관리자 계정의 암호를 입력합니다. 암호 요구 사항에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD 디렉터리 생성을 참조하세요.

e. (선택 사항) 설명에 디렉터리에 대한 설명을 입력합니다.

f. [VPC]에서 앞서 생성한 VPC를 선택합니다.

g. [Subnets]에서 2개의 프라이빗 서브넷(CIDR 블록 `10.0.1.0/24` 및 `10.0.2.0/24`를 포함)을 선택합니다.

h. 다음 단계(Next Step)를 선택합니다.

5. [Create Microsoft AD]를 선택합니다.

6. 완료(Done)를 선택합니다. 디렉터리의 초기 상태는 `Creating`입니다. 디렉터리 생성 과정이 완료되면 상태가 `Active`로 변경됩니다.

2단계: WorkSpaces 생성

이제 AWS Managed Microsoft AD 디렉터리를 생성했으므로 WorkSpace를 생성할 준비가 되었습니다.

WorkSpaces를 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.

2. 탐색 창에서 WorkSpaces를 선택합니다.

3. [Launch WorkSpaces]를 선택합니다.

4. 디렉터리 선택 페이지에서 생성한 디렉터리를 선택하고 다음 단계를 선택합니다. WorkSpaces가 디렉터리를 등록합니다.

5. [Identify Users] 페이지에서 다음과 같이 디렉터리에 새 사용자를 추가합니다.

   a. [Username], [First Name], [Last Name] 및 [Email]을 완성합니다. 액세스할 수 있는 이메일 주소를 사용하십시오.

   b. [Create Users]를 선택합니다.

   c. 다음 단계(Next Step)를 선택합니다.

6. [Select Bundle] 페이지에서 번들을 선택하고 [Next Step]을 선택합니다.

> **Note**
>
> 각 번들의 권장 용도와 사양을 검토하여 사용자에게 가장 적합한 번들을 선택하세요. 자세한 내용은 Amazon WorkSpaces 번들 섹션을 참조하세요. 번들 사양, 권장 용도 및 요금에 대한 자세한 내용은 Amazon WorkSpaces 요금을 참조하세요.

7. [WorkSpaces Configuration] 페이지에서 실행 모드를 선택하고 [Next Step]을 선택합니다.
8. [Review & Launch WorkSpaces] 페이지에서 [Launch WorkSpaces]를 선택합니다. WorkSpaces의 초기 상태는 `PENDING`입니다. 시작이 완료되면 상태가 `AVAILABLE`로 변경되고 각 사용자에 대해 지정한 이메일 주소로 초대가 발송됩니다.

> **Note**
>
> 사용자가 이미 Active Directory에 있는 경우에는 초대 이메일이 전송되지 않습니다. 대신 사용자에게 수동으로 초대 이메일을 보내세요. 자세한 내용은 초대 이메일 전송 섹션을 참조하세요.

9. (선택 사항) Amazon WorkDocs를 지원하는 리전에서는 디렉터리의 모든 사용자에 대해 Amazon WorkDocs를 활성화할 수 있습니다. 자세한 내용은 AWS Managed Microsoft AD에 Amazon WorkDocs 활성화 섹션을 참조하세요. 자세한 내용은 Amazon WorkDocs 관리 안내서의 Amazon WorkDocs Drive를 참조하세요.

3단계: WorkSpaces에 연결

초대 이메일을 수신한 후 원하는 클라이언트를 사용하여 WorkSpaces에 연결할 수 있습니다. 로그인하면 클라이언트에 WorkSpaces 데스크톱이 표시됩니다.

WorkSpaces에 연결하려면

1. 초대 이메일에서 링크를 엽니다. 메시지가 표시되면 암호를 지정하고 사용자를 활성화합니다. WorkSpaces에 로그인할 때 필요하므로 이 암호를 기억하십시오.

> **Note**
>
> 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 암호는 소문자(a~z), 대문자(A~Z), 숫자(0~9) 및 ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.를 최소 1자씩 포함해야 합니다.

2. 각 클라이언트의 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients를 검토한 후 다음 중 하나를 수행하세요.

   - 메시지가 표시되면 클라이언트 애플리케이션 중 하나를 다운로드하거나 웹 액세스를 시작합니다.
   - 메시지가 표시되지 않고 클라이언트 애플리케이션을 아직 설치하지 않은 경우 https://clients.amazonworkspaces.com/ 을 열고 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작하세요.

   > **Note**
   >
   > 웹 브라우저(Web Access)로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

3. 클라이언트를 시작하고 초대 이메일의 등록 코드를 입력한 다음 [Register]를 선택합니다.
4. 로그인하라는 메시지가 표시되면 사용자의 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.
5. (선택 사항) 자격 증명을 저장하라는 메시지가 표시되면 [Yes]를 선택합니다.

다음 단계

계속해서 방금 생성한 WorkSpaces를 사용자 정의할 수 있습니다. 예를 들어 소프트웨어를 설치한 다음 WorkSpaces에서 사용자 지정 번들을 생성할 수 있습니다. 또한 WorkSpaces 및 WorkSpaces 디렉터리에 대해 다양한 관리 작업을 수행할 수 있습니다. 사용을 마친 WorkSpaces를 삭제할 수 있습니다. 자세한 내용은 다음 문서 섹션을 참조하세요.

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 관리하십시오 WorkSpaces
- WorkSpaces 디렉터리 관리
- WorkSpace 삭제

다중 모니터 설정 또는 주변 디바이스 사용과 같은 WorkSpaces 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

Simple AD를 사용하여 WorkSpaces 시작

WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Microsoft Windows 및 Linux 데스크톱을 프로비저닝할 수 있습니다.

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 디렉터리는 Simple AD, AD Connector, 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service 중에서 선택할 수 있습니다. 또한 AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 설정할 수 있습니다.

이 자습서에서는 Simple AD를 사용하는 WorkSpaces를 시작합니다. 다른 옵션을 사용하는 자습서는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

작업

- 시작하기 전에
- 1단계: Simple AD 디렉터리 생성
- 2단계: WorkSpaces 생성
- 3단계: WorkSpaces에 연결
- 다음 단계

시작하기 전에

- 일부 리전에서는 Simple AD를 사용할 수 없습니다. 지원되는 리전을 확인한 후 Simple AD 디렉터리용 리전을 선택합니다. Simple AD가 지원되는 리전에 대한 자세한 내용은 AWS Directory Service의 리전 가용성을 참조하세요.
- 일부 리전에서는 WorkSpaces를 사용할 수 없습니다. 지원되는 리전을 확인한 후 WorkSpaces용 리전을 선택합니다. 지원되는 리전에 대한 자세한 내용은 AWS 리전별 WorkSpaces 요금을 참조하세요.
- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 번들은 운영 체제, 스토리지, 컴퓨팅 및 소프트웨어 리소스의 조합입니다. 자세한 내용은 Amazon WorkSpaces 번들 단원을 참조하십시오.
- AWS Directory Service을(를) 사용하여 디렉터리를 생성하거나 WorkSpace를 시작할 때 퍼블릭 서브넷 1개와 프라이빗 서브넷 2개를 포함하여 구성된 가상 사설 클라우드를 생성하거나 선택해야 합니다. 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요.

1단계: Simple AD 디렉터리 생성

Simple AD 디렉터리를 생성합니다. AWS Directory Service이(가) VPC의 각 프라이빗 서브넷에 하나씩 두 개의 디렉터리 서버를 생성합니다. 처음에는 디렉터리에 사용자가 없습니다. 다음 단계에서 WorkSpaces를 생성할 때 사용자를 추가합니다.

> **Note**
>
> Simple AD는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
>
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

Simple AD 디렉터리를 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리 설정, Simple AD, 다음을 선택합니다.
4. 다음과 같이 디렉터리를 구성합니다.
   a. 조직 이름에 디렉터리의 고유한 조직 이름(예: my-example-directory)을 입력합니다. 이 이름은 길이가 4자 이상이고, 영숫자 및 하이픈(-)만으로 구성되고, 하이픈 이외의 문자로 시작하거나 끝나야 합니다.
   b. 디렉터리 DNS 이름에 디렉터리의 정규화된 이름(예: example.com)을 입력합니다.

      > **Important**
      >
      > WorkSpaces를 시작한 후 DNS 서버를 업데이트해야 하는 경우, Amazon WorkSpaces에 사용되는 DNS 서버 업데이트의 절차에 따라 WorkSpaces가 제대로 업데이트되도록 하세요.

   c. NetBIOS 이름에 디렉터리의 짧은 이름(예: example)을 입력합니다.

d. 관리자 암호 및 암호 확인에 디렉터리 관리자 계정의 암호를 입력합니다. 암호 요구 사항에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 How to Create a Microsoft AD Directory를 참조하세요.

e. (선택 사항) 설명에 디렉터리에 대한 설명을 입력합니다.

f. 디렉터리 크기에서 스몰을 선택합니다.

g. [VPC]에서 앞서 생성한 VPC를 선택합니다.

h. [Subnets]에서 2개의 프라이빗 서브넷(CIDR 블록 `10.0.1.0/24` 및 `10.0.2.0/24`를 포함)을 선택합니다.

i. 다음(Next)을 선택합니다.

5. 디렉터리 생성을 선택합니다.
6. 디렉터리의 초기 상태는 `Requested`이며 그런 다음 `Creating`으로 변경됩니다. 디렉터리 생성이 완료되면(몇 분 정도 걸릴 수 있음) 상태는 `Active`입니다.

디렉터리 생성 중 발생하는 사항

WorkSpaces가 사용자를 대신하여 다음 작업을 완료합니다.

- WorkSpaces 서비스에서 탄력적 네트워크 인터페이스를 생성하고 WorkSpaces 디렉터리를 나열하도록 허용하는 IAM 역할을 생성합니다. 이 역할의 이름은 `workspaces_DefaultRole`입니다.
- VPC 내에서 사용자 및 WorkSpaces 정보를 저장하는 데 사용되는 Simple AD를 설정합니다. 디렉터리는 사용자 이름 Administrator와 지정된 암호를 사용하는 관리자 계정을 포함합니다.
- 디렉터리 컨트롤러와 디렉터리 내 WorkSpaces에 대해 각각 하나씩 두 보안 그룹을 생성합니다.

2단계: WorkSpaces 생성

이제 WorkSpaces를 시작할 준비가 되었습니다.

사용자에 대한 WorkSpaces를 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. [Launch WorkSpaces]를 선택합니다.
4. [Select a Directory] 페이지에서 다음을 수행합니다.

   a. [Directory]에서 생성한 디렉터리를 선택합니다.

b. 셀프 서비스 권한 활성화에서 예 또는 아니요를 선택하고 설명을 입력합니다.

c. [Enable Amazon WorkDocs]에서 [Yes]를 선택합니다.

> **Note**
>
> 이 옵션은 선택한 리전에서 Amazon WorkDocs를 사용할 수 있는 경우에만 표시됩니다.

d. 다음 단계(Next Step)를 선택합니다. WorkSpaces가 Simple AD 디렉터리를 등록합니다.

5. [Identify Users] 페이지에서 다음과 같이 디렉터리에 새 사용자를 추가합니다.

a. [Username], [First Name], [Last Name] 및 [Email]을 완성합니다. 액세스할 수 있는 이메일 주소를 사용하십시오.

b. [Create Users]를 선택합니다.

c. 다음 단계(Next Step)를 선택합니다.

6. [Select Bundle] 페이지에서 번들을 선택하고 [Next Step]을 선택합니다.

> **Note**
>
> 각 번들의 권장 용도와 사양을 검토하여 사용자에게 가장 적합한 번들을 선택하세요. 자세한 내용은 Amazon WorkSpaces 번들 섹션을 참조하세요. 번들 사양, 권장 용도 및 요금에 대한 자세한 내용은 Amazon WorkSpaces 요금을 참조하세요.

7. [WorkSpaces Configuration] 페이지에서 실행 모드를 선택하고 [Next Step]을 선택합니다.

8. [Review & Launch WorkSpaces] 페이지에서 [Launch WorkSpaces]를 선택합니다. WorkSpaces의 초기 상태는 `PENDING`입니다. 시작이 완료되면(최대 20분 정도 걸릴 수 있음) 상태가 `AVAILABLE`로 변경되고 각 사용자에 대해 지정한 이메일 주소로 초대가 발송됩니다.

> **Note**
>
> 사용자가 이미 Active Directory에 있는 경우에는 초대 이메일이 전송되지 않습니다. 대신 사용자에게 수동으로 초대 이메일을 보내세요. 자세한 내용은 초대 이메일 전송 섹션을 참조하세요.

3단계: WorkSpaces에 연결

초대 이메일을 수신한 후 원하는 클라이언트를 사용하여 WorkSpaces에 연결할 수 있습니다. 로그인하면 클라이언트에 WorkSpaces 데스크톱이 표시됩니다.

WorkSpaces에 연결하려면

1. 초대 이메일에서 링크를 엽니다. 메시지가 표시되면 암호를 입력하고 사용자를 활성화합니다. WorkSpaces에 로그인할 때 필요하므로 이 암호를 기억하십시오.

   > **Note**
   >
   > 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 암호는 소문자(a~z), 대문자(A~Z), 숫자(0~9) 및 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.를 최소 1자씩 포함해야 합니다.

2. 각 클라이언트의 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients를 검토한 후 다음 중 하나를 수행하세요.

   - 메시지가 표시되면 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작합니다.
   - 메시지가 표시되지 않고 클라이언트 애플리케이션을 아직 설치하지 않은 경우 https://clients.amazonworkspaces.com/ 을 열고 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작하세요.

   > **Note**
   >
   > 웹 브라우저(Web Access)로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

3. 클라이언트를 시작하고 초대 이메일의 등록 코드를 입력한 다음 [Register]를 선택합니다.
4. 로그인하라는 메시지가 표시되면 사용자의 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.
5. (선택 사항) 자격 증명을 저장하라는 메시지가 표시되면 [Yes]를 선택합니다.

다음 단계

계속해서 방금 생성한 WorkSpaces를 사용자 정의할 수 있습니다. 예를 들어 소프트웨어를 설치한 다음 WorkSpaces에서 사용자 지정 번들을 생성할 수 있습니다. 또한 WorkSpaces 및 WorkSpaces 디렉

터리에 대해 다양한 관리 작업을 수행할 수 있습니다. 사용을 마친 WorkSpaces를 삭제할 수 있습니다. 자세한 내용은 다음 문서 섹션을 참조하세요.

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 관리하십시오 WorkSpaces
- WorkSpaces 디렉터리 관리
- WorkSpace 삭제

다중 모니터 설정 또는 주변 디바이스 사용과 같은 WorkSpaces 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

AD Connector를 사용하여 WorkSpaces 시작

WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Microsoft Windows 및 Linux 데스크톱을 프로비저닝할 수 있습니다.

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 디렉터리는 Simple AD, AD Connector, 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service 중에서 선택할 수 있습니다. 또한 AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 설정할 수 있습니다.

이 자습서에서는 AD Connector를 사용하는 WorkSpaces를 시작합니다. 다른 옵션을 사용하는 자습서는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

작업

- 시작하기 전에
- 1단계: AD Connector 생성
- 2단계: WorkSpaces 생성
- 3단계: WorkSpaces에 연결
- 다음 단계

시작하기 전에

- 일부 리전에서는 WorkSpaces를 사용할 수 없습니다. 지원되는 리전을 확인한 후 WorkSpaces용 리전을 선택합니다. 지원되는 리전에 대한 자세한 내용은 AWS 리전별 WorkSpaces 요금을 참조하세요.
- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 번들은 운영 체제, 스토리지, 컴퓨팅 및 소프트웨어 리소스의 조합입니다. 자세한 내용은 Amazon WorkSpaces 번들 단원을 참조하십시오.
- 프라이빗 서브넷을 2개 이상 포함하는 가상 사설 클라우드를 생성합니다. 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요. VPC는 반드시 가상 프라이빗 네트워크(VPN) 연결이나 AWS Direct Connect을(를) 통해 온프레미스 네트워크에 연결되어야 합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 AD Connector 사전 조건을 참조하세요.
- WorkSpace에서 인터넷 액세스를 제공합니다. 자세한 내용은 귀하의 인터넷 액세스 제공 WorkSpace 섹션을 참조하세요.

1단계: AD Connector 생성

> **Note**
>
> AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

AD Connector를 생성하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. [Set up Directory], [Create AD Connector]를 선택합니다.
4. 조직 이름에 디렉터리의 고유한 조직 이름(예: my-example-directory)을 입력합니다. 이 이름은 길이가 4자 이상이고, 영숫자 및 하이픈(-)만으로 구성되고, 하이픈 이외의 문자로 시작하거나 끝나야 합니다.

5. 연결된 디렉터리 DNS에 온프레미스 디렉터리의 정규화된 이름(예: example.com)을 입력합니다.
6. 연결된 디렉터리 NetBIOS 이름에 온프레미스 디렉터리의 짧은 이름(예: example)을 입력합니다.
7. 커넥터 계정 사용자 이름에 온프레미스 디렉터리 내 사용자의 사용자 이름을 입력합니다. 이 사용자는 사용자 및 그룹을 읽고, 컴퓨터 객체를 생성하고, 컴퓨터를 도메인에 조인할 수 있는 권한이 있어야 합니다.
8. 커넥터 계정 암호 및 암호 확인에 온프레미스 사용자의 암호를 입력합니다.
9. DNS 주소에 온프레미스 디렉터리에 포함된 DNS 서버의 IP 주소를 한 개 이상 입력합니다.

> **Important**
>
> WorkSpaces를 시작한 후 DNS 서버 IP 주소를 업데이트해야 하는 경우, Amazon WorkSpaces에 사용되는 DNS 서버 업데이트의 절차에 따라 WorkSpaces가 제대로 업데이트되도록 하세요.

10. (선택 사항) 설명에 디렉터리에 대한 설명을 입력합니다.
11. [Size]를 [Small]로 유지합니다.
12. VPC에서 해당 VPC를 선택합니다.
13. [Subnets]에서 해당 서브넷을 선택합니다. 지정한 DNS 서버는 각 서브넷에서 액세스할 수 있어야 합니다.
14. 다음 단계(Next Step)를 선택합니다.
15. [Create AD Connector]를 선택합니다. 디렉터리를 연결하는 데 몇 분 정도 걸립니다. 디렉터리의 초기 상태는 `Requested`이며 그런 다음 `Creating`으로 변경됩니다. 디렉터리 생성 과정이 완료되면 상태가 `Active`로 변경됩니다.

2단계: WorkSpaces 생성

이제 온프레미스 디렉터리에서 한 명 이상의 사용자에 대해 WorkSpaces를 시작할 준비가 되었습니다.

기존 사용자에 대한 WorkSpaces를 시작하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. [Launch WorkSpaces]를 선택합니다.
4. [Directory]에서 생성한 디렉터리를 선택합니다.

5. (선택 사항) 이 디렉터리에서 WorkSpace를 처음으로 시작하고 리전에서 Amazon WorkDocs를 지원하는 경우 디렉터리 내의 모든 사용자에 대해 Amazon WorkDocs를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 Amazon WorkDocs 관리 안내서의 Amazon WorkDocs Drive를 참조하세요.
6. 다음(Next)을 선택합니다. WorkSpaces가 AD 커넥터를 등록합니다.
7. 온프레미스 디렉터리에서 하나 이상의 기존 사용자를 선택합니다. WorkSpaces 콘솔을 통해 새 사용자를 온프레미스 디렉터리에 추가하지 마세요.

   선택할 사용자를 찾으려면 사용자의 이름을 전부 또는 일부만 입력하고 검색을 선택하거나 Show All Users(모든 사용자 표시)를 선택하면 됩니다. 이메일 주소가 없는 사용자는 선택할 수 없습니다.

   사용자를 선택한 후 [Add Selected]를 선택하고 [Next Step]을 선택합니다.
8. [Select Bundle] 아래에서 WorkSpaces에 사용할 기본 WorkSpaces 번들을 선택합니다. 필요한 경우 [Assign WorkSpace Bundles] 아래에서 개별 WorkSpaces마다 다른 번들을 선택할 수 있습니다. 마쳤으면 [Next Step]을 선택합니다.

   > **Note**
   >
   > 각 번들의 권장 용도와 사양을 검토하여 사용자에게 가장 적합한 번들을 선택하세요. 자세한 내용은 Amazon WorkSpaces 번들 섹션을 참조하세요. 번들 사양, 권장 용도 및 요금에 대한 자세한 내용은 Amazon WorkSpaces 요금을 참조하세요.
9. WorkSpaces 실행 모드를 선택하고 [Next Step]을 선택합니다. 자세한 내용은 WorkSpace 실행 모드 관리 섹션을 참조하세요.
10. [Launch WorkSpaces]를 선택합니다. WorkSpaces의 초기 상태는 `PENDING`입니다. 시작이 완료되면 상태가 `AVAILABLE`로 변경됩니다.
11. 각 사용자의 이메일 주소로 초대를 발송합니다. (AD Connector를 사용하는 경우에는 이러한 초대가 자동으로 전송되지 않습니다.) 자세한 내용은 초대 이메일 전송 섹션을 참조하세요.

3단계: WorkSpaces에 연결

원하는 클라이언트를 사용하여 WorkSpaces에 연결할 수 있습니다. 로그인하면 클라이언트에 WorkSpaces 데스크톱이 표시됩니다.

WorkSpaces에 연결하려면

1. 초대 이메일에서 링크를 엽니다.
2. 각 클라이언트의 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients를 검토한 후 다음 중 하나를 수행하세요.
   - 메시지가 표시되면 클라이언트 애플리케이션 중 하나를 다운로드하거나 웹 액세스를 시작합니다.
   - 메시지가 표시되지 않고 클라이언트 애플리케이션을 아직 설치하지 않은 경우 https://clients.amazonworkspaces.com/ 을 열고 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작하세요.

   > **Note**
   >
   > 웹 브라우저(Web Access)로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

3. 클라이언트를 시작하고 초대 이메일의 등록 코드를 입력한 다음 [Register]를 선택합니다.
4. 로그인하라는 메시지가 표시되면 사용자의 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.
5. (선택 사항) 자격 증명을 저장하라는 메시지가 표시되면 [Yes]를 선택합니다.

> **Note**
>
> AD Connector를 사용하기 때문에 사용자가 자신의 암호를 재설정할 수 없습니다. (WorkSpaces 클라이언트 애플리케이션 로그인 화면에서 암호 찾기 옵션을 사용할 수 없습니다.) 사용자 암호를 재설정하는 방법에 대한 자세한 내용은 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

다음 단계

계속해서 방금 생성한 WorkSpaces를 사용자 정의할 수 있습니다. 예를 들어 소프트웨어를 설치한 다음 WorkSpaces에서 사용자 지정 번들을 생성할 수 있습니다. 또한 WorkSpaces 및 WorkSpaces 디렉터리에 대해 다양한 관리 작업을 수행할 수 있습니다. 사용을 마친 WorkSpaces를 삭제할 수 있습니다. 자세한 내용은 다음 문서 섹션을 참조하세요.

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 관리하십시오 WorkSpaces
- WorkSpaces 디렉터리 관리
- WorkSpace 삭제

다중 모니터 설정 또는 주변 디바이스 사용과 같은 WorkSpaces 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

신뢰할 수 있는 도메인을 사용하여 WorkSpace 시작

WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Microsoft Windows, Amazon Linux 또는 Ubuntu Linux 데스크톱을 프로비저닝할 수 있습니다.

WorkSpaces에서는 디렉터리를 사용하여 WorkSpaces 및 사용자의 정보를 저장하고 관리합니다. 디렉터리는 Simple AD, AD Connector, 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory Service 중에서 선택할 수 있습니다. 또한 AWS Managed Microsoft AD 디렉터리와 온프레미스 도메인 간에 신뢰 관계를 설정할 수 있습니다.

이 자습서에서는 신뢰 관계를 사용하는 WorkSpaces를 시작합니다. 다른 옵션을 사용하는 자습서는 WorkSpaces를 사용하여 가상 데스크톱 시작 단원을 참조하십시오.

작업

- 시작하기 전에
- 1단계: 신뢰 관계 설정
- 2단계: WorkSpaces 생성
- 3단계: WorkSpaces에 연결
- 다음 단계

시작하기 전에

- 별도의 신뢰할 수 있는 도메인에서 AWS 계정을 사용하여 WorkSpaces를 시작하는 것은 온프레미스 디렉터리에 대한 신뢰 관계로 구성된 AWS Managed Microsoft AD와 호환됩니다. 하지만 Simple AD 또는 AD Connector를 사용하는 WorkSpaces는 신뢰할 수 있는 도메인의 사용자를 위해 WorkSpaces를 시작할 수 없습니다.

- 일부 리전에서는 WorkSpaces를 사용할 수 없습니다. 지원되는 리전을 확인한 후 WorkSpaces용 리전을 선택합니다. 지원되는 리전에 대한 자세한 내용은 AWS 리전별 WorkSpaces 요금을 참조하세요.
- WorkSpaces를 시작할 때 WorkSpaces 번들을 선택해야 합니다. 번들은 스토리지, 컴퓨팅 및 소프트웨어 리소스의 조합입니다. 자세한 내용은 Amazon WorkSpaces 번들 단원을 참조하십시오.
- AWS Directory Service을(를) 사용하여 디렉터리를 생성하거나 WorkSpace를 시작할 때 퍼블릭 서브넷 1개와 프라이빗 서브넷 2개를 포함하여 구성된 가상 사설 클라우드를 생성하거나 선택해야 합니다. 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요.

1단계: 신뢰 관계 설정

신뢰 관계를 설정하려면

1. 가상 사설 클라우드(VPC)에서 AWS Managed Microsoft AD를 설정합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD 디렉터리 생성을 참조하세요.

   > **Note**
   >
   > - 공유 디렉터리는 현재 WorkSpaces에서 사용이 지원되지 않습니다.
   > - 다중 리전 복제를 위해 AWS Managed Microsoft AD 디렉터리가 구성된 경우 기본 리전의 디렉터리만 Amazon WorkSpaces에서 사용하도록 등록할 수 있습니다. Amazon WorkSpaces에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. AWS Managed Microsoft AD를 사용한 다중 리전 복제는 복제된 리전 내의 Amazon WorkSpaces에서 사용할 수 없습니다.

2. AWS Managed Microsoft AD와 온프레미스 도메인 간에 신뢰 관계를 생성합니다. 양방향 신뢰로 구성되었는지 확인합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Tutorial: Create a Trust Relationship Between Your AWS Managed Microsoft AD and Your On-Premises Domain을 참조하세요.

WorkSpaces를 통한 관리 및 인증에 단방향 또는 양방향 신뢰를 사용하여 온프레미스 사용자와 그룹에 WorkSpaces를 프로비저닝할 수 있습니다. 자세한 내용은 디렉터리 Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain with AWS Directory Service를 참조하세요.

> **Note**
>
> Ubuntu WorkSpaces는 Active Directory 통합을 위해 System Security Services Daemon(SSSD)을 사용하며 SSSD는 포리스트 트러스트를 지원하지 않습니다. 대신 외부 신뢰를 구성하세요. Amazon Linux 및 Ubuntu WorkSpaces의 경우 양방향 트러스트를 사용하는 것이 좋습니다.

2단계: WorkSpaces 생성

AWS Managed Microsoft AD와 온프레미스 Microsoft Active Directory 도메인 간에 신뢰 관계를 설정한 다음 온프레미스 도메인의 사용자에게 WorkSpaces를 프로비저닝할 수 있습니다.

GPO 설정을 WorkSpaces에 적용하기 이전에 도메인에 GPO 설정이 복제되는지 확인해야 합니다.

신뢰할 수 있는 온프레미스 도메인의 사용자에 대해 WorkSpaces를 시작하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. [Launch WorkSpaces]를 선택합니다.
4. [Select a Directory] 페이지에서 방금 등록한 디렉터리를 선택하고 [Next Step]을 선택합니다.
5. [Identify Users] 페이지에서 다음을 수행합니다.
   a. [Select trust from forest]에서 앞서 생성한 신뢰 관계를 선택합니다.
   b. 온프레미스 도메인에서 사용자를 선택하고 [Add Selected]를 선택합니다.
   c. 다음 단계(Next Step)를 선택합니다.
6. WorkSpaces에 사용할 번들을 선택하고 [Next Step]을 선택합니다.

   > **Note**
   >
   > 각 번들의 권장 용도와 사양을 검토하여 사용자에게 가장 적합한 번들을 선택하세요. 자세한 내용은 Amazon WorkSpaces 번들 섹션을 참조하세요. 번들 사양, 권장 용도 및 요금에 대한 자세한 내용은 Amazon WorkSpaces 요금을 참조하세요.
7. 실행 모드를 선택하고 암호화 설정을 선택한 다음 태그를 구성합니다. 마쳤으면 [Next Step]을 선택합니다.

8. [Launch WorkSpaces]를 선택합니다. WorkSpaces를 사용하려면 최대 20분 정도 걸릴 수 있으며, 암호화를 활성화한 경우에는 최대 40분 정도 걸릴 수 있습니다. WorkSpaces의 초기 상태는 PENDING입니다. 시작이 완료되면 상태가 AVAILABLE로 변경됩니다.
9. 각 사용자의 이메일 주소로 초대를 발송합니다. (신뢰 관계를 사용하는 경우에는 이러한 초대가 자동으로 전송되지 않습니다.) 자세한 내용은 초대 이메일 전송 섹션을 참조하세요.

3단계: WorkSpaces에 연결

초대 이메일을 수신한 후 WorkSpaces에 연결할 수 있습니다. 사용자는 사용자 이름을 입력할 수 있습니다(예: username, corp\username 또는 corp.example.com\username).

WorkSpaces에 연결하려면

1. 초대 이메일에서 링크를 엽니다. 메시지가 표시되면 암호를 입력하고 사용자를 활성화합니다. WorkSpaces에 로그인할 때 필요하므로 이 암호를 기억하십시오.

> **Note**
>
> 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다. 암호는 소문자(a~z), 대문자(A~Z), 숫자(0~9) 및 ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.를 최소 1자씩 포함해야 합니다.

2. 각 클라이언트의 요구 사항에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients를 검토한 후 다음 중 하나를 수행하세요.
   - 메시지가 표시되면 클라이언트 애플리케이션 중 하나를 다운로드하거나 웹 액세스를 시작합니다.
   - 메시지가 표시되지 않고 클라이언트 애플리케이션을 아직 설치하지 않은 경우 https://clients.amazonworkspaces.com/ 을 열고 클라이언트 애플리케이션 중 하나를 다운로드하거나 Web Access를 시작하세요.

> **Note**
>
> 웹 브라우저(Web Access)로는 Amazon Linux WorkSpaces에 연결할 수 없습니다.

3. 클라이언트를 시작하고 초대 이메일의 등록 코드를 입력한 다음 [Register]를 선택합니다.
4. 로그인하라는 메시지가 표시되면 사용자의 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.

5. (선택 사항) 자격 증명을 저장하라는 메시지가 표시되면 [Yes]를 선택합니다.

다음 단계

계속해서 방금 생성한 WorkSpaces를 사용자 정의할 수 있습니다. 예를 들어 소프트웨어를 설치한 다음 WorkSpaces에서 사용자 지정 번들을 생성할 수 있습니다. 또한 WorkSpaces 및 WorkSpaces 디렉터리에 대해 다양한 관리 작업을 수행할 수 있습니다. 사용을 마친 WorkSpaces를 삭제할 수 있습니다. 자세한 내용은 다음 문서 섹션을 참조하세요.

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 관리하십시오 WorkSpaces
- WorkSpaces 디렉터리 관리
- WorkSpace 삭제

다중 모니터 설정 또는 주변 디바이스 사용과 같은 WorkSpaces 클라이언트 애플리케이션 사용에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces Clients 및 Peripheral Device Support를 참조하세요.

관리자 WorkSpace 사용자

각 WorkSpace는 단일 사용자에 할당되며 여러 사용자가 공유할 수 없습니다. 기본적으로 디렉터리별로 사용자당 하나의 WorkSpace만 허용됩니다.

목차

WorkSpaces 사용자 관리

WorkSpaces 관리자는 다음 작업을 수행하여 WorkSpaces 사용자를 관리할 수 있습니다.

사용자 정보 편집

WorkSpaces 콘솔을 사용하여 WorkSpace 사용자 정보를 편집할 수 있습니다.

> **Note**
>
> 이 기능은 AWS Managed Microsoft AD 또는 Simple AD를 사용하는 경우에만 제공됩니다. AD Connector 또는 신뢰 관계를 통해 Microsoft Active Directory를 사용하는 경우 Active Directory 모듈을 사용하여 사용자 및 그룹을 관리할 수 있습니다.

사용자 정보를 편집하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. 사용자를 선택하고 작업, 사용자 편집을 선택합니다.
4. 필요에 따라 이름, 성 및 이메일을 업데이트합니다.
5. 업데이트를 선택합니다.

사용자 추가 또는 삭제

WorkSpace를 시작하는 프로세스 동안에만 Amazon WorkSpaces 콘솔에서 사용자를 생성할 수 있으며, Amazon WorkSpaces 콘솔을 통해 사용자를 삭제할 수는 없습니다. 사용자 그룹 관리를 포함한 대부분의 사용자 관리 작업은 디렉터리를 통해 수행해야 합니다.

사용자 및 그룹을 추가하거나 삭제하려면

사용자 및 그룹을 추가하거나 삭제 또는 관리하려면 디렉터리를 통해 이를 수행해야 합니다. WorkSpaces 디렉터리 관리 작업은 대부분 Active Directory 관리 도구와 같은 디렉터리 관리 도구를 사용하여 수행합니다. 자세한 내용은 WorkSpaces용 Active Directory 관리 도구 설정 섹션을 참조하세요.

> **Important**
>
> 사용자를 제거하려면 먼저 해당 사용자에 할당된 WorkSpaces를 삭제해야 합니다. 자세한 내용은 WorkSpace 삭제 섹션을 참조하세요.

사용자 및 그룹을 관리하는 데 사용하는 프로세스는 사용 중인 디렉터리 유형에 따라 다릅니다.

- AWS Managed Microsoft AD를 사용하는 경우 AWS Directory Service 관리 안내서의 Manage Users and Groups in AWS Managed Microsoft AD를 참조하세요.
- Simple AD를 사용하는 경우 AWS Directory Service 관리 안내서의 Simple AD에서 사용자 및 그룹 관리를 참조하세요.
- AD Connector 또는 신뢰 관계를 통해 Microsoft Active Directory를 사용하는 경우 Active Directory 모듈을 사용하여 사용자 및 그룹을 관리할 수 있습니다.

초대 이메일 전송

필요할 경우 수동으로 사용자에게 초대 이메일을 발송할 수 있습니다.

> **Note**
>
> AD Connector 또는 신뢰할 수 있는 도메인을 사용하는 경우 초대 이메일이 사용자에게 자동으로 전송되지 않으므로 수동으로 보내야 합니다. 사용자가 이미 Active Directory에 있는 경우에도 초대 이메일이 자동으로 전송되지 않습니다.

초대 이메일을 재발송하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. WorkSpaces 페이지에서 검색 상자를 사용하여 초대를 보낼 사용자를 검색하고 검색 결과에서 해당 WorkSpace를 선택합니다. 한 번에 하나의 WorkSpace만 선택할 수 있습니다.
4. 작업, 사용자 초대를 선택합니다.
5. WorkSpace에 사용자 초대 페이지에서 초대 보내기를 선택합니다.

한 사용자에 대해 여러 WorkSpaces 만들기

기본적으로 디렉터리별로 사용자당 하나의 WorkSpace만 만들 수 있습니다. 그러나 필요한 경우 디렉터리 설정에 따라 한 사용자에 대해 둘 이상의 WorkSpace를 만들 수 있습니다.

- WorkSpaces용 디렉터리가 하나뿐인 경우 해당 사용자에 대해 여러 사용자 이름을 만듭니다. 예를 들어, Mary Major라는 사용자가 mmajor1, mmajor2 등을 사용자 이름으로 사용할 수 있습니다. 각 사용자 이름은 동일한 디렉터리의 다른 WorkSpace와 연결되지만 WorkSpaces가 모두 동일한 AWS 리전의 동일한 디렉터리에 생성되는 한 WorkSpaces의 등록 코드는 동일합니다.
- WorkSpaces용 디렉터리가 여러 개 있는 경우 사용자의 WorkSpaces를 별도의 디렉터리에 만듭니다. 디렉터리에서 동일한 사용자 이름을 사용하거나 디렉터리에서 다른 사용자 이름을 사용할 수 있습니다. WorkSpaces 등록 코드는 서로 다릅니다.

> **Tip**
>
> 사용자를 위해 생성한 모든 WorkSpaces를 쉽게 찾을 수 있도록 각 WorkSpace에 동일한 기본 사용자 이름을 사용하세요.
> 예를 들어 Active Directory 사용자 이름이 mmajor인 Mary Major라는 사용자가 있는 경우 mmajor, mmajor1, mmajor2, mmajor3와 같은 사용자 이름이나 mmajor_windows 또는 mmajor_linux와 같은 기타 변형을 사용하여 해당 사용자를 위한 WorkSpaces를 생성하세요. 모든 WorkSpaces가 동일한 기본 사용자 이름(mmajor)으로 시작하는 경우 WorkSpaces 콘솔에서 사용자 이름을 기준으로 정렬하여 해당 사용자의 모든 WorkSpaces를 그룹화할 수 있습니다.

> **Important**
>
> - 사용자는 PCoIP WorkSpace와 WSP WorkSpace를 모두 가질 수 있습니다. 단, 두 개의 WorkSpaces가 별도의 디렉터리에 있어야 합니다. 동일한 사용자는 동일한 디렉터리에 PCoIP WorkSpace와 WSP WorkSpace를 둘 수 없습니다.
> - 리전 간 리디렉션에 사용할 여러 WorkSpaces를 설정하는 경우 여러 AWS 리전의 서로 다른 디렉터리에 WorkSpaces를 설정하고 각 디렉터리에서 동일한 사용자 이름을 사용해야 합니다. 리전 간 리디렉션에 대한 자세한 내용은 Amazon을 위한 지역 간 리디렉션 WorkSpaces 섹션을 참조하세요.

WorkSpaces 간에 전환하기 위해 사용자는 특정 Workspace와 연결된 사용자 이름 및 등록 코드를 사용하여 로그인합니다. 사용자가 Windows, macOS 또는 Linux용 WorkSpaces 클라이언트 애플리케이션의 3.0+ 버전을 사용하는 경우 클라이언트 애플리케이션의 설정, 로그인 정보 관리로 이동하여 WorkSpaces에 다른 이름을 할당할 수 있습니다.

사용자가 로그인하는 방법을 사용자 지정합니다. WorkSpaces

유니폼 리소스 식별자 (URI) 를 사용하여 사용자 액세스를 WorkSpaces 사용자 지정하면 조직의 기존 워크플로와 통합되는 간소화된 로그인 환경을 제공할 수 있습니다. 예를 들어 등록 코드를 사용하여 사용자를 등록하는 로그인 URI를 자동으로 생성할 수 있습니다. WorkSpaces 결과:

- 사용자는 수동 등록 프로세스를 무시할 수 있습니다.
- 사용자 이름은 WorkSpaces 클라이언트 로그인 페이지에 자동으로 입력됩니다.
- 조직에서 다중 인증(MFA)이 사용되는 경우에는 클라이언트 로그인 페이지에 사용자 이름과 MFA 코드가 자동으로 입력됩니다.

URI 액세스는 리전 기반 등록 코드(예: `WSpdx+ABC12D`)와 정규화된 도메인 이름(FQDN) 기반 등록 코드(예: `desktop.example.com`) 모두에서 작동합니다. FQDN 기반 등록 코드 생성 및 사용에 대한 자세한 내용은 Amazon을 위한 지역 간 리디렉션 WorkSpaces 섹션을 참조하세요.

지원되는 다음 기기에서 클라이언트 애플리케이션에 WorkSpaces 대한 URI 액세스를 구성할 수 있습니다.

- Windows 컴퓨터
- macOS 컴퓨터

- 우분투 리눅스 18.04, 20.04, 22.04컴퓨터
- iPad
- Android 디바이스

URI를 사용하여 URI에 액세스하려면 사용자는 먼저 WorkSpaces https://clients.amazonworkspaces.com/ https://s3 을 열어 장치용 클라이언트 애플리케이션을 설치해야 합니다. us-iso-eastworkspaces-client-updates-dcaus-isob-east

URI 액세스는 윈도우 및 macOS 컴퓨터의 파이어폭스 및 크롬 브라우저, 우분투 리눅스 18.04, 20.04, 22.04 컴퓨터의 파이어폭스 브라우저, 윈도우 컴퓨터의 인터넷 익스플로러 및 Microsoft Edge 브라우저에서 지원됩니다. WorkSpaces 클라이언트에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 WorkSpaces 클라이언트를 참조하십시오.

> **Note**
>
> Android 디바이스의 경우 URI 액세스는 Google Chrome 브라우저가 아닌 Firefox 브라우저에서만 작동합니다.

URI 액세스를 구성하려면 다음 표에 설명된 URI 형식 중 하나를 사용하십시오. WorkSpaces

> **Note**
>
> URI의 데이터 구성 요소에 다음에 나오는 예약된 문자가 하나라도 포함되어 있으면 모호함이 발생하지 않도록 데이터 구성 요소에서 퍼센트 인코딩을 사용하는 것이 좋습니다.
> `@ : / ? & =`
> 예를 들어 사용자 이름에 이 문자가 하나라도 포함되어 있으면 URI에서 해당 사용자 이름을 퍼센트 인코딩해야 합니다. 자세한 내용은 Uniform Resource Identifier (URI): Generic Syntax 단원을 참조하십시오.

지원되는 구문	설명
workspaces://	WorkSpaces 클라이언트 애플리케이션을 엽니다. (참고: Linux 클라이언트 애플리케이션에서는 현재 Workspaces://를 단독으로 사용하는 것이 지원되지 않습니다.)

지원되는 구문	설명
workspaces://@registrationcode	등록 코드를 사용하여 사용자를 WorkSpaces 등록합니다. 클라이언트 로그인 페이지도 표시합니다.
workspaces://username@registrationcode	등록 코드를 사용하여 사용자를 WorkSpaces 등록합니다. 또한 클라이언트 로그인 페이지의 사용자 이름 필드에 사용자 이름을 자동으로 입력합니다.
workspaces://username@registrationcode?MFACode=mfa	등록 코드를 사용하여 사용자를 WorkSpaces 등록합니다. 또한 사용자 이름 필드에 사용자 이름을 입력하고 클라이언트 로그인 페이지의 MFA 코드 필드에 Multi-Factor Authentication(MFA) 코드를 자동으로 입력합니다.
workspaces://@registrationcode?MFACode=mfa	등록 코드를 사용하여 사용자를 WorkSpaces 등록합니다. 또한 클라이언트 로그인 페이지의 MFA 코드 필드에 Multi-Factor Authentication(MFA) 코드를 자동으로 입력합니다.

> **Note**
>
> 사용자가 Windows 클라이언트에서 이미 연결된 상태에서 URI 링크를 열면 새 WorkSpaces 세션이 열리고 원래 WorkSpaces 세션은 열린 상태로 유지됩니다. WorkSpace 사용자가 macOS, iPad 또는 Android 클라이언트에서 URI 링크를 연결했을 때 URI 링크를 열면 새 세션이 열리지 않고 원래 WorkSpaces 세션만 열린 상태로 유지됩니다. WorkSpace

사용자를 위한 셀프 서비스 WorkSpace 관리 기능 활성화

WorkSpaces에서는 사용자가 자신의 경험을 더 잘 제어할 수 있도록 셀프 서비스 WorkSpace 관리 기능을 활성화할 수 있습니다. 또한 IT 지원 직원의 업무량도 줄일 수 있습니다. WorkSpaces 셀프 서비스 기능을 활성화하면 사용자가 WorkSpaces 클라이언트에서 직접 다음 작업 중 하나 이상을 수행할 수 있습니다.

- 클라이언트에서 자격 증명을 캐시합니다. 이렇게 하면 자격 증명을 다시 WorkSpace 입력하지 않고도 서버에 다시 연결할 수 있습니다.
- 다시 시작 (재부팅) 하십시오. WorkSpace
- 의 루트 및 사용자 볼륨 크기를 늘리십시오 WorkSpace.

- 해당 컴퓨팅 유형 (번들) 을 WorkSpace 변경하십시오.
- 그들의 실행 모드를 WorkSpace 전환하십시오.
- 다시 빌드하세요. WorkSpace

지원 클라이언트

- Android 또는 Android 호환 Chrome OS 시스템에서 실행되는 Android
- Linux
- macOS
- Windows

사용자를 위해 셀프 서비스 관리 기능을 활성화하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 여세요.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 셀프 서비스 관리 기능을 활성화하려는 디렉터리를 선택합니다.
4. 아래로 스크롤하여 셀프 서비스 권한으로 이동한 다음 편집을 선택합니다. 필요에 따라 다음 옵션을 활성화 또는 비활성화하여 사용자가 클라이언트에서 수행할 수 있는 WorkSpace 관리 작업을 결정합니다.

   - Remember me - 사용자가 로그인 화면에서 Remember me 또는 로그인 유지 확인란을 선택하여 클라이언트에 보안 인증 정보를 캐시할지 선택할 수 있습니다. 자격 증명은 RAM에만 캐시됩니다. 사용자가 자격 증명을 캐시하도록 선택하면 자격 증명을 다시 WorkSpaces 입력하지 않고도 자격 증명에 다시 연결할 수 있습니다. 사용자가 자격 증명을 캐시할 수 있는 기간을 제어하는 방법은 Kerberos 티켓에 최대 수명 설정 단원을 참조하십시오.
   - WorkSpace 클라이언트에서 재시작 - 사용자가 클라이언트를 재시작 (재부팅) 할 수 있습니다. WorkSpace 다시 시작하면 사용자와의 연결이 끊기고 WorkSpace, 종료되고, 재부팅됩니다. 사용자 데이터, 운영 체제 및 시스템 설정은 영향을 받지 않습니다.
   - 볼륨 크기 늘리기 - 사용자는 IT 지원 부서에 문의하지 않고도 루트 및 사용자 볼륨을 지정된 크기로 확장할 수 있습니다. WorkSpace 사용자는 루트 볼륨 (Windows의 경우 C: 드라이브, Linux의 경우,/) 의 크기를 최대 175GB까지 늘리고 사용자 볼륨 (Windows의 경우 D: 드라이브, Linux의 경우 /home) 의 크기를 최대 100GB까지 늘릴 수 있습니다. WorkSpace 루트 볼륨과 사용자 볼륨은 세트 그룹으로 구성되며 변경할 수 없습니다. 사용 가능한 그룹은 [루트(GB), 사용자(GB)]: [80, 10], [80, 50], [80, 100], [175 ~ 2000, 100~ 2000]입니다. 자세한 정보는 a 수정 WorkSpace을 참조하세요.

새로 만든 드라이브의 WorkSpace 경우 사용자는 6시간을 기다려야 드라이브 크기를 늘릴 수 있습니다. 이 시간 이후에는 6시간 기간 동안 한 번만 그렇게 할 수 있습니다. 볼륨 크기가 커지는 동안 사용자는 볼륨 크기 증가로 대부분의 작업을 수행할 수 WorkSpace 있습니다. 수행할 수 없는 작업은 WorkSpace 컴퓨팅 유형 변경, WorkSpace 실행 모드 전환, 재시작 또는 재구축입니다. WorkSpace WorkSpace 프로세스가 끝나면 를 다시 WorkSpace 부팅해야 변경 사항이 적용됩니다. 이 프로세스는 최대 한 시간이 걸릴 수 있습니다.

> **Note**
>
> 사용자가 볼륨 크기를 WorkSpace 늘리면 해당 볼륨의 청구 요금이 증가합니다. WorkSpace

- 컴퓨팅 유형 변경 - 사용자가 컴퓨팅 유형 (번들) WorkSpace 간에 전환할 수 있습니다. 새로 만든 번들의 WorkSpace 경우 사용자는 6시간을 기다려야 다른 번들로 전환할 수 있습니다. 이 시간 이후에는 6시간 기간 동안 한 번만 더 큰 번들로 전환하거나 30일 기간 동안 더 작은 번들로 전환할 수 있습니다. WorkSpace 컴퓨팅 유형 변경이 진행 중인 경우 사용자는 해당 WorkSpace 사용자와의 연결이 끊어져 사용하거나 변경할 수 없습니다. WorkSpace 컴퓨팅 유형 변경 프로세스 중에 WorkSpace 가 자동으로 재부팅됩니다. 이 프로세스는 최대 한 시간이 걸릴 수 있습니다.

  > **Note**
  >
  > 사용자가 WorkSpace 컴퓨팅 유형을 변경하면 해당 유형에 대한 청구 요율도 변경됩니다. WorkSpace

- 실행 모드 전환 - 사용자가 실행 AlwaysOn모드와 AutoStop실행 모드 WorkSpace 사이를 전환할 수 있습니다. 자세한 정보는 WorkSpace 실행 모드 관리을 참조하세요.

  > **Note**
  >
  > 사용자가 자신의 러닝 모드를 전환하면 WorkSpace 그에 따른 청구 요율이 변경됩니다 WorkSpace.

- WorkSpace 클라이언트에서 재구축 - 사용자는 a의 운영 체제를 원래 상태로 WorkSpace 재빌드할 수 있습니다. WorkSpace a가 재구축되면 사용자 볼륨 (D: 드라이브) 이 최신 백업에서 다시 생성됩니다. 12시간마다 백업이 완료되므로 사용자 데이터의 수명은 최대 12시간입니다. 새로 만든 파일의 WorkSpace 경우 사용자는 12시간을 기다려야 다시 빌드할 수 있습니다.

WorkSpace WorkSpace재구축이 진행 중인 경우 사용자는 해당 사용자와의 연결이 WorkSpace 끊기고 기존 계정을 사용하거나 변경할 수 없습니다. WorkSpace 이 프로세스는 최대 한 시간이 걸릴 수 있습니다.

- 진단 로그 업로드 - 사용자는 클라이언트 사용을 중단하지 않고도 WorkSpaces 클라이언트 로그 파일을 직접 WorkSpaces 업로드하여 문제를 해결할 수 있습니다. WorkSpaces 사용자에 대한 진단 로그 업로드를 활성화하거나 사용자가 직접 업로드하도록 허용하면 로그 파일이 자동으로 전송됩니다. WorkSpaces WorkSpaces 스트리밍 세션 이전 또는 도중에 진단 로그 업로드를 활성화할 수 있습니다.

5. 저장을 선택합니다.

사용자를 위해 Amazon Connect 오디오 최적화 활성화

WorkSpaces 관리 콘솔에서 WorkSpaces 플릿에 대한 Amazon Connect 연락 제어판(CCP) 오디오 최적화를 활성화하여 보안을 강화하고 네이티브 품질의 오디오를 사용할 수 있습니다. CCP 오디오 최적화를 활성화하고 나면 CCP 오디오는 클라이언트 엔드포인트에서 처리되며, WorkSpaces 사용자가 WorkSpaces 내에서 CCP와 상호 작용할 수 있습니다.

Amazon Connect 연락 제어판(CCP) 오디오 최적화는 다음과 호환됩니다.

- The WorkSpaces Windows 클라이언트
- Amazon Linux 및 Windows WorkSpaces
- PCoIP 또는 WSP를 사용하는 WorkSpaces

요구 사항

- Amazon Connect를 사용하여 설정해야 합니다.
- Amazon Connect Stream API를 통해 통화 신호 전송을 위한 미디어 없는 CCP를 생성하여 사용자 지정 CCP를 구축해야 합니다. 이 방식에서 미디어는 표준 CCP를 사용해 로컬 데스크톱에서 처리되고, 신호 전송 및 통화 제어는 미디어 없는 CCP를 사용해 원격 연결에서 처리됩니다. Amazon Connect Streams API에 대한 자세한 내용은 GitHub 리포지토리(https://github.com/aws/amazon-connect-streams)를 참조하세요. 구축한 사용자 지정 CCP는 Amazon Connect 에이전트가 WorkSpaces 내에서 사용할 CCP입니다.
- Amazon Connect에서 지원하는 WorkSpaces 클라이언트 엔드포인트에 웹 브라우저를 설치해야 합니다. 지원되는 브라우저 목록은 Browsers supported by Amazon Connect를 참조하세요.

> **Note**
>
> 지원되지 않는 브라우저를 사용하는 사용자는 CCP에 로그인하려고 할 때 지원되는 브라우저를 다운로드하라는 메시지가 표시됩니다.

Amazon Connect 오디오 최적화 활성화

사용자를 위해 Amazon Connect 오디오 최적화를 활성화하는 방법:

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. Amazon Connect 오디오 최적화를 확장합니다.

   > **Note**
   >
   > Amazon Connect로 구성하기 전에 업데이트를 선택하여 이전에 관리 콘솔에서 저장하지 않은 변경 사항을 모두 저장합니다.

5. Amazon Connect 구성을 선택합니다.
6. Amazon Connect 연락 제어판(CCP) 이름을 입력합니다.

   > **Note**
   >
   > CCP에 지정한 이름은 사용자 추가 기능 메뉴에 사용됩니다. 사용자에게 의미 있는 이름을 선택하세요.

7. Amazon Connect에서 생성한 Amazon Connect 연락 제어판 URL을 입력합니다. URL 가져오기에 대한 자세한 내용은 Provide access to the Contact Control Panel을 참조하세요.
8. Amazon Connect 생성을 선택합니다.

디렉터리의 Amazon Connect 오디오 최적화 세부 정보 업데이트

디렉터리의 Amazon Connect 오디오 최적화 세부 정보를 업데이트하는 방법

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. Amazon Connect 오디오 최적화를 확장합니다.

> **Note**
>
> Amazon Connect로 구성하기 전에 업데이트를 선택하여 이전에 관리 콘솔에서 저장하지 않은 변경 사항을 모두 저장합니다.

5. Amazon Connect 구성을 선택합니다.
6. 편집(Edit)을 선택합니다.
7. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
8. Amazon Connect 연락 제어판 이름 및 URL을 업데이트합니다.
9. Save를 선택합니다.

디렉터리의 Amazon Connect 오디오 최적화 삭제

디렉터리의 Amazon Connect 오디오 최적화를 삭제하는 방법

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. Amazon Connect 오디오 최적화를 확장합니다.

> **Note**
>
> Amazon Connect로 구성하기 전에 업데이트를 선택하여 이전에 관리 콘솔에서 저장하지 않은 변경 사항을 모두 저장합니다.

5. Amazon Connect 구성을 선택합니다.
6. Amazon Connect 삭제를 선택합니다.

자세한 내용은 에이전트 교육 가이드를 참조하세요.

진단 로그 업로드 활성화

WorkSpaces 클라이언트 문제를 해결하려면 자동 진단 로그 업로드를 활성화하십시오. 이 기능은 현재 Windows, macOS, Linux 및 웹 액세스 클라이언트에서 지원됩니다.

> **Note**
>
> WorkSpaces 클라이언트 진단 로그 업로드 기능은 현재 AWS GovCloud (미국 서부) 지역에서 사용할 수 없습니다.

진단 로그 업로드

진단 로그 업로드를 사용하면 클라이언트 사용을 중단하지 않고도 WorkSpaces 클라이언트 로그 파일을 직접 WorkSpaces 업로드하여 문제를 해결할 수 있습니다. WorkSpaces 사용자에 대한 진단 로그 업로드를 활성화하거나 사용자가 직접 업로드하도록 허용하면 로그 파일이 자동으로 전송됩니다. WorkSpaces WorkSpaces 스트리밍 세션 이전 또는 도중에 진단 로그 업로드를 활성화할 수 있습니다.

관리 대상 장치의 진단 로그를 자동으로 업로드하려면 진단 업로드를 지원하는 WorkSpaces 클라이언트를 설치하십시오. 로그 업로드는 기본적으로 활성화됩니다. 다음 방법 중 하나를 사용하여 설정을 수정할 수 있습니다.

옵션 1: 콘솔 사용 AWS

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 진단 로깅을 활성화할 디렉터리 이름을 선택합니다.
4. 아래로 스크롤하여 셀프 서비스 권한으로 이동합니다.
5. 세부 정보 보기를 선택합니다.
6. 편집을 선택합니다.
7. 진단 로그 업로드를 선택합니다.
8. 저장을 선택합니다.

옵션 2: API 호출 사용

디렉터리 설정을 편집하여 WorkSpaces Windows, macOS 및 Linux 클라이언트가 API 호출을 사용하여 진단 로그를 자동으로 업로드하도록 활성화하거나 비활성화할 수 있습니다. 활성화하면 클

라이언트 문제가 발생할 때 사용자 개입 WorkSpaces 없이 로그가 로 전송됩니다. 자세한 내용은 WorkSpaces API 참조를 참조하십시오.

또한 사용자가 클라이언트를 설치한 후에 자동 진단 로그 업로드를 활성화할지 선택하도록 할 수 있습니다. 자세한 내용은 WorkSpacesWindows 클라이언트 응용 프로그램, WorkSpaces macOS 클라이언트 응용 프로그램 및 WorkSpacesLinux 클라이언트 응용 프로그램을 참조하십시오.

> **Note**
>
> - 진단 로그에는 민감한 정보가 포함되어 있지 않습니다. 디렉터리 수준에서 사용자에 대한 자동 진단 로그 업로드를 비활성화하거나 사용자가 이 기능을 직접 비활성화하도록 할 수 있습니다.
> - 진단 로그 업로드 기능에 액세스하려면 다음 버전의 클라이언트를 설치해야 합니다 WorkSpaces .
>   - Windows 클라이언트 5.4.0 이상
>   - macOS 클라이언트 5.8.0 이상
>   - 우분투 22.04의 2023.1 클라이언트
>   - 우분투 20.04 클라이언트의 2023.1
>   - 웹 액세스 클라이언트를 사용하여 진단 로그 업로드 기능에 액세스할 수도 있습니다.

관리하십시오 WorkSpaces

WorkSpaces 콘솔을 WorkSpaces 사용하여 관리할 수 있습니다.

디렉터리 관리 작업을 수행하려면 the section called “디렉터리 관리 설정” 섹션을 참조하세요.

> **Note**
>
> - ENA, NVMe, PV 드라이버와 같은 네트워킹 종속성 드라이버를 업데이트해야 합니다. WorkSpaces 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 Windows 인스턴스용 ENA (엘라스틱 네트워크 어댑터) 드라이버 설치 또는 업그레이드 및 Windows 인스턴스의 PV 드라이버 업그레이드를 참조하십시오. AWS NVMe 드라이버
> - EC2Config, EC2Launch 및 EC2Launch V2 에이전트를 정기적으로 최신 버전으로 업데이트하십시오. 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 EC2Config 및 EC2Launch 업데이트를 참조하십시오.

내용

- 윈도우 BYOL 업그레이드 WorkSpaces
- 마이그레이션 a WorkSpace
- WorkSpace 삭제

윈도우 관리하기 WorkSpaces

GPO (그룹 정책 개체) 를 사용하여 Windows WorkSpaces 또는 Windows WorkSpaces 디렉터리에 속하는 사용자를 관리하기 위한 설정을 적용할 수 있습니다.

> **Note**
>
> Linux 인스턴스는 그룹 정책을 준수하지 않습니다. Amazon Linux 관리에 대한 자세한 내용은 WorkSpaces 을 참조하십시오아마존 리눅스 관리 WorkSpaces.

WorkSpaces 컴퓨터 개체에 대한 조직 단위와 WorkSpaces 사용자 개체에 대한 조직 단위를 생성하는 것이 좋습니다.

Amazon WorkSpaces 전용 그룹 정책 설정을 사용하려면 사용 중인 프로토콜 (PCoIP 또는 WorkSpaces 스트리밍 프로토콜) 에 대한 그룹 정책 관리 템플릿을 설치해야 합니다.

> **Warning**
>
> 그룹 정책 설정은 다음과 같이 WorkSpace 사용자 환경에 영향을 줄 수 있습니다.
>
> - 대화형 로그온 메시지를 구현하여 로그온 배너를 표시하면 사용자가 로그온 배너에 액세스할 수 없게 됩니다. WorkSpaces 에서는 현재 대화형 로그온 메시지 그룹 정책 설정이 지원되지 않습니다. WorkSpaces
> - 그룹 정책 설정을 통해 이동식 스토리지를 비활성화하면 로그인 실패로 인해 사용자가 D 드라이브에 액세스할 수 없는 임시 사용자 프로필로 로그인됩니다.
> - 그룹 정책 설정을 통해 원격 데스크톱 사용자 로컬 그룹에서 사용자를 제거하면 해당 사용자가 WorkSpaces 클라이언트 응용 프로그램을 통해 인증할 수 없습니다. 이 그룹 정책 설정에 대한 자세한 내용은 Microsoft 설명서의 원격 데스크톱 서비스를 통한 로그온 허용을 참조하세요.
> - 로컬 로그온 허용 보안 정책에서 기본 제공 사용자 그룹을 제거하면 PCoIP WorkSpaces 사용자는 클라이언트 응용 프로그램을 WorkSpaces 통해 해당 그룹에 연결할 수 없습니다. WorkSpaces WorkSpaces 또한 PCoIP는 PCoIP 에이전트 소프트웨어에 대한 업데이트를

받지 못합니다. PCoIP 에이전트 업데이트는 보안 및 기타 수정 사항을 포함하거나 새 기능을 활성화할 수 있습니다. WorkSpaces 이 보안 정책을 사용하는 방법에 대한 자세한 내용은 Microsoft 설명서의 로컬로 로그온 허용을 참조하세요.

- 그룹 정책 설정을 사용하여 드라이브 액세스를 제한할 수 있습니다. C 드라이브 또는 D 드라이브에 대한 액세스를 제한하도록 그룹 정책 설정을 구성하면 사용자가 해당 드라이브에 액세스할 수 없습니다. WorkSpaces 이 문제가 발생하지 않도록 하려면 사용자가 C 드라이브 및 D 드라이브에 액세스할 수 있는지 확인합니다.
- WorkSpaces 오디오 입력 기능을 사용하려면 내부 로컬 로그온 액세스가 필요합니다. WorkSpace Windows에서는 오디오 입력 기능이 기본적으로 활성화되어 있습니다. WorkSpaces 하지만 그룹 정책 설정을 통해 사용자의 로컬 로그온을 제한하는 경우에는 오디오 입력이 WorkSpaces 작동하지 않습니다. WorkSpaces 해당 그룹 정책 설정을 제거하면 다음에 을 (를) 재부팅하면 오디오 입력 기능이 활성화됩니다. WorkSpace 이 그룹 정책 설정에 대한 자세한 내용은 Microsoft 설명서의 로컬로 로그온 허용을 참조하세요.

  오디오 입력 리디렉션을 활성화하거나 비활성화하는 방법에 대한 자세한 내용은 PCoIP에서 오디오 입력 리디렉션 활성화 또는 비활성화 또는 WSP에서 오디오 입력 리디렉션 활성화 또는 비활성화 섹션을 참조하세요.
- 그룹 정책을 사용하여 Windows 전원 관리 옵션을 밸런스 또는 절전 모드로 설정하면 유휴 상태가 되면 절전 모드로 WorkSpaces 전환될 수 있습니다. 그룹 정책을 사용하여 Windows 전원 계획을 고성능으로 설정하는 것이 좋습니다. 자세한 정보는 Windows가 WorkSpace 유휴 상태로 남아 있으면 절전 모드로 전환됩니다.을 참조하세요.
- 일부 그룹 정책 설정에서는 사용자가 세션에서 연결 해제될 경우 사용자를 강제로 로그오프합니다. 사용자가 연 응용 프로그램은 모두 닫힙니다 WorkSpaces .
- “활성 상태이지만 유휴 상태인 원격 데스크톱 서비스 세션에 대한 시간 제한 설정”은 현재 WorkSpaces WSP에서 지원되지 않습니다. 활동이 있고 세션이 유휴 상태가 아닌 경우에도 연결이 끊어질 수 있으므로 WSP 세션 중에는 사용하지 마세요.

Active Directory 관리 도구를 사용하여 GPO를 작업하는 방법에 대한 자세한 내용은 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

내용

- WorkSpaces 스트리밍 프로토콜 (WSP) 용 그룹 정책 관리 템플릿 파일을 설치합니다.
- WorkSpaces 스트리밍 프로토콜 (WSP) 에 대한 그룹 정책 설정 관리
- PCoIP에 그룹 정책 관리 템플릿 설치

WorkSpaces 스트리밍 프로토콜 (WSP) 용 그룹 정책 관리 템플릿 파일을 설치합니다.

WorkSpaces 스트리밍 프로토콜 (WSP) 을 사용할 WorkSpaces 때와 관련된 그룹 정책 설정을 사용하려면 WSP용 그룹 정책 관리 `wsp.admx` 템플릿과 `wsp.adml` 파일을 디렉터리의 도메인 컨트롤러의 중앙 저장소에 추가해야 합니다. WorkSpaces `.admx` 및 `.adml` 파일에 대한 자세한 내용은 How to create and manage the Central Store for Group Policy Administrative Templates in Windows를 참조하세요.

다음 절차에서는 중앙 저장소를 생성하고 관리 템플릿 파일을 추가하는 방법을 설명합니다. 디렉터리에 연결된 디렉터리 관리 WorkSpace 또는 Amazon EC2 인스턴스에서 다음 절차를 수행합니다. WorkSpaces

WSP에 그룹 정책 관리 템플릿 파일을 설치하는 방법

1. 실행 중인 WorkSpace Windows에서 `C:\Program Files\Amazon\WSP` 디렉터리에 있는 `wsp.admx` 및 `wsp.adml` 파일의 복사본을 만드십시오.

2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 Windows 파일 탐색기를 열고 주소 표시줄에 조직의 FQDN (정규화된 도메인 이름) (예:) 을 입력합니다. WorkSpaces `\\example.com`
3. `sysvol` 폴더를 엽니다.
4. 이름이 *FQDN*인 폴더를 엽니다.
5. `Policies` 폴더를 엽니다. 이제 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies`에 들어왔을 것입니다.
6. 아직 폴더가 없다면 이름을 `PolicyDefinitions`로 지정하여 폴더를 만듭니다.
7. `PolicyDefinitions` 폴더를 엽니다.
8. `wsp.admx` 파일을 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions` 폴더로 복사합니다.
9. `PolicyDefinitions` 폴더에 이름이 `en-US`인 폴더를 만듭니다.
10. `en-US` 폴더를 엽니다.
11. `wsp.adml` 파일을 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions\en-US` 폴더로 복사합니다.

관리 템플릿 파일이 제대로 설치되었는지 확인하는 방법

1. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
2. 포리스트(Forest:***FQDN***)를 확장합니다.
3. 도메인을 확장합니다.
4. FQDN(예: `example.com`)을 확장합니다.
5. 그룹 정책 개체를 확장합니다.
6. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 권한이 위임된 도메인 컨테이너 아래에 GPO를 생성하고 연결해야 합니다.
> 로 디렉터리를 만들면 도메인 루트 AWS Managed Microsoft AD아래에 *### ##* OU (조직 구성 단위) 가 AWS Directory Service 만들어집니다. 이 OU의 이름은 디렉터리 생성

시 입력한 NetBIOS 이름을 바탕으로 합니다. NetBIOS 이름을 지정하지 않은 경우 디렉터리 DNS 이름의 첫 부분으로 기본 설정됩니다. 예를 들어, `corp.example.com`의 경우 NetBIOS 이름은 `corp`입니다.
GPO를 만들려면 기본 도메인 정책을 선택하는 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다.
yourdomainname OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

7. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
8. 이제 이 WSP 그룹 정책 개체를 사용하여 WSP 사용 시에만 적용되는 WorkSpaces 그룹 정책 설정을 수정할 수 있습니다.

WorkSpaces 스트리밍 프로토콜 (WSP) 에 대한 그룹 정책 설정 관리

그룹 정책 설정을 사용하여 WSP를 WorkSpaces 사용하는 Windows를 관리할 수 있습니다.

WSP에서 프린터 지원 구성

기본적으로 기본 원격 인쇄가 WorkSpaces 활성화됩니다. 기본 원격 인쇄는 호환되는 인쇄를 보장하기 위해 호스트 측의 일반 프린터 드라이버를 사용하기 때문에 제한된 인쇄 기능을 제공합니다.

Windows 클라이언트용 고급 원격 인쇄(WSP에서는 사용할 수 없음)를 사용하면 양면 인쇄와 같은 프린터의 특정 기능을 사용할 수 있지만, 고급 원격 인쇄를 사용하려면 호스트 측에서 일치하는 프린터 드라이버를 설치해야 합니다.

원격 인쇄는 가상 채널로 구현됩니다. 가상 채널이 비활성화되면 원격 인쇄가 작동하지 않습니다.

Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 필요에 따라 프린터 지원을 구성할 수 있습니다.

프린터 지원을 구성하려면

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 WorkSpaces 디렉터리의 도메인 컨트롤러의 중앙 저장소에 설치되어 있는지 확인하십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.

4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. [Configure remote printing] 설정을 엽니다.
10. Configure remote printing(원격 인쇄 구성) 대화 상자에서 다음 중 하나를 수행합니다.
    - 로컬 프린터 리디렉션을 활성화하려면 활성화됨을 선택한 다음 인쇄 옵션에서 기본을 선택합니다. 클라이언트 컴퓨터의 현재 기본 프린터를 자동으로 사용하려면 로컬 기본 프린터를 원격 호스트에 매핑을 선택합니다.
    - 인쇄를 비활성화하려면 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP용 클립보드 리디렉션 (복사/붙여넣기) 을 구성합니다.

기본적으로 양방향 (복사/붙여넣기) WorkSpaces 클립보드 리디렉션을 지원합니다. Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정하거나 클립보드 리디렉션이 허용되는 방향을 구성할 수 있습니다.

Windows용 클립보드 리디렉션을 구성하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *`yourdomainname`* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *`yourdomainname`* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. [Configure clipboard redirection] 설정을 엽니다.
10. 클립보드 리디렉션 구성 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.

    클립보드 리디렉션 구성을 활성화됨으로 설정하면 다음과 같은 클립보드 리디렉션 옵션을 사용할 수 있게 됩니다.

    - 복사 및 붙여넣기를 선택하여 양방향 클립보드 복사 및 붙여넣기 리디렉션을 허용합니다.
    - 서버 클립보드의 데이터를 클라이언트 클립보드로 복사만 할 수 있도록 하려면 복사만을 선택합니다.
    - 클라이언트 클립보드의 데이터를 서버 클립보드로 붙여넣기만 할 수 있도록 하려면 붙여넣기만을 선택합니다.

11. 확인을 선택합니다.

12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

알려진 제한 사항

에서 클립보드 리디렉션을 사용하도록 설정한 상태에서 Microsoft Office 응용 프로그램에서 890KB보다 큰 콘텐츠를 복사하면 응용 프로그램이 최대 5초 동안 속도가 느려지거나 응답하지 않을 수 있습니다. WorkSpace

WSP에 세션 재개 제한 시간 설정

네트워크 연결이 끊어지면 활성 WorkSpaces 클라이언트 세션의 연결이 끊어집니다. WorkSpaces Windows 및 macOS용 클라이언트 응용 프로그램은 일정 시간 내에 네트워크 연결이 복원되면 자동으로 세션 재연결을 시도합니다. 기본 세션 재개 제한 시간은 20분 (1200초) 이지만 도메인의 그룹 정책 설정에 따라 이 값을 수정할 수 있습니다. WorkSpaces

자동 세션 재개 제한 시간 값을 설정하려면

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 자동 재연결 활성화/비활성화 설정을 엽니다.
10. 자동 재연결 활성화/비활성화 대화 상자에서 활성화됨을 선택한 다음 재연결 제한 시간(초)을 원하는 제한 시간간(초)으로 설정합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP에서 비디오 입력 리디렉션 활성화 또는 비활성화

기본적으로 로컬 카메라의 데이터 리디렉션을 WorkSpaces 지원합니다. WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows용 비디오 입력 리디렉션을 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.

6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 비디오 입력 리디렉션 활성화/비활성화 설정을 엽니다.
10. 비디오 입력 리디렉션 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **gpupdate /force**를 입력합니다.

WSP에서 오디오 입력 리디렉션 활성화 또는 비활성화

기본적으로 로컬 마이크의 데이터 리디렉션을 WorkSpaces 지원합니다. WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows용 오디오 입력 리디렉션을 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.

4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 오디오 입력 리디렉션 활성화/비활성화 설정을 엽니다.
10. 오디오 입력 리디렉션 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP에서 오디오 출력 리디렉션 활성화 또는 비활성화

기본적으로 데이터를 로컬 스피커로 WorkSpaces 리디렉션합니다. WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows의 오디오 출력 리디렉션을 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces

2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:*FQDN*)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN을 확장합니다. 예를 들어 `example.com`입니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 오디오 출력 리디렉션 활성화/비활성화 설정을 엽니다.
10. 오디오 출력 리디렉션 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 다시 부팅합니다. WorkSpace Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 > 재부팅을 선택합니다 WorkSpaces. WorkSpace
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP에서 시간대 리디렉션 비활성화

기본적으로 Workspace 내의 시간은 연결에 사용되는 클라이언트의 시간대를 반영하도록 설정됩니다 WorkSpace. 이 동작은 시간대 리디렉션을 통해 제어됩니다. 여러 가지 이유로 시간대 리디렉션을 해제할 수 있습니다. 예:

- 회사가 모든 직원이 특정 시간대에서 일하기를 원합니다(일부 직원이 다른 시간대에 있더라도).

- 특정 시간대의 특정 시간에 WorkSpace 실행되도록 스케줄링된 작업이 a에 있습니다.
- 여행을 많이 하는 사용자는 일관성과 개인 취향을 위해 한 시간대에 WorkSpaces 머물기를 원합니다.

WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows의 시간대 리디렉션을 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *`yourdomainname`* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *`yourdomainname`* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 시간대 리디렉션 활성화/비활성화 설정을 엽니다.
10. 시간대 리디렉션 활성화/비활성화 대화 상자에서 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

- 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
- 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

13. 의 시간대를 원하는 시간대로 설정합니다. WorkSpaces

의 시간대는 이제 WorkSpaces 정적이며 더 이상 클라이언트 컴퓨터의 시간대를 미러링하지 않습니다.

WSP 보안 설정 구성

WSP의 경우 전송 중 데이터는 TLS 1.2 암호화를 사용하여 암호화됩니다. 기본적으로 다음 암호는 모두 암호화에 허용되며 클라이언트와 서버는 사용할 암호를 협상합니다.

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 TLS 보안 모드를 수정하고 특정 암호 그룹을 새로 추가하거나 차단할 수 있습니다. 이러한 설정과 지원되는 암호 제품군에 대한 자세한 설명은 보안 설정 구성 그룹 정책 대화 상자에 나와 있습니다.

WSP 보안 설정을 구성하는 방법

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN을 확장합니다. 예를 들어 `example.com`입니다.
6. 그룹 정책 개체를 확장합니다.

7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 보안 설정 구성을 엽니다.
10. 보안 설정 구성 대화 상자에서 활성화됨을 선택합니다. 허용하려는 암호 그룹을 추가하고 차단하려는 암호 그룹을 제거합니다. 이러한 설정에 대한 자세한 내용은 보안 설정 구성 대화 상자에 제공된 설명을 참조하세요.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 이후와 세션을 다시 시작한 후에 적용됩니다. WorkSpace WorkSpace 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
    - 를 재부팅하려면 Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces. WorkSpace
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP에 확장 구성

기본적으로 WorkSpaces 확장에 대한 지원은 비활성화되어 있습니다. 필요한 경우 다음과 같은 방법으로 확장을 WorkSpace 사용하도록 구성할 수 있습니다.

- 서버 및 클라이언트 - 서버와 클라이언트 모두에 확장을 활성화합니다.
- 서버만 - 서버에만 확장을 활성화합니다.
- 클라이언트만 - 클라이언트에만 확장을 활성화합니다.

Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 확장 사용을 구성할 수 있습니다.

WSP에 확장을 구성하는 방법

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 WorkSpaces 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:*FQDN*)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN을 확장합니다. 예제: `example.com`
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 확장 구성 설정을 엽니다.
10. 확장 구성 대화 상자에서 활성화됨을 선택한 다음 원하는 지원 옵션을 설정합니다. 클라이언트만, 서버 및 클라이언트 또는 서버만을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 세션을 다시 시작한 후에 적용됩니다. WorkSpace 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 다시 부팅합니다 WorkSpace. Amazon WorkSpaces 콘솔에서 을 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces.
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP에서 스마트 카드 리디렉션 활성화 또는 비활성화

기본적으로 WorkSpaces Amazon은 세션 전 인증 또는 세션 내 인증을 위한 스마트 카드 사용을 지원하지 않습니다. 사전 세션 인증은 사용자가 로그인하는 동안 수행되는 스마트 카드 인증을 말합니다. WorkSpaces 세션 내 인증은 로그인 후 수행되는 인증을 말합니다.

필요한 경우 그룹 정책 설정을 사용하여 WorkSpaces Windows에 대한 사전 세션 및 세션 내 인증을 활성화할 수 있습니다. 또한 EnableClientAuthentication API 작업 또는 enable-client-authentication AWS CLI 명령을 사용하여 AD Connector 디렉터리 설정을 통해 세션 전 인증을 활성화해야 합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Enable Smart Card Authentication for AD Connector를 참조하세요.

> **Note**
>
> Windows에서 스마트 카드를 사용할 수 있게 WorkSpaces 하려면 추가 단계가 필요합니다. 자세한 정보는 인증에 스마트 카드 사용을 참조하세요.

Windows용 스마트 카드 리디렉션을 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *`yourdomainname`* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인

에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 스마트 카드 리디렉션 활성화/비활성화 설정을 엽니다.
10. 스마트 카드 리디렉션 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 WorkSpace 세션을 다시 시작한 후에 적용됩니다. 그룹 정책 변경 내용을 적용하려면 Amazon WorkSpaces 콘솔에서 을 WorkSpace (를 선택한 다음 Actions WorkSpace, Reboot WorkSpaces) 를 재부팅하십시오.

WSP에 대한 WebAuthn (FIDO2) 리디렉션을 활성화 또는 비활성화합니다.

Amazon은 기본적으로 세션 내 인증에 WebAuthn 인증자를 사용할 수 WorkSpaces 있도록 합니다. 세션 내 인증이란 로그인 후 수행되고 세션 내에서 실행되는 웹 애플리케이션에서 요청하는 WebAuthn 인증을 말합니다.

요구 사항

WebAuthn WSP용 (FIDO2) 리디렉션에는 다음이 필요합니다.

- WSP 호스트 에이전트 버전 2.0.0.1425 이상
- WorkSpaces 클라이언트:
  - 리눅스 우분투 22.04 2023.3 이상
  - 윈도우 5.19.0 이상
  - 맥 클라이언트 5.19.0 이상
- Amazon DCV WebAuthn 리디렉션 WorkSpaces 확장을 실행하는 데 설치된 웹 브라우저:
  - 구글 크롬 1.16+
  - 마이크로소프트 엣지 116+

윈도우용 WebAuthn (FIDO2) 리디렉션 활성화 또는 비활성화 WorkSpaces

필요한 경우 그룹 정책 설정을 사용하여 WorkSpaces Windows용 WebAuthn 인증자와의 세션 내 인증 지원을 활성화하거나 비활성화할 수 있습니다. 이 설정을 사용하거나 구성하지 않으면 WebAuthn 리디렉션이 활성화되고 사용자는 원격 내의 로컬 인증자를 활용할 수 있습니다. WorkSpace

기능을 사용하도록 설정하면 세션의 브라우저에서 WebAuthn 들어오는 모든 요청이 로컬 클라이언트로 리디렉션됩니다. 사용자는 Windows Hello 또는 로컬로 연결된 보안 디바이스 YubiKey 또는 다른 FIDO2 호환 인증자를 사용하여 인증 프로세스를 완료할 수 있습니다.

Windows용 WebAuthn (FIDO2) 리디렉션을 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *`yourdomainname`* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *`yourdomainname`* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 리디렉션 사용/사용 안 함 설정을 WebAuthn 엽니다.
10. WebAuthn 리디렉션 활성화/비활성화 대화 상자에서 활성화 또는 비활성화를 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 내용을 적용하려면 Amazon WorkSpace WorkSpaces 콘솔로 이동하여 를 선택하여 WorkSpace 재부팅하십시오. 그런 다음 [작업], [재부팅 WorkSpaces] 을 선택합니다.

Amazon DCV WebAuthn 리디렉션 확장 프로그램 설치

사용자는 다음 중 하나를 수행하여 기능을 활성화한 WebAuthn 후 사용할 Amazon DCV WebAuthn 리디렉션 확장을 설치해야 합니다.

- 브라우저에서 브라우저 확장 프로그램을 활성화하라는 메시지가 사용자에게 표시됩니다.

> **Note**
>
> 이 메시지는 일회성 브라우저 프롬프트입니다. WSP 에이전트 버전을 2.0.0.1425 이상으로 업데이트하면 사용자에게 알림이 전송됩니다. 최종 사용자에게 WebAuthn 리디렉션이 필요하지 않은 경우 브라우저에서 확장 프로그램을 제거하기만 하면 됩니다. 아래 GPO 정책을 사용하여 WebAuthn 리디렉션 확장 프로그램 설치 프롬프트를 차단할 수도 있습니다.

- 아래 GPO 정책을 사용하여 사용자를 위한 리디렉션 확장 프로그램을 강제로 설치할 수 있습니다. GPO 정책을 사용하면 사용자가 인터넷 액세스가 가능한 지원되는 브라우저를 실행할 때 확장 프로그램이 자동으로 설치됩니다.
- 사용자는 Microsoft Edge 애드온 또는 Chrome 웹 스토어를 사용하여 확장 프로그램을 수동으로 설치할 수 있습니다.

그룹 정책을 사용하여 브라우저 확장 프로그램을 관리하고 설치합니다.

Active Directory (AD) 도메인에 가입된 세션 호스트의 경우 사용자 도메인에서 중앙에서 그룹 정책을 사용하거나 각 세션 호스트의 로컬 그룹 정책 편집기를 사용하여 Amazon DCV WebAuthn 리디렉션 확장을 설치할 수 있습니다. 이 프로세스는 사용 중인 브라우저에 따라 달라집니다.

마이크로소프트 엣지의 경우

1. Microsoft Edge 관리 템플릿을 다운로드하고 설치합니다.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

8. 컴퓨터 구성, 관리 템플릿, Microsoft Edge 및 확장 프로그램을 선택합니다.
9. 확장 관리 설정 구성을 열고 활성화로 설정합니다.
10. 확장 관리 설정 구성에서 다음을 입력합니다.

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 WorkSpace 세션을 다시 시작한 후에 적용됩니다. 그룹 정책 변경 내용을 적용하려면 Amazon WorkSpace WorkSpaces 콘솔로 이동하여 를 선택하여 WorkSpace 재부팅 하십시오. 그런 다음 [작업], [재부팅 WorkSpaces] 을 선택합니다.

> **Note**
>
> 다음 구성 관리 설정을 적용하여 확장 프로그램 설치를 차단할 수 있습니다.
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

구글 크롬의 경우

1. Google 크롬 관리 템플릿을 다운로드하여 설치합니다. 자세한 내용은 관리되는 PC에 Chrome 브라우저 정책 설정을 참조하십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.
8. 컴퓨터 구성, 관리 템플릿, Google Chrome, 확장 프로그램을 선택합니다.

9. 확장 프로그램 관리 설정 구성을 열고 활성화됨으로 설정합니다.
10. 확장 관리 설정 구성에서 다음을 입력합니다.

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 WorkSpace 세션을 다시 시작한 후에 적용됩니다. 그룹 정책 변경 내용을 적용하려면 Amazon WorkSpace WorkSpaces 콘솔로 이동하여 를 선택하여 WorkSpace 재부팅 하십시오. 그런 다음 [작업], [재부팅 WorkSpaces] 을 선택합니다.

> **Note**
>
> 다음 구성 관리 설정을 적용하여 확장 프로그램 설치를 차단할 수 있습니다.
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

WSP에서 화면 잠금 시 세션 연결 해제 활성화 또는 비활성화

필요한 경우 Windows 잠금 화면이 감지되면 사용자 WorkSpaces 세션 연결을 끊을 수 있습니다. WorkSpaces 클라이언트에 다시 연결하려면 활성화된 인증 유형에 따라 사용자가 암호 또는 스마트 카드를 사용하여 자신을 인증할 수 있습니다. WorkSpaces

이 그룹 정책 설정은 기본적으로 비활성화되어 있습니다. 필요한 경우 그룹 정책 설정을 사용하여 Windows에서 Windows 잠금 화면이 감지될 때 세션 연결을 끊을 수 있도록 설정할 수 있습니다. WorkSpaces

> **Note**
>
> - 이 그룹 정책 설정은 암호 인증 세션과 스마트 카드 인증 세션 모두에 적용됩니다.
> - Windows에서 스마트 카드를 사용할 수 있게 WorkSpaces 하려면 추가 단계가 필요합니다. 자세한 정보는 인증에 스마트 카드 사용을 참조하세요.

Windows의 화면 잠금에서 세션 연결 끊기를 활성화 또는 비활성화하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *`yourdomainname`* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *`yourdomainname`* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 화면 잠금 시 세션 연결 해제 활성화/비활성화 설정을 엽니다.
10. 화면 잠금 시 세션 연결 해제 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 해당 세션에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

WSP용 간접 디스플레이 드라이버 (IDD) 활성화 또는 비활성화

기본적으로 간접 디스플레이 드라이버 (IDD) 사용을 WorkSpaces 지원합니다. WorkSpacesWindows 에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows용 간접 디스플레이 드라이버 (IDD) 를 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon Elastic Compute Cloud 인스턴스에서 그룹 정책 관리 도구 (gpmc.msc) 를 엽니다. WorkSpaces
3. 포리스트 (포리스트:FQDN) 를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 메뉴를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트를 연 다음 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 AWS 관리형 Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 만들 수 없습니다. WorkSpaces 대신 OU (Organization Unit) 나 해당 도메인 이름 아래의 OU를 선택하고 메뉴를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트를 연 다음 이 도메인에 GPO 만들기를 선택하고 여기에 연결을 선택합니다. `yourdomainname` `yourdomainnameOU`에 대한 자세한 내용은 AWS Directory Service 관리 가이드의 생성 항목을 참조하십시오.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. AWS 간접 디스플레이 드라이버 사용 설정을 엽니다.
10. AWS 간접 디스플레이 드라이버 활성화 대화 상자에서 활성화 또는 비활성화를 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션을 다시 시작한 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    a. 를 다시 부팅합니다 WorkSpace (WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).

b. 관리 명령 프롬프트에 `gpupdate /force`를 입력합니다.

WSP에 디스플레이 설정 구성

WorkSpaces 최대 프레임 속도, 최소 이미지 품질, 최대 이미지 품질, YUV 인코딩 등 여러 가지 디스플레이 설정을 구성할 수 있습니다. 필요한 이미지 품질, 반응성 및 색상 정확도에 따라 이러한 설정을 조정하세요.

기본적으로 최대 프레임 속도 값은 25입니다. 최대 프레임 속도 값은 초당 허용되는 최대 프레임 수(fps)를 지정합니다. 값 0은 제한이 없음을 의미합니다.

기본적으로 최소 이미지 품질 값은 30입니다. 최소 이미지 품질은 최상의 이미지 반응성 또는 최상의 이미지 품질을 위해 최적화될 수 있습니다. 반응성을 극대화하려면 최소 품질을 낮추세요. 최상의 품질을 위해서는 최소 품질을 높이세요.

- 최상의 반응성을 위한 이상적인 값은 30에서 90 사이입니다.
- 최상의 품질을 위한 이상적인 값은 60에서 90 사이입니다.

기본적으로 최대 이미지 품질 값은 80입니다. 최대 이미지 품질은 이미지 반응성이나 품질에는 영향을 주지 않지만 네트워크 사용을 제한하기 위해 최댓값을 설정합니다.

기본적으로 이미지 인코딩은 YUV420으로 설정됩니다. YUV444 인코딩 활성화를 선택하면 높은 색상 정확도를 위해 YUV444 인코딩이 활성화됩니다.

WorkSpacesWindows의 경우 그룹 정책 설정을 사용하여 최대 프레임 속도, 최소 이미지 품질 및 최대 이미지 품질 값을 구성할 수 있습니다.

Windows용 디스플레이 설정을 구성하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 WorkSpaces 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.

7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 디스플레이 설정 구성 설정을 엽니다.
10. 디스플레이 설정 구성 대화 상자에서 활성화됨을 선택한 다음 최대 프레임 속도(fps), 최소 이미지 품질 및 최대 이미지 품질 값을 원하는 수준으로 설정합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 세션을 다시 시작한 후에 적용됩니다. WorkSpace 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - Amazon WorkSpaces 콘솔을 재부팅하고 원하는 항목을 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpace. WorkSpaces
    - 관리 명령 프롬프트에 **gpupdate /force**를 입력합니다.

WSP용 AWS 가상 디스플레이 전용 드라이버용 vSync 활성화 또는 비활성화

기본적으로 가상 디스플레이 전용 드라이버의 vSync 기능 사용을 WorkSpaces 지원합니다. AWS WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

Windows용 vSync를 사용하거나 사용하지 않도록 설정하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오 WorkSpaces .
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon Elastic Compute Cloud 인스턴스에서 그룹 정책 관리 도구 (gpmc.msc) 를 엽니다. WorkSpaces
3. 포리스트 (포리스트:FQDN) 를 확장합니다.

4. 도메인을 확장합니다.
5. FQDN(예: `example.com`)을 확장합니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 메뉴를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트를 연 다음 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 AWS 관리형 Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 만들 수 없습니다. WorkSpaces 대신 OU (Organization Unit) 나 해당 도메인 이름 아래의 OU를 선택하고 메뉴를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트를 연 다음 이 도메인에 GPO 만들기를 선택하고 여기에 연결을 선택합니다. `yourdomainname` `yourdomainnameOU`에 대한 자세한 내용은 AWS Directory Service 관리 가이드의 생성 항목을 참조하십시오.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. AWS 가상 디스플레이 전용 드라이버 설정의 vSync 활성화 기능을 엽니다.
10. AWS 가상 디스플레이 전용 드라이버 대화 상자의 vSync 활성화 기능에서 활성화 또는 비활성화를 선택합니다.
11. 확인을 선택합니다.
12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 이후 WorkSpace 및 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 내용을 적용하려면 다음과 같이 하십시오.

    a. 다음 중 하나를 WorkSpace 수행하여 를 다시 시작합니다.

        i. 옵션 1 — WorkSpaces 콘솔에서 WorkSpace 재부팅하려는 항목을 선택합니다. 그런 다음 작업, 재부팅을 선택합니다 WorkSpaces.

        ii. 옵션 2 — 관리 명령 프롬프트에서 를 입력합니다`gpupdate /force`.

    b. 설정을 적용하려면 WorkSpace 에 다시 연결합니다.

    c. 워크스페이스를 다시 재부팅합니다.

WSP에 로그 세부 정보 표시 수준 구성

기본적으로 WSP의 로그 상세 정보 수준은 Info로 WorkSpaces 설정됩니다. 아래에 설명된 대로 로그의 세부 정보 표시 수준을 최소 상세에서 최대 상세까지 설정할 수 있습니다.

- 오류 - 최소 상세
- 경고
- 정보 - 기본값
- 디버그 - 최대 상세

Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 로그 세부 정보 표시 수준을 구성할 수 있습니다.

Windows의 로그 세부 정보 표시 수준을 구성하려면 WorkSpaces

1. WSP용 최신 WorkSpaces 그룹 정책 관리 템플릿이 디렉터리의 도메인 컨트롤러 중앙 저장소에 설치되어 있는지 확인하십시오. WorkSpaces
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
3. 포리스트(Forest:***FQDN***)를 확장합니다.
4. 도메인을 확장합니다.
5. FQDN을 확장합니다. 예를 들어 `example.com`입니다.
6. 그룹 정책 개체를 확장합니다.
7. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

   > **Note**
   >
   > 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다. *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

8. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, Amazon 및 WSP를 선택합니다.
9. 로그 세부 정보 표시 수준 구성 설정을 엽니다.
10. 로그 세부 정보 표시 수준 구성 대화 상자에서 활성화됨을 선택한 다음 로그 세부 정보 표시 수준을 디버그, 오류, 정보 또는 경고로 설정합니다.
11. 확인을 선택합니다.

12. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 WorkSpace 이후와 세션을 다시 시작한 후에 적용됩니다. WorkSpace 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 다시 부팅합니다 WorkSpace. Amazon WorkSpaces 콘솔에서 을 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces.
    - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

PCoIP에 그룹 정책 관리 템플릿 설치

PCoIP 프로토콜을 사용할 WorkSpaces 때 Amazon에만 적용되는 그룹 정책 설정을 사용하려면 사용 중인 PCoIP 에이전트 버전 (32비트 또는 64비트) 에 적합한 그룹 정책 관리 템플릿을 추가해야 합니다. WorkSpaces

> **Note**
>
> 32비트 및 64비트 에이전트를 혼합하여 사용하는 경우 32비트 에이전트용 그룹 정책 관리 템플릿을 사용할 수 있으며, 그룹 정책 설정은 32비트 및 64비트 에이전트 모두에 적용됩니다. WorkSpaces 모든 사용자가 64비트 에이전트를 WorkSpaces 사용하는 경우 64비트 에이전트용 관리 템플릿을 사용하도록 전환할 수 있습니다.

32비트 에이전트가 WorkSpaces 있는지 64비트 에이전트가 있는지 확인하려면

1. 에 로그인한 다음 보기 WorkSpace, 보내기 Ctrl + Alt + Delete를 선택하거나 작업 표시줄을 마우스 오른쪽 단추로 클릭하고 작업 관리자를 선택하여 작업 관리자를 엽니다.
2. 태스크 관리자에서 세부 정보 탭으로 이동하여 열 헤더를 마우스 오른쪽 버튼으로 클릭한 다음 열 선택을 선택합니다.
3. 열 선택 대화 상자에서 플랫폼을 선택한 다음 확인을 선택합니다.
4. 세부 정보 탭에서 `pcoip_agent.exe`를 찾고 플랫폼 열에서 값을 확인하여 PCoIP 에이전트가 32비트인지 64비트인지 확인합니다. (32비트와 64비트 WorkSpaces 구성 요소가 혼합되어 표시될 수 있지만 이는 정상입니다.)

PCoIP(32비트)에 그룹 정책 관리 템플릿 설치

32비트 PCoIP 에이전트에서 PCoIP 프로토콜을 사용할 WorkSpaces 때와 관련된 그룹 정책 설정을 사용하려면 PCoIP용 그룹 정책 관리 템플릿을 설치해야 합니다. 디렉터리에 연결된 디렉터리 관리 WorkSpace 또는 Amazon EC2 인스턴스에서 다음 절차를 수행합니다.

.adm 파일 사용에 대한 자세한 내용은 Microsoft 설명서의 Recommendations for managing Group Policy administrative template (.adm) files를 참조하세요.

PCoIP에 그룹 정책 관리 템플릿을 설치하는 방법

1. 실행 중인 WorkSpace Windows에서 `C:\Program Files (x86)\Teradici\PCoIP Agent \configuration` 디렉터리에 있는 `pcoip.adm` 파일의 복사본을 만드십시오.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 (gpmc.msc) 를 열고 WorkSpaces 컴퓨터 계정이 포함된 도메인의 조직 구성 단위로 이동합니다. WorkSpaces
3. 머신 계정 조직 구성 단위를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 [Create a GPO in this domain, and link it here]를 선택합니다.
4. 새 GPO 대화 상자에 GPO를 설명하는 이름 (예: WorkSpaces 시스템 정책) 을 입력하고 소스 스타터 GPO는 (없음) 으로 설정된 상태로 둡니다. 확인을 선택합니다.
5. 새 GPO의 컨텍스트(오른쪽 클릭) 메뉴를 열고 편집을 선택합니다.
6. 그룹 정책 관리 편집기에서 [Computer Configuration], [Policies] 및 [Administrative Templates]를 선택합니다. 주 메뉴에서 [Action], [Add/Remove Templates]를 선택합니다.
7. [Add/Remove Templates] 대화 상자에서 [Add]를 선택하여 앞서 복사한 `pcoip.adm` 파일을 선택한 다음 [Open], [Close]를 선택합니다.
8. 그룹 정책 관리 편집기를 닫습니다. 이제 이 GPO를 사용하여 특정 그룹 정책 설정을 수정할 수 있습니다. WorkSpaces

관리 템플릿 파일이 제대로 설치되었는지 확인하는 방법

1. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 (gpmc.msc) 를 열고 컴퓨터 계정의 WorkSpaces WorkSpaces GPO로 이동하여 선택합니다. WorkSpaces 주 메뉴에서 [Action], [Edit]를 선택합니다.
2. 그룹 정책 관리 편집기에서 [Computer Configuration], [Policies], [Administrative Templates], [Classic Administrative Templates] 및 [PCoIP Session Variables]를 선택합니다.
3. 이제 이 PCoIP 세션 변수 그룹 정책 객체를 사용하여 PCoIP를 사용할 WorkSpaces 때 Amazon에만 적용되는 그룹 정책 설정을 수정할 수 있습니다.

> **Note**
>
> 사용자가 설정을 재정의하도록 허용하려면 관리자 설정 재정의 가능을 선택하고, 허용하지 않으려면 관리자 설정 재정의 불가능를 선택합니다.

PCoIP(64비트)에 그룹 정책 관리 템플릿 설치

PCoIP 프로토콜을 사용할 WorkSpaces 때와 관련된 그룹 정책 설정을 사용하려면 해당 디렉터리의 도메인 컨트롤러의 중앙 저장소에 PCoIP용 그룹 정책 관리 `PCoIP.admx` 템플릿과 `PCoIP.adml` 파일을 추가해야 합니다. WorkSpaces `.admx` 및 `.adml` 파일에 대한 자세한 내용은 How to create and manage the Central Store for Group Policy Administrative Templates in Windows를 참조하세요.

다음 절차에서는 중앙 저장소를 생성하고 관리 템플릿 파일을 추가하는 방법을 설명합니다. 디렉터리에 연결된 디렉터리 관리 WorkSpace 또는 Amazon EC2 인스턴스에서 다음 절차를 수행합니다. WorkSpaces

PCoIP에 그룹 정책 관리 템플릿 파일을 설치하는 방법

1. 실행 중인 WorkSpace Windows에서 `C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions` 디렉터리에 있는 `PCoIP.admx` 및 `PCoIP.adml` 파일의 복사본을 만드십시오. `PCoIP.adml` 파일은 해당 디렉터리의 `en-US` 하위 폴더에 있습니다.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 Windows 파일 탐색기를 열고 주소 표시줄에 조직의 FQDN (정규화된 도메인 이름) (예:) 을 입력합니다. WorkSpaces `\\example.com`
3. `sysvol` 폴더를 엽니다.
4. 이름이 *`FQDN`*인 폴더를 엽니다.
5. `Policies` 폴더를 엽니다. 이제 `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`에 들어왔을 것입니다.
6. 아직 폴더가 없다면 이름을 `PolicyDefinitions`로 지정하여 폴더를 만듭니다.
7. `PolicyDefinitions` 폴더를 엽니다.
8. `PCoIP.admx` 파일을 `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions` 폴더로 복사합니다.
9. `PolicyDefinitions` 폴더에 이름이 `en-US`인 폴더를 만듭니다.
10. `en-US` 폴더를 엽니다.

11. PCoIP.adml 파일을 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 폴더로 복사합니다.

관리 템플릿 파일이 제대로 설치되었는지 확인하는 방법

1. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
2. 포리스트(Forest:***FQDN***)를 확장합니다.
3. 도메인을 확장합니다.
4. FQDN(예: example.com)을 확장합니다.
5. 그룹 정책 개체를 확장합니다.
6. 기본 도메인 정책을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 후 편집을 선택합니다.

> **Note**
>
> 지원하는 도메인이 WorkSpaces AWS Managed Microsoft AD 디렉터리인 경우 기본 도메인 정책을 사용하여 GPO를 생성할 수 없습니다. 대신 권한이 위임된 도메인 컨테이너 아래에 GPO를 생성하고 연결해야 합니다.
> 로 디렉터리를 만들면 도메인 루트 AWS Managed Microsoft AD아래에 *### ##* OU (조직 구성 단위) 가 AWS Directory Service 만들어집니다. 이 OU의 이름은 디렉터리 생성 시 입력한 NetBIOS 이름을 바탕으로 합니다. NetBIOS 이름을 지정하지 않은 경우 디렉터리 DNS 이름의 첫 부분으로 기본 설정됩니다. 예를 들어, corp.example.com의 경우 NetBIOS 이름은 corp입니다.
> GPO를 만들려면 기본 도메인 정책을 선택하는 대신 *yourdomainname* OU 또는 해당 OU 아래에 있는 것을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다.
> *yourdomainname* OU에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 What Gets Created를 참조하세요.

7. 그룹 정책 관리 편집기에서 컴퓨터 구성, 정책, 관리 템플릿, PCoIP 세션 변수를 선택합니다.
8. 이제 이 PCoIP 세션 변수 그룹 정책 개체를 사용하여 PCoIP 사용 시에만 적용되는 그룹 정책 설정을 수정할 수 있습니다. WorkSpaces

> **Note**
>
> 사용자가 설정을 재정의하도록 허용하려면 관리자 설정 재정의 가능을 선택하고, 허용하지 않으려면 관리자 설정 재정의 불가능를 선택합니다.

PCoIP의 그룹 정책 설정을 관리합니다.

그룹 정책 설정을 사용하여 PCoIP를 WorkSpaces 사용하는 Windows를 관리할 수 있습니다.

PCoIP에서 프린터 지원 구성

기본적으로 기본 원격 인쇄가 WorkSpaces 활성화되어 있습니다. 기본 원격 인쇄는 호환되는 인쇄를 보장하기 위해 호스트 측의 일반 프린터 드라이버를 사용하기 때문에 제한된 인쇄 기능을 제공합니다.

Windows 클라이언트용 고급 원격 인쇄를 사용하면 양면 인쇄와 같은 프린터의 특정 기능을 사용할 수 있지만, 고급 원격 인쇄를 사용하려면 호스트 측에서 일치하는 프린터 드라이버를 설치해야 합니다.

원격 인쇄는 가상 채널로 구현됩니다. 가상 채널이 비활성화되면 원격 인쇄가 작동하지 않습니다.

Windows의 WorkSpaces 경우 그룹 정책 설정을 사용하여 필요에 따라 프린터 지원을 구성할 수 있습니다.

프린터 지원을 구성하려면

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. [Configure remote printing] 설정을 엽니다.
4. Configure remote printing(원격 인쇄 구성) 대화 상자에서 다음 중 하나를 수행합니다.
   - 고급 원격 인쇄를 활성화하려면 Enabled(활성)를 선택한 다음, Options(옵션), Configure remote printing(원격 인쇄 구성)에서 Basic and Advanced printing for Windows clients(Windows 클라이언트용 기본 및 고급 인쇄)를 선택합니다. 클라이언트 컴퓨터의 현재 기본 프린터를 자동으로 사용하려면 Automatically set default printer(기본 프린터 자동 설정)를 선택합니다.
   - 인쇄를 비활성화하려면 Enabled(활성)를 선택한 다음, Options(옵션), Configure remote printing(원격 인쇄 구성)에서 Printing disabled(인쇄 비활성)를 선택합니다.

5. 확인을 선택합니다.
6. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

로컬 프린터 리디렉션은 기본적으로 비활성화됩니다. 그룹 정책 설정을 사용하여 이 기능을 활성화하여 연결할 때마다 로컬 프린터가 기본 프린터로 설정되도록 할 수 있습니다 WorkSpace.

> **Note**
>
> Amazon WorkSpaces Linux에서는 로컬 프린터 리디렉션을 사용할 수 없습니다.

로컬 프린터 자동 리디렉션을 활성화하려면

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. [Configure remote printing] 설정을 엽니다.
4. 활성화됨을 선택한 다음 옵션의 원격 인쇄 구성에서 다음 중 하나를 선택합니다.
   - Windows 클라이언트용 기본 및 고급 인쇄
   - 기본 인쇄
5. 기본 프린터 자동 설정을 선택한 다음 확인을 선택합니다.
6. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

PCoIP에 대한 클립보드 리디렉션 (복사/붙여넣기) 활성화 또는 비활성화

기본적으로 클립보드 리디렉션을 지원합니다. WorkSpaces WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

클립보드 리디렉션을 활성화 또는 비활성화하려면

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. [Configure clipboard redirection] 설정을 엽니다.
4. Configure clipboard redirection(클립보드 리디렉션 구성) 대화 상자에서 Enabled(활성화)를 선택한 후 다음 설정 중 하나를 선택하여 클립보드 리디렉션을 허용할 방향을 결정합니다. 완료했으면 확인을 선택합니다.

   - 양방향으로 비활성화됨
   - 에이전트를 클라이언트에서만 (로컬 컴퓨터로) 사용할 WorkSpace 수 있도록 했습니다.
   - 클라이언트에서 에이전트만 사용할 수 있도록 설정 (로컬 컴퓨터로 WorkSpace)
   - 양방향으로 활성화됨
5. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 이후 WorkSpace 및 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

알려진 제한 사항

에서 클립보드 리디렉션을 사용하도록 설정한 상태에서 Microsoft Office 응용 프로그램에서 890KB보다 큰 콘텐츠를 복사하면 응용 프로그램이 최대 5초 동안 속도가 느려지거나 응답하지 않을 수 있습니다. WorkSpace

PCoIP에 세션 재개 제한 시간 설정

네트워크 연결이 끊어지면 활성 WorkSpaces 클라이언트 세션의 연결이 끊어집니다. WorkSpaces Windows 및 macOS용 클라이언트 응용 프로그램은 일정 시간 내에 네트워크 연결이 복원되면 자동으

로 세션 재연결을 시도합니다. 기본 세션 재개 제한 시간은 20분이지만 도메인의 그룹 정책 설정에 따라 이 값을 수정할 수 있습니다. WorkSpaces

자동 세션 재개 제한 시간 값을 설정하려면

1. 최신 PCoIP (32비트) 용 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. [Configure Session Automatic Reconnection Policy] 설정을 엽니다.
4. [Configure Session Automatic Reconnection Policy] 대화 상자에서 [Enabled]를 선택하고 [Configure Session Automatic Reconnection Policy] 옵션을 원하는 제한 시간(분)으로 설정한 다음 [OK]를 선택합니다.
5. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

PCoIP에서 오디오 입력 리디렉션 활성화 또는 비활성화

기본적으로 Amazon은 로컬 마이크의 데이터 리디렉션을 WorkSpaces 지원합니다. WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 비활성화할 수 있습니다.

> **Note**
>
> 그룹 정책 설정을 통해 사용자의 로컬 로그온을 제한하는 경우 오디오 입력은 사용자 WorkSpaces 계정에서 작동하지 않습니다. WorkSpaces 해당 그룹 정책 설정을 제거하면 다음에 을 (를) 재부팅하면 오디오 입력 기능이 활성화됩니다. WorkSpace 이 그룹 정책 설정에 대한 자세한 내용은 Microsoft 설명서의 로컬로 로그온 허용을 참조하세요.

오디오 입력 리디렉션을 활성화 또는 비활성화하는 방법

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. PCoIP 세션에서 오디오 입력 활성화/비활성화 설정을 엽니다.
4. PCoIP 세션에서 오디오 입력 활성화/비활성화 대화 상자에서 활성화됨 또는 비활성화됨을 선택합니다.
5. 확인을 선택합니다.
6. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

PCoIP에서 시간대 리디렉션 비활성화

기본적으로 Workspace 내의 시간은 연결에 사용되는 클라이언트의 시간대를 반영하도록 설정됩니다 WorkSpace. 이 동작은 시간대 리디렉션을 통해 제어됩니다. 여러 가지 이유로 시간대 리디렉션을 해제할 수 있습니다.

- 회사가 모든 직원이 특정 시간대에서 일하기를 원합니다(일부 직원이 다른 시간대에 있더라도).
- 특정 시간대의 특정 시간에 WorkSpace 실행되도록 스케줄링된 작업이 a에 있습니다.
- 여행을 많이 하는 사용자는 일관성과 개인 취향을 위해 한 시간대에 WorkSpaces 머물기를 원합니다.

WorkSpacesWindows에 필요한 경우 그룹 정책 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

시간대 리디렉션을 비활성화하려면

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. 시간대 리디렉션 구성 설정을 엽니다.
4. 시간대 리디렉션 구성 대화 상자에서 비활성화됨을 선택합니다.

5. 확인을 선택합니다.
6. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.
7. 의 시간대를 원하는 시간대로 설정합니다. WorkSpaces

의 시간대는 이제 WorkSpaces 정적이며 더 이상 클라이언트 컴퓨터의 시간대를 미러링하지 않습니다.

PCoIP 보안 설정 구성

PCoIP의 경우 전송 중 데이터는 TLS 1.2 암호화 및 SigV4 요청 서명을 사용하여 암호화됩니다. PCoIP 프로토콜은 AES 암호화로 암호화된 UDP 트래픽을 스트리밍 픽셀에 사용합니다. 포트 4172(TCP 및 UDP)를 사용하는 스트리밍 연결은 AES-128 및 AES-256 암호를 사용하여 암호화되지만 암호화는 기본적으로 128비트로 설정됩니다. PCoIP 보안 설정 구성 그룹 정책 설정을 사용하여 이 기본값을 256비트로 변경할 수 있습니다.

또한 이 그룹 정책 설정을 사용하여 TLS 보안 모드를 수정하고 특정 암호 그룹을 차단할 수 있습니다. 이러한 설정과 지원되는 암호 제품군에 대한 자세한 설명은 PCoIP 보안 설정 구성 그룹 정책 대화 상자에 나와 있습니다.

PCoIP 보안 설정을 구성하는 방법

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. PCoIP 보안 설정 구성 설정을 엽니다.
4. PCoIP 보안 설정 구성 대화 상자에서 활성화됨을 선택합니다. 스트리밍 트래픽의 기본 암호화를 256비트로 설정하려면 PCoIP 데이터 암호화 암호 옵션으로 이동하여 AES-256-GCM 전용을 선택합니다.
5. (선택 사항) TLS 보안 모드 설정을 조정한 다음 차단하려는 모든 암호 그룹을 나열합니다. 이러한 설정에 대한 자세한 내용은 PCoIP 보안 설정 구성 대화 상자에 제공된 설명을 참조하세요.
6. 확인을 선택합니다.

7. 그룹 정책 설정 변경은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

U2F용 YubiKey USB 리디렉션 활성화

> **Note**
>
> Amazon은 WorkSpaces 현재 YubiKey U2F에 대해서만 USB 리디렉션을 지원합니다. 다른 유형의 USB 디바이스는 리디렉션될 수 있지만 지원되지 않고 제대로 작동하지 않을 수 있습니다.

U2F용 USB 리디렉션을 활성화하려면 YubiKey

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. PCoIP 세션에서 USB 활성화/비활성화 설정을 엽니다.
4. 활성화됨을 선택한 다음 확인을 선택합니다.
5. PCoIP USB 허용되는 디바이스 규칙 및 허용되지 않는 디바이스 규칙 구성 설정을 엽니다.
6. 활성화됨을 선택하고 USB 권한 부여 테이블 입력(규칙 최대 10개)에서 USB 디바이스 허용 목록 규칙을 구성합니다.

   - 권한 부여 규칙 - 110500407. 이 값은 제공업체 ID(VID)와 제품 ID(PID)의 조합입니다. VID/PID 조합의 형식은 1xxxxyyyyy입니다. 여기서 xxxx는 16진수 형식의 VID이고 yyyyy는 16진수 형식의 PID입니다. 이 예시에서 1050은 VID이고 0407은 PID입니다. USB 값에 대한 자세한 내용은 YubiKey USB ID 값을 참조하십시오YubiKey .

7. USB 권한 부여 테이블 입력(규칙 최대 10개)에서 USB 디바이스 차단 목록 규칙을 구성합니다.

   - 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 미부여 규칙에 대한 자세한 내용은 Teradici PCoIP Standard Agent for Windows를 참조하세요.

8. 확인을 선택합니다.
9. 그룹 정책 설정 변경은 에 대한 다음 그룹 정책 업데이트 이후 WorkSpace 및 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
   - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에 **`gpupdate /force`**를 입력합니다.

설정이 적용된 후에는 USB 디바이스 규칙 설정을 통해 제한을 WorkSpaces 구성하지 않는 한 지원되는 모든 USB 디바이스를 리디렉션할 수 있습니다.

Kerberos 티켓에 최대 수명 설정

WorkSpacesWindows의 내 정보 저장 기능을 사용하지 않도록 설정하지 않은 경우 WorkSpace 사용자는 WorkSpaces 클라이언트 응용 프로그램의 내 정보 저장 또는 로그인 유지 확인란을 사용하여 자격 증명을 저장할 수 있습니다. 이 기능을 사용하면 클라이언트 응용 프로그램이 실행 중인 WorkSpaces 상태에서 사용자가 자신의 컴퓨터에 쉽게 연결할 수 있습니다. 자격 증명은 Kerberos 티켓의 최대 수명까지 안전하게 캐시됩니다.

AD Connector 디렉터리를 WorkSpace 사용하는 경우 Microsoft Windows 설명서의 사용자 티켓의 최대 수명에 나와 있는 단계에 따라 그룹 정책을 통해 WorkSpaces 사용자에 대한 Kerberos 티켓의 최대 수명을 수정할 수 있습니다.

Remember Me(자격 증명 저장) 기능을 활성화 또는 비활성화하려면 사용자를 위한 셀프 서비스 WorkSpace 관리 기능 활성화 단원을 참조하십시오.

인터넷 액세스를 위한 디바이스 프록시 서버 설정 구성

기본적으로 WorkSpaces 클라이언트 응용 프로그램은 HTTPS (포트 443) 트래픽에 대해 장치 운영 체제 설정에 지정된 프록시 서버를 사용합니다. Amazon WorkSpaces 클라이언트 애플리케이션은 업데이트, 등록 및 인증에 HTTPS 포트를 사용합니다.

> **Note**
>
> 로그인 보안 인증 정보를 통한 인증이 필요한 프록시 서버는 지원되지 않습니다.

Microsoft 설명서의 장치 프록시 및 인터넷 연결 설정 구성의 단계에 따라 그룹 정책을 WorkSpaces 통해 Windows용 장치 프록시 서버 설정을 구성할 수 있습니다.

WorkSpaces Windows 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces macOS 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces Web Access 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

데스크톱 트래픽 프록시 사용

WorkSpacesPCoIP의 경우 데스크톱 클라이언트 애플리케이션은 UDP의 포트 4172 트래픽 (데스크톱 트래픽용) 에 대한 프록시 서버 사용이나 TLS 암호 해독 및 검사를 지원하지 않습니다. 포트 4172에 직접 연결해야 합니다.

WSP의 WorkSpaces 경우 WorkSpaces Windows 클라이언트 애플리케이션 (버전 5.1 이상) 및 macOS 클라이언트 애플리케이션 (버전 5.4 이상) 은 포트 4195 TCP 트래픽에 HTTP 프록시 서버 사용을 지원합니다. TLS 암호 해독 및 검사는 지원되지 않습니다.

WSP는 UDP를 통한 데스크톱 트래픽의 프록시 사용을 지원하지 않습니다. WorkSpacesWindows 및 macOS 데스크톱 클라이언트 애플리케이션과 WSP 웹 액세스만 TCP 트래픽에 대한 프록시 사용을 지원합니다.

> **Note**
>
> 프록시 서버를 사용하도록 선택하면 클라이언트 애플리케이션이 WorkSpaces 서비스에 보내는 API 호출도 프록시됩니다. API 호출과 데스크톱 트래픽 모두 동일한 프록시 서버를 통과해야 합니다.

프록시 서버 사용에 대한 권장 사항

WorkSpaces 데스크톱 트래픽에는 프록시 서버를 사용하지 않는 것이 좋습니다.

Amazon WorkSpaces 데스크톱 트래픽은 이미 암호화되어 있으므로 프록시는 보안을 향상시키지 않습니다. 프록시는 네트워크 경로의 추가 홉을 나타내며, 지연 시간을 유발하여 스트리밍 품질에 영향을 미칠 수 있습니다. 프록시 크기가 데스크톱 스트리밍 트래픽을 처리하기에 적절하지 않은 경우 프록시는 처리량을 감소시킬 수도 있습니다. 또한 대부분의 프록시는 장기 실행 WebSocket (TCP) 연결을 지원하도록 설계되지 않았으므로 스트리밍 품질 및 안정성에 영향을 미칠 수 있습니다.

프록시를 사용해야 하는 경우 스트리밍 품질 및 응답성에 부정적인 영향을 미칠 수 있는 네트워크 지연 시간이 추가되지 않도록 프록시 서버를 가능한 한 WorkSpace 클라이언트와 가까운 곳에, 가급적이면 동일한 네트워크에 위치시키십시오.

WorkSpaces Amazon용 Zoom 미팅 미디어 플러그인 지원 활성화

Zoom은 Zoom VDI 플러그인을 사용하여 WSP 및 PCoIP Windows 기반의 WorkSpaces 최적화된 실시간 커뮤니케이션을 지원합니다. 직접 클라이언트 커뮤니케이션을 통해 화상 통화는 클라우드 기반 가상 데스크톱을 우회하여 사용자 사무실 내에서 회의가 진행될 때 로컬과 비슷한 Zoom 경험을 제공할 수 있습니다. WorkSpace

WSP용 Zoom 미팅 미디어 플러그인을 활성화합니다.

Zoom VDI 구성 요소를 설치하기 전에 Zoom 최적화를 지원하도록 WorkSpaces 구성을 업데이트하세요.

필수 조건

플러그인을 사용하기 전에 다음 요구 사항이 충족되는지 확인하세요.

- 윈도우 WorkSpaces 클라이언트 버전 5.10.0 이상, Zoom VDI 플러그인 버전 5.17.10+
- 귀하의 — Zoom VDI 미팅 클라이언트 버전 5.17.10+ WorkSpaces 내에서

시작하기 전 준비 사항

1. 확장 그룹 정책 설정을 활성화합니다. 자세한 정보는 WSP에 확장 구성을 참조하세요.
2. 자동 재연결 그룹 정책 설정을 사용하지 않도록 설정합니다. 자세한 정보는 WSP에 세션 재개 제한 시간 설정을 참조하세요.

Zoom 구성 요소 설치

Zoom 최적화를 활성화하려면 Zoom에서 제공하는 두 가지 구성 요소를 Windows에 설치하세요 WorkSpaces. 자세한 내용은 Amazon Web Services용 Zoom 사용을 참조하십시오.

1. Zoom VDI Meeting 클라이언트 버전 5.12.6+를 귀사 내에 설치하십시오. WorkSpace
2. Zoom VDI 플러그인 (윈도우 유니버설 인스톨러) 버전 5.12.6+를 설치된 클라이언트에 설치합니다. WorkSpace
3. VDI 플러그인 상태가 Zoom VDI 클라이언트 내에서 연결됨으로 표시되는지 확인하여 플러그인이 Zoom 트래픽을 최적화하고 있는지 확인하세요. 자세한 내용은 Amazon WorkSpaces 최적화 확인 방법을 참조하십시오.

PCoIP용 Zoom 미팅 미디어 플러그인 활성화

Active Directory에 대한 관리자 권한이 있는 사용자는 그룹 정책 개체 (GPO) 를 사용하여 레지스트리 키를 생성할 수 있습니다. 이렇게 하면 사용자가 강제 업데이트를 통해 도메인 WorkSpaces 내의 모든 Windows에 레지스트리 키를 보낼 수 있습니다. 또는 관리자 권한이 있는 사용자가 WorkSpaces 호스트에 개별적으로 레지스트리 키를 설치할 수도 있습니다.

필수 조건

플러그인을 사용하기 전에 다음 요구 사항이 충족되는지 확인하십시오.

- 윈도우 WorkSpaces 클라이언트 버전 5.4.0 이상, Zoom VDI 플러그인 버전 5.12.6 이상
- 사용 중인 Zoom VDI 미팅 클라이언트 버전 5.12.6+ 내에서 사용할 수 있습니다. WorkSpaces

Windows 호스트에서 레지스트리 키를 생성하십시오. WorkSpaces

Windows WorkSpaces 호스트에 레지스트리 키를 만들려면 다음 절차를 완료하십시오. Windows에서 Zoom을 사용하려면 레지스트리 키가 필요합니다 WorkSpaces.

1. Windows 레지스트리 편집기를 관리자 권한으로 엽니다.
2. `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`로 이동합니다.
3. Extension 키가 없는 경우 마우스 오른쪽 버튼을 클릭하고 새로 만들기 > 키를 선택하고 이름을 Extension으로 지정합니다.
4. 새 Extension 키에서 마우스 오른쪽 버튼을 클릭하고 새로 만들기 > DWORD를 선택하고 이름을 enable로 지정합니다. 이름은 소문자여야 합니다.
5. 새 DWORD를 선택하고 값을 1로 변경합니다.
6. 컴퓨터를 재부팅하여 프로세스를 완료합니다.
7. WorkSpaces 호스트에서 최신 Zoom VDI 클라이언트를 다운로드하여 설치합니다. WorkSpaces 클라이언트 (5.4 이상) 에서 Amazon용 최신 Zoom VDI 클라이언트 플러그인을 다운로드하여 설치

합니다. WorkSpaces 자세한 내용은 Zoom 지원 웹 사이트의 VDI releases and downloads를 참조하세요.

Zoom을 실행하여 영상 통화를 시작합니다.

문제 해결

Windows용 Zoom 문제를 해결하려면 다음 작업을 완료하세요. WorkSpaces

- 레지스트리 키 활성화가 올바르게 적용되었는지 확인하십시오.
- `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`로 이동합니다. `wse_core_dll`을 확인해야 합니다.
- 호스트와 클라이언트의 버전이 정확하고 동일한지 확인합니다.

문제가 계속되면 AWS Support 센터를 AWS Support 통해 문의하세요.

다음 예시를 사용하여 디렉터리 관리자로 GPO를 적용할 수 있습니다.

- Wse.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
```

```
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
```

```
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

아마존 리눅스 관리 WorkSpaces

Windows와 WorkSpaces 마찬가지로 Amazon WorkSpaces Linux는 도메인에 가입되어 있으므로 Active Directory 사용자 및 그룹을 사용하여 다음을 수행할 수 있습니다.

- 아마존 리눅스 관리 WorkSpaces
- 사용자에게 WorkSpaces 액세스 권한 제공

Linux 인스턴스는 그룹 정책을 준수하지 않으므로 구성 관리 솔루션을 사용하여 정책을 배포하고 적용하는 것이 좋습니다. 예를 들어, AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise 또는 Ansible을 사용할 수 있습니다.

> **Note**
>
> Amazon WorkSpaces Linux에서는 로컬 프린터 리디렉션을 사용할 수 없습니다.

Amazon Linux에서의 WorkSpaces 스트리밍 프로토콜 (WSP) 동작 제어 WorkSpaces

WSP의 동작은 `/etc/wsp/` 디렉터리에 있는 `wsp.conf` 파일의 구성 설정에 의해 제어됩니다. 정책에 변경 사항을 배포하고 적용하려면 Amazon Linux를 지원하는 구성 관리 솔루션을 사용하세요. 에이전트가 시작되면 모든 변경 사항이 적용됩니다.

> **Note**
>
> - `wsp.conf`파일을 잘못 변경하거나 지원되지 않는 변경을 수행한 경우 정책 변경 사항이 서버에서 새로 설정된 연결에 적용되지 않을 수 있습니다. WorkSpace

- WSP 기반 Amazon WorkSpaces Linux 번들에는 현재 다음과 같은 제한 사항이 있습니다.
  - 현재는 AWS GovCloud (미국 서부) 및 AWS GovCloud (미국 동부) 에서만 사용할 수 있습니다.
  - 비디오 입력은 지원되지 않습니다.
  - 화면 잠금 시 세션 연결 해제는 지원되지 않습니다.

다음 섹션에서는 특정 기능을 활성화 또는 비활성화하는 방법에 대해 설명합니다.

WSP 아마존 리눅스용 클립보드 리디렉션 구성 WorkSpaces

기본적으로 클립보드 리디렉션을 지원합니다 WorkSpaces . 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 구성하세요. 이 설정은 연결을 끊었다가 다시 연결할 때 적용됩니다. WorkSpace

WSP Amazon Linux용 클립보드 리디렉션을 구성하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.
```
clipboard = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

`enabled` - 클립보드 리디렉션이 양방향으로 활성화됩니다(기본값).

`disabled` - 클립보드 리디렉션은 양방향으로 비활성화됩니다.

`paste-only` - 클립보드 리디렉션이 활성화되지만 로컬 클라이언트 디바이스에서 콘텐츠를 복사하여 원격 호스트 데스크톱에 붙여넣는 동작만 허용됩니다.

`copy-only` - 클립보드 리디렉션이 활성화되지만 원격 호스트 데스크톱에서 콘텐츠를 복사하여 로컬 클라이언트 디바이스에 붙여넣는 동작만 허용됩니다.

WSP Amazon Linux의 오디오 입력 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 오디오 입력 리디렉션을 지원합니다 WorkSpaces . 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 비활성화하세요. 이 설정은 연결을 끊었다가 다시 연결할 때 적용됩니다. WorkSpace

WSP Amazon Linux의 오디오 입력 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. 파일 끝부분에 다음 행을 추가합니다.

   ```
   audio-in = X
   ```

   여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

   `enabled` - 오디오 입력 리디렉션이 활성화됩니다(기본값).

   `disabled` - 오디오 입력 리디렉션이 비활성화됩니다.

WSP Amazon Linux의 시간대 리디렉션을 활성화 또는 비활성화합니다. WorkSpaces

기본적으로 Workspace 내의 시간은 연결에 사용되는 클라이언트의 시간대를 미러링하도록 설정됩니다. WorkSpace 이 동작은 시간대 리디렉션을 통해 제어됩니다. 다음과 같은 이유로 시간대 리디렉션을 해제할 수 있습니다.

- 회사가 모든 직원이 특정 시간대에서 일하기를 원합니다(일부 직원이 다른 시간대에 있더라도).
- 특정 시간대의 특정 시간에 WorkSpace 실행되도록 스케줄링된 작업이 a에 있습니다.
- 여행을 많이 하는 사용자는 일관성과 개인 취향을 위해 한 시간대에 WorkSpaces 머물기를 원합니다.

필요한 경우 WSP 구성 파일을 사용하여 이 기능을 구성하세요. 이 설정은 연결을 끊었다가 다시 연결한 후에 적용됩니다. WorkSpace

WSP Amazon Linux의 시간대 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
   ```

2. 파일 끝부분에 다음 행을 추가합니다.

   ```
   timezone_redirect= X
   ```

   여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

   enabled - 시간대 리디렉션이 활성화됩니다(기본값).

   disabled - 시간대 리디렉션이 비활성화됩니다.

아마존 리눅스에서의 PCoIP 에이전트 동작 제어 WorkSpaces

PCoIP 에이전트의 동작은 `/etc/pcoip-agent/` 디렉터리에 있는 `pcoip-agent.conf` 파일의 구성 설정에 의해 제어됩니다. 정책에 변경 사항을 배포하고 적용하려면 Amazon Linux를 지원하는 구성 관리 솔루션을 사용하세요. 에이전트가 시작되면 모든 변경 사항이 적용됩니다. 에이전트를 다시 시작하면 모든 개방 연결이 종료되고 창 관리자가 다시 시작됩니다. 변경 사항을 적용하려면 를 재부팅하는 것이 좋습니다. WorkSpace

> **Note**
>
> `pcoip-agent.conf`파일을 잘못 변경하거나 지원되지 않는 변경을 한 경우 작업이 중단될 수 있습니다 WorkSpace . 작업이 WorkSpace 중단되면 WorkSpace 사용 중인 SSH에 연결하여 변경 내용을 롤백하거나 다시 빌드해야 할 수 있습니다. WorkSpace

다음 섹션에서는 특정 기능을 활성화 또는 비활성화하는 방법에 대해 설명합니다. 사용 가능한 설정의 전체 목록을 보려면 모든 Amazon Linux의 `man pcoip-agent.conf` 터미널에서 WorkSpace 실행하십시오.

PCoIP 아마존 리눅스용 클립보드 리디렉션을 구성합니다 WorkSpaces

기본적으로 클립보드 리디렉션을 지원합니다. WorkSpaces 필요한 경우 PCoIP 에이전트 구성을 사용하여 이 기능을 비활성화하십시오. 이 설정은 를 재부팅할 때 적용됩니다. WorkSpace

PCoIP 아마존 리눅스용 클립보드 리디렉션을 구성하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `pcoip-agent.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 파일 끝부분에 다음 행을 추가합니다.

```
pcoip.server_clipboard_state = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

0 - 클립보드 리디렉션이 양방향으로 비활성화됩니다.

1 - 클립보드 리디렉션이 양방향으로 활성화됩니다.

2 - 클라이언트에서 에이전트로만 클립보드 리디렉션이 활성화됩니다(로컬 클라이언트 디바이스에서 원격 호스트 데스크톱으로만 복사 후 붙여넣기가 허용됨).

3 - 에이전트에서 클라이언트로만 클립보드 리디렉션이 활성화됩니다(원격 호스트 데스크톱에서 로컬 클라이언트 디바이스로만 복사 후 붙여넣기가 허용됨).

> **Note**
>
> 클립보드 리디렉션은 가상 채널로 구현됩니다. 가상 채널을 비활성화하면 클립보드 리디렉션이 작동하지 않습니다. 가상 채널을 활성화하려면 Teradici 설명서의 CoIP Virtual Channels를 참조하세요.

PCoIP Amazon Linux에 대한 오디오 입력 리디렉션을 활성화 또는 비활성화합니다. WorkSpaces

기본적으로 오디오 입력 리디렉션을 지원합니다. WorkSpaces 필요한 경우 PCoIP 에이전트 구성을 사용하여 이 기능을 비활성화하십시오. 이 설정은 를 재부팅할 때 적용됩니다. WorkSpace

PCoIP Amazon Linux에 대한 오디오 입력 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `pcoip-agent.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 파일 끝부분에 다음 행을 추가합니다.

```
pcoip.enable_audio = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

0 - 오디오 입력 리디렉션이 비활성화됩니다.

1 - 오디오 입력 리디렉션이 활성화됩니다.

PCoIP Amazon Linux에 대한 시간대 리디렉션을 활성화 또는 비활성화합니다. WorkSpaces

기본적으로 Workspace 내의 시간은 연결에 사용되는 클라이언트의 시간대를 미러링하도록 설정됩니다. WorkSpace 이 동작은 시간대 리디렉션을 통해 제어됩니다. 다음과 같은 이유로 시간대 리디렉션을 해제할 수 있습니다.

- 회사가 모든 직원이 특정 시간대에서 일하기를 원합니다(일부 직원이 다른 시간대에 있더라도).
- 특정 시간대의 특정 시간에 WorkSpace 실행되도록 스케줄링된 작업이 a에 있습니다.
- 여행을 많이 하는 사용자는 일관성과 개인 취향을 위해 한 시간대에 WorkSpaces 머물기를 원합니다.

WorkSpacesLinux에 필요한 경우 PCoIP Agent conf를 사용하여 이 기능을 비활성화할 수 있습니다. 이 설정은 를 재부팅할 때 적용됩니다. WorkSpace

PCoIP Amazon Linux에 대한 시간대 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `pcoip-agent.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 파일 끝부분에 다음 행을 추가합니다.

```
pcoip.enable_timezone_redirect= X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

0 - 시간대 리디렉션이 비활성화됩니다.

1 - 시간대 리디렉션이 활성화됩니다.

아마존 리눅스 WorkSpaces 관리자에게 SSH 액세스 권한 부여

기본적으로 도메인 관리자 그룹의 할당된 사용자 및 계정만 SSH를 사용하여 Amazon WorkSpaces Linux에 연결할 수 있습니다.

Active Directory에서 Amazon Linux 관리자를 위한 전담 WorkSpaces 관리자 그룹을 생성하는 것이 좋습니다.

Linux_Workspaces_Admins Active Directory 그룹의 구성원에 대해 sudo 액세스를 활성화하려면

1. 다음 예제와 같이 `visudo`를 사용하여 `sudoers` 파일을 편집합니다.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. 다음 행을 추가합니다.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

전용 관리자 그룹을 생성한 후에 이 단계에 따라 그룹 구성원에 대한 로그인을 활성화합니다.

Linux_ WorkSpaces _Admins 액티브 디렉터리 그룹 구성원의 로그인을 활성화하려면

1. 승격된 권한으로 `/etc/security/access.conf`를 편집합니다.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 다음 행을 추가합니다.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

SSH 연결을 활성화하는 방법에 대한 자세한 내용은 리눅스용 SSH 연결 활성화 WorkSpaces 단원을 참조하십시오.

Amazon Linux용 기본 셸 재정의 WorkSpaces

WorkSpacesLinux용 기본 셸을 재정의하려면 사용자 파일을 편집하는 것이 좋습니다. `~/.bashrc` 예를 들어 `Bash` 셸 대신 `Z shell`을 사용하려면 다음 줄을 `/home/username/.bashrc`에 추가합니다.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 변경한 후에는 다시 WorkSpace 부팅하거나 연결을 끊을 필요 없이 에서 로그아웃한 다음 다시 로그인해야 변경 사항이 적용됩니다. WorkSpace

무단 액세스로부터 사용자 지정 리포지토리 보호

사용자 지정 리포지토리에 대한 액세스를 제어하려면 암호를 사용하는 것보다 Amazon Virtual Private Cloud(VPC)에 내장된 보안 기능을 사용하는 것이 좋습니다. 예를 들어, 네트워크 액세스 제어 목록(ACL)과 보안 그룹을 사용합니다. 이러한 기능에 대한 자세한 내용은 Amazon VPC 사용 설명서의 보안을 참조하세요.

리포지토리를 보호하기 위해 암호를 사용해야 하는 경우 Fedora 설명서의 Repository Definition Files에서처럼 `yum` 리포지토리 정의 파일을 생성해야 합니다.

Amazon Linux Extras Library 리포지토리 사용

Amazon Linux를 사용하면 Extras Library를 사용하여 인스턴스에 애플리케이션 및 소프트웨어 업데이트를 설치할 수 있습니다. Extras Library 사용에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서에서 Extras Library(Amazon Linux)를 참조하세요.

> **Note**
>
> Amazon Linux 리포지토리를 사용하는 경우 Amazon WorkSpaces Linux가 인터넷에 액세스할 수 있거나 이 리포지토리와 기본 Amazon Linux 리포지토리에 대한 가상 사설 클라우드 (VPC) 엔드포인트를 구성해야 합니다. 자세한 설명은 귀하의 인터넷 액세스 제공 WorkSpace 섹션을 참조하세요.

Linux에서는 인증에 스마트 카드를 사용합니다. WorkSpaces

Linux WorkSpaces 온 WorkSpaces 스트리밍 프로토콜 (WSP) 번들을 사용하면 CAC (공용 액세스 카드) 및 PIV (개인 신원 확인) 스마트 카드를 인증에 사용할 수 있습니다. 자세한 설명은 인증에 스마트 카드 사용 섹션을 참조하세요.

인터넷 액세스를 위한 디바이스 프록시 서버 설정 구성

기본적으로 WorkSpaces 클라이언트 애플리케이션은 HTTPS (포트 443) 트래픽에 대한 장치 운영 체제 설정에 지정된 프록시 서버를 사용합니다. Amazon WorkSpaces 클라이언트 애플리케이션은 업데이트, 등록 및 인증에 HTTPS 포트를 사용합니다.

> **Note**
>
> 로그인 보안 인증 정보를 통한 인증이 필요한 프록시 서버는 지원되지 않습니다.

Microsoft 설명서의 장치 프록시 및 인터넷 연결 설정 구성의 단계에 따라 그룹 정책을 WorkSpaces 통해 Linux용 장치 프록시 서버 설정을 구성할 수 있습니다.

WorkSpaces Windows 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces macOS 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces Web Access 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

데스크톱 트래픽 프록시 사용

WorkSpacesPCoIP의 경우 데스크톱 클라이언트 애플리케이션은 UDP의 포트 4172 트래픽 (데스크톱 트래픽용) 에 대한 프록시 서버 사용이나 TLS 암호 해독 및 검사를 지원하지 않습니다. 포트 4172에 직접 연결해야 합니다.

WSP의 WorkSpaces 경우 WorkSpaces Windows 클라이언트 애플리케이션 (버전 5.1 이상) 및 macOS 클라이언트 애플리케이션 (버전 5.4 이상) 은 포트 4195 TCP 트래픽에 HTTP 프록시 서버 사용을 지원합니다. TLS 암호 해독 및 검사는 지원되지 않습니다.

WSP는 UDP를 통한 데스크톱 트래픽의 프록시 사용을 지원하지 않습니다. WorkSpaces Windows 및 macOS 데스크톱 클라이언트 애플리케이션과 WSP 웹 액세스만 TCP 트래픽에 대한 프록시 사용을 지원합니다.

> **Note**
>
> 프록시 서버를 사용하도록 선택하면 클라이언트 애플리케이션이 WorkSpaces 서비스에 보내는 API 호출도 프록시됩니다. API 호출과 데스크톱 트래픽 모두 동일한 프록시 서버를 통과해야 합니다.

프록시 서버 사용에 대한 권장 사항

WorkSpaces 데스크톱 트래픽에는 프록시 서버를 사용하지 않는 것이 좋습니다.

Amazon WorkSpaces 데스크톱 트래픽은 이미 암호화되어 있으므로 프록시는 보안을 향상시키지 않습니다. 프록시는 네트워크 경로의 추가 홉을 나타내며, 지연 시간을 유발하여 스트리밍 품질에 영향을 미칠 수 있습니다. 프록시 크기가 데스크톱 스트리밍 트래픽을 처리하기에 적절하지 않은 경우 프록시는 처리량을 감소시킬 수도 있습니다. 또한 대부분의 프록시는 장기 실행 WebSocket (TCP) 연결을 지원하도록 설계되지 않았으므로 스트리밍 품질 및 안정성에 영향을 미칠 수 있습니다.

프록시를 사용해야 하는 경우 스트리밍 품질 및 응답성에 부정적인 영향을 미칠 수 있는 네트워크 지연 시간이 추가되지 않도록 프록시 서버를 가능한 한 WorkSpace 클라이언트와 가까운 곳에, 가급적이면 동일한 네트워크에 위치시키십시오.

우분투 관리 WorkSpaces

Windows 및 Amazon WorkSpaces Linux와 마찬가지로 WorkSpaces 우분투는 도메인에 가입되어 있으므로 Active Directory 사용자 및 그룹을 사용하여 다음을 수행할 수 있습니다.

- 우분투 관리 WorkSpaces
- 사용자에게 액세스 권한 제공 WorkSpaces

ADSys를 사용하여 그룹 WorkSpaces 정책으로 Ubuntu를 관리할 수 있습니다. 자세한 내용은 Ubuntu Active Directory integration FAQ를 참조하세요. Landscape 및 Ansible과 같은 다른 구성 및 관리 솔루션도 사용할 수 있습니다.

WorkSpaces 우분투에서의 스트리밍 프로토콜 (WSP) 동작 제어 WorkSpaces

WSP의 동작은 /etc/wsp/ 디렉터리에 있는 wsp.conf 파일의 구성 설정에 의해 제어됩니다. 정책에 변경 사항을 배포하고 적용하려면 Ubuntu를 지원하는 구성 관리 솔루션을 사용하세요. 에이전트가 시작되면 모든 변경 사항이 적용됩니다.

> **Note**
>
> 올바르지 않거나 지원되지 않는 변경을 한 경우 새로 설정된 사용자 연결에 wsp.conf 정책이 적용되지 않을 수 있습니다. WorkSpace

다음 섹션에서는 특정 기능을 활성화 또는 비활성화하는 방법에 대해 설명합니다.

Ubuntu의 클립보드 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 클립보드 리디렉션을 지원합니다. WorkSpaces 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 비활성화하세요.

Ubuntu의 클립보드 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 wsp.conf 파일을 엽니다.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. [policies] 그룹 끝부분에 다음 행을 추가합니다.

   ```
   clipboard = X
   ```

   여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

   enabled - 클립보드 리디렉션이 양방향으로 활성화됩니다(기본값).

   disabled - 클립보드 리디렉션이 양방향으로 비활성화됩니다.

   paste-only - 클립보드 리디렉션이 활성화되며 로컬 클라이언트 디바이스에서 콘텐츠를 복사하여 원격 호스트 데스크톱에 붙여넣는 동작만 허용됩니다.

paste-only - 클립보드 리디렉션이 활성화되며 원격 호스트 데스크톱에서 콘텐츠를 복사하여 로컬 클라이언트 디바이스에 붙여넣는 동작만 허용됩니다.

Ubuntu의 오디오 입력 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 오디오 입력 리디렉션을 지원합니다. WorkSpaces 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 비활성화하세요.

Ubuntu의 오디오 입력 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` 그룹 끝부분에 다음 행을 추가합니다.

```
audio-in = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

enabled - 오디오 입력 리디렉션이 활성화됩니다(기본값).

disabled - 오디오 입력 리디렉션이 비활성화됩니다.

Ubuntu의 비디오 입력 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 비디오 입력 리디렉션을 지원합니다. WorkSpaces 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 비활성화하세요.

Ubuntu의 비디오 입력 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` 그룹 끝부분에 다음 행을 추가합니다.

```
video-in = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

enabled - 비디오 입력 리디렉션이 활성화됩니다(기본값).

disabled - 비디오 입력 리디렉션이 비활성화됩니다.

Ubuntu의 시간대 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 Workspace 내의 시간은 연결에 사용되는 클라이언트의 시간대를 미러링하도록 설정됩니다. WorkSpace 이 동작은 시간대 리디렉션을 통해 제어됩니다. 다음과 같은 이유로 시간대 리디렉션을 해제할 수 있습니다.

- 회사가 모든 직원이 특정 시간대에서 일하기를 원합니다(일부 직원이 다른 시간대에 있더라도).
- 특정 시간대의 특정 시간에 WorkSpace 실행되도록 스케줄링된 작업이 a에 있습니다.
- 사용자는 여행을 많이 다니며 일관성과 개인 취향을 위해 한 시간대에 WorkSpaces 머물기를 원합니다.

필요한 경우 WSP 구성 파일을 사용하여 이 기능을 구성하세요.

Ubuntu의 시간대 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` 그룹 끝부분에 다음 행을 추가합니다.

```
timezone-redirection = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

enabled - 시간대 리디렉션이 활성화됩니다(기본값).

disabled - 시간대 리디렉션이 비활성화됩니다.

Ubuntu의 프린터 리디렉션 활성화 또는 비활성화 WorkSpaces

기본적으로 프린터 리디렉션을 WorkSpaces 지원합니다. 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 비활성화하세요.

Ubuntu의 프린터 리디렉션을 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` 그룹 끝부분에 다음 행을 추가합니다.

```
remote-printing = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

enabled - 프린터 리디렉션이 활성화됩니다(기본값).

disabled - 프린터 리디렉션이 비활성화됩니다.

WSP에서 화면 잠금 시 세션 연결 해제 활성화 또는 비활성화

잠금 화면이 감지될 때 사용자가 세션을 종료할 수 있도록 화면 잠금에서 WorkSpaces 세션 연결 해제를 활성화하십시오. WorkSpaces 클라이언트에 다시 연결하려면 활성화된 인증 유형에 따라 사용자가 암호 또는 스마트 카드를 사용하여 자신을 인증할 수 있습니다. WorkSpaces

기본적으로 화면 잠금 시 세션 연결 해제를 WorkSpaces 지원하지 않습니다. 필요한 경우 WSP 구성 파일을 사용하여 이 기능을 활성화하세요.

Ubuntu의 화면 잠금에서 세션 연결 해제를 활성화 또는 비활성화하려면 WorkSpaces

1. 다음 명령을 사용하여 승격된 권한으로 편집기에서 `wsp.conf` 파일을 엽니다.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` 그룹 끝부분에 다음 행을 추가합니다.

```
disconnect-on-lock = X
```

여기에서 *X*에 대해 가능한 값은 다음과 같습니다.

enabled - 화면 잠금 시 연결 해제가 활성화됩니다.

disabled - 화면 잠금 시 연결 해제가 비활성화됩니다(기본값).

우분투 관리자에게 SSH 액세스 권한 부여 WorkSpaces

기본적으로 Domain Admins 그룹의 할당된 사용자 및 계정만 SSH를 사용하여 WorkSpaces Ubuntu에 연결할 수 있습니다. 다른 사용자와 계정이 SSH를 WorkSpaces 사용하여 우분투에 연결할 수 있게 하려면 Active Directory에서 Ubuntu 관리자를 위한 전용 관리자 그룹을 만드는 것이 좋습니다. WorkSpaces

`Linux_WorkSpaces_Admins` Active Directory 그룹의 구성원에 대해 sudo 액세스를 활성화하는 방법

1. 다음 예제와 같이 `visudo`를 사용하여 `sudoers` 파일을 편집합니다.

```
[username@workspace-id ~]$ sudo visudo
```

2. 다음 행을 추가합니다.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

전용 관리자 그룹을 생성한 후에 이 단계에 따라 그룹 구성원에 대한 로그인을 활성화합니다.

`Linux_WorkSpaces_Admins` Active Directory 그룹의 구성원에 대해 로그인을 활성화하는 방법

1. 승격된 권한으로 `/etc/security/access.conf`를 편집합니다.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 다음 행을 추가합니다.

```
+:(Linux_WorkSpaces_Admins):ALL
```

Ubuntu를 WorkSpaces 사용하면 SSH 연결을 위한 사용자 이름을 지정할 때 도메인 이름을 추가할 필요가 없으며 기본적으로 암호 인증은 비활성화됩니다. SSH를 통해 연결하려면 `$HOME/.ssh/authorized_keys` WorkSpace Ubuntu에서 SSH 공개 키를 추가하거나 설정하도록 편집해야 합니다. `/etc/ssh/sshd_config` PasswordAuthentication `yes` SSH 연결을 활성화하는 방법에 대한 자세한 내용은 Linux용 SSH 연결 활성화를 참조하십시오. WorkSpaces

Ubuntu의 기본 셸을 재정의하십시오. WorkSpaces

Ubuntu의 기본 셸을 재정의하려면 사용자 WorkSpaces 파일을 편집하는 것이 좋습니다. `~/.bashrc` 예를 들어 `Bash` 셸 대신 `Z shell`을 사용하려면 다음 줄을 `/home/username/.bashrc`에 추가합니다.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 이렇게 변경한 후에는 다시 WorkSpace 부팅하거나 연결을 끊을 필요 없이 로그아웃한 다음 다시 로그인해야 변경 사항이 적용됩니다. WorkSpace

인터넷 액세스를 위한 디바이스 프록시 서버 설정 구성

기본적으로 WorkSpaces 클라이언트 응용 프로그램은 HTTPS (포트 443) 트래픽에 대해 장치 운영 체제 설정에 지정된 프록시 서버를 사용합니다. Amazon WorkSpaces 클라이언트 애플리케이션은 업데이트, 등록 및 인증에 HTTPS 포트를 사용합니다.

> **Note**
>
> 로그인 보안 인증 정보를 통한 인증이 필요한 프록시 서버는 지원되지 않습니다.

Microsoft 설명서의 장치 프록시 및 인터넷 연결 설정 구성의 단계에 따라 그룹 정책을 WorkSpaces 통해 Ubuntu의 장치 프록시 서버 설정을 구성할 수 있습니다.

WorkSpaces Windows 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces macOS 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

WorkSpaces 웹 액세스 클라이언트 애플리케이션에서 프록시 설정을 구성하는 방법에 대한 자세한 내용은 Amazon WorkSpaces 사용 설명서의 프록시 서버를 참조하십시오.

데스크톱 트래픽 프록시 사용

WorkSpacesPCoIP의 경우 데스크톱 클라이언트 애플리케이션은 UDP의 포트 4172 트래픽 (데스크톱 트래픽용) 에 대한 프록시 서버 사용이나 TLS 암호 해독 및 검사를 지원하지 않습니다. 포트 4172에 직접 연결해야 합니다.

WSP의 WorkSpaces 경우 WorkSpaces Windows 클라이언트 애플리케이션 (버전 5.1 이상) 및 macOS 클라이언트 애플리케이션 (버전 5.4 이상) 은 포트 4195 TCP 트래픽에 HTTP 프록시 서버 사용을 지원합니다. TLS 암호 해독 및 검사는 지원되지 않습니다.

WSP는 UDP를 통한 데스크톱 트래픽의 프록시 사용을 지원하지 않습니다. WorkSpaces Windows 및 macOS 데스크톱 클라이언트 애플리케이션과 WSP 웹 액세스만 TCP 트래픽에 대한 프록시 사용을 지원합니다.

> **Note**
>
> 프록시 서버를 사용하도록 선택하면 클라이언트 애플리케이션이 WorkSpaces 서비스에 보내는 API 호출도 프록시됩니다. API 호출과 데스크톱 트래픽 모두 동일한 프록시 서버를 통과해야 합니다.

프록시 서버 사용에 대한 권장 사항

WorkSpaces 데스크톱 트래픽에는 프록시 서버를 사용하지 않는 것이 좋습니다.

Amazon WorkSpaces 데스크톱 트래픽은 이미 암호화되어 있으므로 프록시는 보안을 향상시키지 않습니다. 프록시는 네트워크 경로의 추가 홉을 나타내며, 지연 시간을 유발하여 스트리밍 품질에 영향을

미칠 수 있습니다. 프록시 크기가 데스크톱 스트리밍 트래픽을 처리하기에 적절하지 않은 경우 프록시는 처리량을 감소시킬 수도 있습니다. 또한 대부분의 프록시는 장기 실행 WebSocket (TCP) 연결을 지원하도록 설계되지 않았으므로 스트리밍 품질 및 안정성에 영향을 미칠 수 있습니다.

프록시를 사용해야 하는 경우 스트리밍 품질 및 응답성에 부정적인 영향을 미칠 수 있는 네트워크 지연 시간이 추가되지 않도록 프록시 서버를 가능한 한 WorkSpace 클라이언트와 가까운 곳에, 가급적이면 동일한 네트워크에 위치시키십시오.

실시간 커뮤니케이션을 WorkSpaces 위한 Amazon 최적화

WorkSpaces Amazon은 Microsoft Teams, Zoom, Webex 등과 같은 통합 커뮤니케이션 (UC) 애플리케이션의 배포를 용이하게 하는 다양한 기술을 제공합니다. 현대 애플리케이션 환경에서 대부분의 UC 애플리케이션은 1:1 채팅방, 협업용 그룹 채팅 채널, 원활한 파일 저장 및 교환, 라이브 이벤트, 웨비나, 브로드캐스트, 대화형 화면 공유 및 제어, 화이트보딩, 오프라인 오디오/비디오 메시징 기능을 비롯한 다양한 기능으로 구성되어 있습니다. 이 기능의 대부분은 추가 미세 조정 또는 개선 없이 표준 WorkSpaces 기능으로 원활하게 사용할 수 있습니다. 하지만 실시간 커뮤니케이션 요소, 특히 one-on-one 통화 및 단체 그룹 회의는 이 규칙의 예외라는 점에 유의할 필요가 있습니다. 이러한 기능을 성공적으로 통합하려면 WorkSpaces 배포 과정에서 집중하고 계획을 세워야 하는 경우가 많습니다.

WorkSpacesAmazon에서 UC 애플리케이션의 실시간 통신 기능 구현을 계획할 때는 세 가지 실시간 통신 (RTC) 구성 모드 중에서 선택할 수 있습니다. 어떤 구성 모드를 사용할지는 사용자에게 제공하려는 특정 애플리케이션과 사용하려는 클라이언트 디바이스에 따라 달라집니다.

이 문서는 Amazon에서 가장 일반적인 UC 애플리케이션에 대한 사용자 경험을 최적화하는 데 중점을 둡니다. WorkSpaces WorkSpaces Core별 최적화에 대해서는 파트너별 설명서를 참조하십시오.

주제

- 미디어 최적화 모드 개요
- 어떤 RTC 최적화 모드를 사용해야 하나요?
- RTC 최적화 가이드

미디어 최적화 모드 개요

사용할 수 있는 미디어 최적화 옵션은 다음과 같습니다.

옵션 1: 미디어 최적화 실시간 통신(미디어 최적화 RTC)

이 모드에서는 타사 UC 및 VoIP 애플리케이션이 WorkSpace 원격에서 실행되고 미디어 프레임워크는 지원되는 클라이언트로 오프로드되어 직접 통신이 가능합니다. WorkSpacesAmazon에서 이 접근 방식을 사용하는 UC 애플리케이션은 다음과 같습니다.

- Zoom 회의
- Cisco Webex 회의

미디어 최적화 RTC 모드가 작동하려면 UC 애플리케이션 공급업체가 DCV Extension SDK와 같은 사용 가능한 소프트웨어 개발 키트 (SDK) 중 하나를 WorkSpaces 사용하여 통합을 개발해야 합니다. 이 모드를 사용하려면 클라이언트 디바이스에 UC 구성 요소를 설치해야 합니다.

이 모드 구성에 대한 자세한 정보는 미디어 최적화 RTC 구성 섹션을 참조하세요.

옵션 2: 세션 내 최적화 실시간 통신(세션 내 최적화 RTC)

이 모드에서는 변경되지 않은 UC 애플리케이션이 에서 실행되어 오디오 및 비디오 트래픽을 WorkSpace 스트리밍 프로토콜을 통해 클라이언트 장치로 전달합니다. WorkSpaces 마이크의 로컬 오디오와 웹캠의 비디오 스트림은 UC 애플리케이션이 소비하는 로 리디렉션됩니다. WorkSpace 이 모드는 광범위한 응용 프로그램 호환성을 제공하고 원격에서 다양한 클라이언트 WorkSpace 플랫폼으로 UC 응용 프로그램을 효율적으로 제공합니다. UC 애플리케이션 구성 요소를 클라이언트 디바이스에 배포할 필요가 없습니다.

이 모드 구성에 대한 자세한 정보는 세션 내 최적화 RTC 구성 섹션을 참조하세요.

옵션 3: 직접 실시간 통신(직접 RTC)

이 모드에서는 에서 작동하는 응용 프로그램이 사용자 책상이나 클라이언트 OS에 있는 실제 또는 가상 전화 세트를 WorkSpace 제어합니다. 그 결과 오디오 트래픽이 사용자 워크스테이션의 실제 전화 또는 클라이언트 디바이스에서 작동하는 가상 전화에서 원격 통화 피어로 직접 전달됩니다. 이 모드에서 작동하는 애플리케이션 중 주목할 만한 사례는 다음과 같습니다.

- 아마존을 위한 아마존 커넥트 최적화 WorkSpaces
- Genesys Cloud WebRTC 미디어 도우미
- Microsoft Teams SIP 게이트웨이
- Microsoft Teams 탁상 전화 및 Teams 디스플레이

- UC 애플리케이션의 다이얼인 또는 '전화 걸기' 기능을 통해 오디오 회의에 참여

이 모드 구성에 대한 자세한 정보는 직접 RTC 구성 섹션을 참조하세요.

어떤 RTC 최적화 모드를 사용해야 하나요?

여러 RTC 최적화 모드를 동시에 사용하거나 대체 수단으로 서로를 보완하도록 설정할 수 있습니다. 예를 들어, Cisco Webex 회의에 미디어 최적화 RTC를 활성화하는 것을 고려해 보세요. 이 구성을 통해 사용자는 데스크톱 클라이언트를 WorkSpace 통해 액세스할 때 최적화된 통신을 경험할 수 있습니다. 그러나 UC 최적화 구성 요소가 없는 공유 인터넷 키오스크에서 Webex에 액세스하는 경우 Webex는 기능을 유지하기 위해 세션 내 최적화 RTC 모드로 원활하게 전환됩니다. 사용자가 여러 UC 애플리케이션을 사용하는 경우 RTC 구성 모드는 고유한 요구 사항에 따라 달라질 수 있습니다.

다음 표는 일반적인 UC 애플리케이션 기능을 나타내며 최상의 결과를 제공하는 RTC 구성 모드를 정의합니다.

기능	직접 RTC	미디어 최적화 RTC	세션 내 최적화 RTC
일대일 채팅	RTC 구성이 필요하지 않음		
그룹 채팅방	RTC 구성이 필요하지 않음		
그룹 오디오 회의	최상급	최상급	좋음
그룹 화상 회의	좋음	최상급	좋음
일대일 음성 통화	최상급	최상급	좋음
일대일 영상 통화	좋음	최상급	좋음
화이트보딩	RTC 구성이 필요하지 않음		
오디오/비디오 클립/메시지	해당 사항 없음	좋음	최상급
파일 공유	해당 사항 없음	UC 애플리케이션에 따라 다름	최상급
화면 공유 및 제어	해당 사항 없음	UC 애플리케이션에 따라 다름	최상급

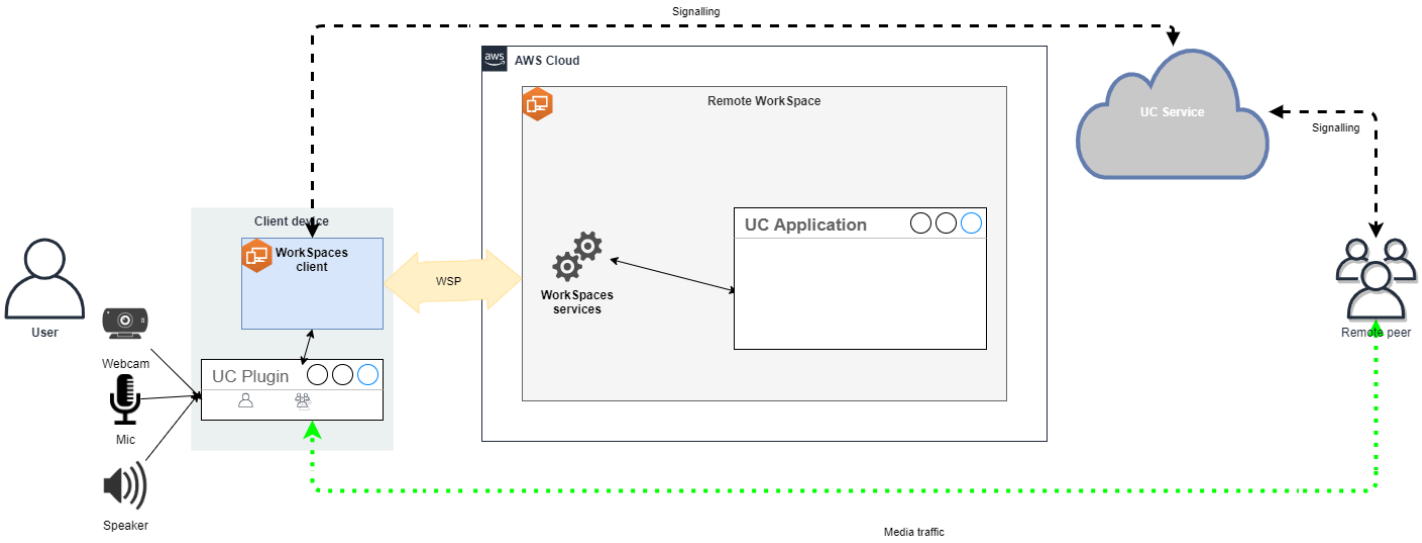
기능	직접 RTC	미디어 최적화 RTC	세션 내 최적화 RTC
웨비나/브로드캐스트 이벤트	해당 사항 없음	좋음	최상급

RTC 최적화 가이드

미디어 최적화 RTC 구성

미디어 최적화 RTC 모드는 UC 애플리케이션 제공업체가 Amazon에서 제공하는 SDK를 사용하여 사용 가능합니다. 이 아키텍처에서는 UC 제공업체가 UC 전용 플러그인 또는 확장을 개발하여 클라이언트에 배포해야 합니다.

DCV Extension SDK와 같은 공개적으로 사용 가능한 옵션과 사용자 지정 비공개 버전을 포함하는 SDK는 내에서 작동하는 UC 애플리케이션 WorkSpace 모듈과 클라이언트 측의 플러그인 사이에 제어 채널을 설정합니다. 일반적으로 이 제어 채널은 클라이언트 확장에 통화를 시작하거나 참여하도록 지시합니다. 클라이언트 측 확장을 통해 통화가 연결되면 UC 플러그인은 마이크의 오디오와 웹캠의 비디오를 캡처한 다음 UC 클라우드 또는 콜 피어로 직접 전송합니다. 수신 오디오는 로컬에서 재생되고 비디오는 원격 클라이언트 UI에 오버레이됩니다. 제어 채널은 통화 상태를 전달하는 역할을 합니다.



Amazon은 WorkSpaces 현재 미디어 최적화 RTC 모드에서 다음과 같은 애플리케이션을 지원합니다.

- 줌 미팅 (PCoIP 및 WSP용) WorkSpaces
- 시스코 웹엑스 미팅 (WSP만 해당) WorkSpaces

목록에 없는 애플리케이션을 사용하는 경우, 애플리케이션 공급업체에 문의하여 WorkSpaces Media Optimized RTC에 대한 지원을 요청하는 것이 좋습니다. 이 프로세스를 신속하게 처리하려면 @amazon .com에 aws-av-offloading 문의하도록 권장합니다.

미디어 최적화 RTC 모드를 사용하면 통화 성능이 향상되고 WorkSpace 리소스 사용량이 최소화되지만 다음과 같은 몇 가지 제한 사항이 있습니다.

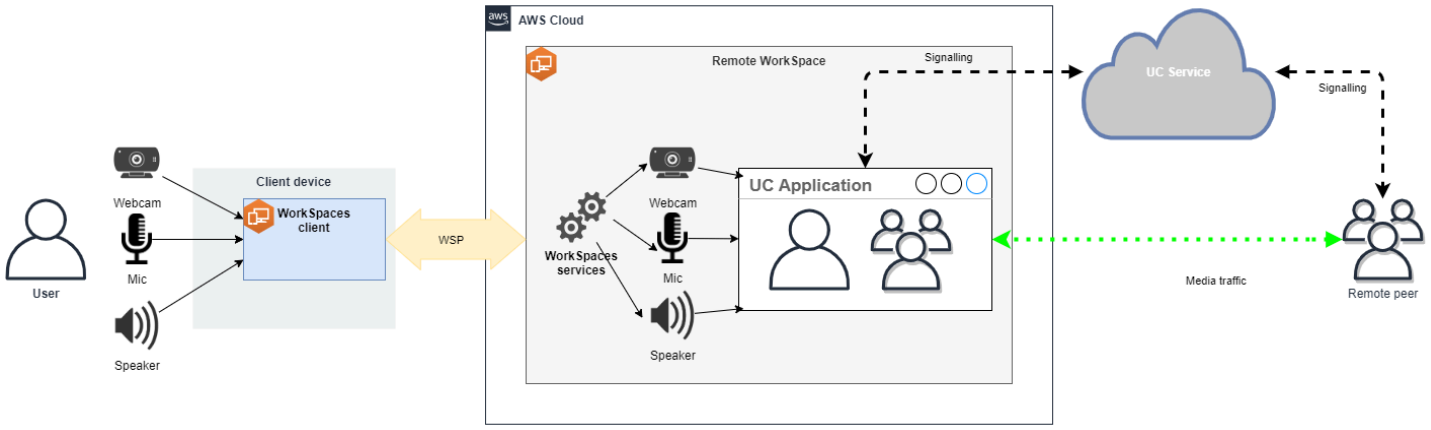
- UC 클라이언트 확장을 클라이언트 디바이스에 설치해야 합니다.
- UC 클라이언트 확장에 독립적인 관리 및 업데이트가 필요합니다.
- 모바일 플랫폼 또는 웹 클라이언트와 같은 특정 클라이언트 플랫폼에서 UC 클라이언트 확장을 사용하지 못할 수 있습니다.
- 이 모드에서는 일부 UC 애플리케이션 기능이 제한될 수 있습니다. 예를 들어 화면 공유 동작이 다를 수 있습니다.
- BYOD(개인 디바이스의 업무상 이용 허용) 또는 공유 키오스크와 같은 시나리오에는 클라이언트 측 확장을 사용하는 것이 적합하지 않을 수 있습니다.

미디어 최적화 RTC 모드가 환경에 적합하지 않은 것으로 확인되거나 특정 사용자가 클라이언트 확장을 설치할 수 없는 경우 세션 내 최적화 RTC 모드를 대체 옵션으로 구성하는 것이 좋습니다.

세션 내 최적화 RTC 구성

세션 내 최적화 RTC 모드에서는 UC 애플리케이션이 수정 WorkSpace 없이 에서 작동하여 로컬과 비슷한 경험을 제공합니다. 애플리케이션에서 생성된 오디오 및 비디오 스트림은 WorkSpaces 스트리밍 프로토콜 (WSP) 에 캡처되어 클라이언트 측으로 전송됩니다. 클라이언트에서는 마이크 (WSP 및 PCoIP 모두 WorkSpaces) 및 웹캠 (WSP에만 해당 WorkSpaces) 신호가 캡처되어 다시 리디렉션되고 UC 애플리케이션으로 원활하게 전달됩니다. WorkSpace

특히 이 옵션은 레거시 애플리케이션과도 탁월한 호환성을 보장하여 애플리케이션의 출처에 관계없이 일관된 사용자 경험을 제공합니다. 세션 내 최적화는 웹 클라이언트에서도 작동합니다.



WorkSpaces 스트리밍 프로토콜 (WSP) 은 원격 RTC 모드의 성능을 향상시키기 위해 세심하게 최적화되었습니다. 최적화 조치에는 다음이 포함됩니다.

- 적응형 UDP 기반 QUIC 전송을 활용하여 효율적인 데이터 전송을 보장합니다.
- 지연 시간이 짧은 오디오 경로를 설정하여 빠른 오디오 입력 및 출력을 지원합니다.
- 음성에 최적화된 오디오 코덱을 구현하여 오디오 품질을 유지하면서 CPU 및 네트워크 사용률을 줄입니다.
- 웹캠 리디렉션을 통해 웹캠 기능을 통합할 수 있습니다.
- 웹캠 해상도를 구성하여 성능을 최적화합니다.
- 적응형 디스플레이 코덱을 통합하여 속도와 화질의 균형을 유지합니다.
- 오디오 지터 보정을 통해 원활한 오디오 전송을 보장합니다.

이러한 최적화는 원격 RTC 모드에서 강력하고 유연한 경험을 제공하는 데 기여합니다.

크기 조정 권장 사항

원격 RTC 모드를 효과적으로 지원하려면 Amazon의 크기를 적절하게 조정하는 것이 중요합니다. WorkSpaces 리모컨은 해당 통합 통신 (UC) 애플리케이션의 시스템 요구 사항을 충족하거나 WorkSpace 초과해야 합니다. 다음 표에는 화상 및 음성 통화에 널리 사용되는 UC 응용 프로그램에 대해 지원되는 최소 구성 및 권장 WorkSpaces 구성이 요약되어 있습니다.

			영상 통화		음성 통화		
애플리케이션	RTC 앱의 CPU 요구 사항	RTC 앱의 RAM 요구 사항	최소 지원 WorkSpace	권장 WorkSpace	최소 지원 WorkSpace	권장 WorkSpace	레퍼런스
Microsoft Teams	코어 2개 필요, 코어 4개 권장	4.0GB RAM	Power(vCPU 4개, 16GB 메모리)	PowerPro(vCPU 8개, 메모리 32기가바이트)	Performance(vCPU 2개, 8GB 메모리)	Power(vCPU 4개, 16GB 메모리)	Microsoft Teams의 하드웨어 요구 사항
확대/축소	코어 2개 필요, 코어 4개 권장	4.0GB RAM	Power(vCPU 4개, 16GB 메모리)	PowerPro(vCPU 8개, 메모리 32기가바이트)	Performance(vCPU 2개, 8GB 메모리)	Power(vCPU 4개, 16GB 메모리)	Zoom 시스템 요구 사항: Windows, macOS, Linux
Webex	코어 2개 필요	4.0GB RAM	Power(vCPU 4개, 16GB 메모리)	PowerPro(vCPU 8개, 메모리 32기가바이트)	Performance(vCPU 2개, 8GB 메모리)	Power(vCPU 4개, 16GB 메모리)	Webex 서비스의 시스템 요구 사항

화상 회의에는 비디오 인코딩 및 디코딩을 위해 상당한 리소스가 사용된다는 점에 유의해야 합니다. 물리적 시스템 시나리오에서는 이러한 작업이 GPU로 오프로드됩니다. 비 WorkSpaces GPU에서 이러한 작업은 원격 프로토콜 인코딩과 병렬로 CPU에서 수행됩니다. 따라서 정기적으로 비디오 스트리밍이나 화상 통화를 하는 사용자의 경우 PowerPro 구성을 선택하는 것이 좋습니다.

화면 공유에도 상당한 리소스가 소모되며 해상도가 높을수록 리소스 소비가 증가합니다. 따라서 비 WorkSpaces GPU에서는 화면 공유가 낮은 프레임 속도로 제한되는 경우가 많습니다.

스트리밍 프로토콜 (WSP) 을 통한 UDP 기반 QUIC 전송을 활용하십시오 WorkSpaces .

UDP 전송은 RTC 애플리케이션을 전송하는 데 특히 적합합니다. 효율성을 극대화하려면 네트워크가 WSP용 QUIC 전송을 활용하도록 설정해야 합니다. UDP 기반 전송은 네이티브 클라이언트에서만 사용할 수 있다는 점에 유의하세요.

UC 애플리케이션을 다음과 같이 구성하십시오. WorkSpaces

배경 흐림, 가상 배경, 반응 또는 라이브 이벤트 호스팅과 같은 향상된 비디오 처리 기능을 위해서는 최적의 성능을 달성하기 위해 GPU 지원 WorkSpace 옵션을 선택하는 것이 필수적입니다.

대부분의 UC 애플리케이션은 고급 비디오 처리를 비활성화하여 비 GPU에서 CPU 사용률을 줄이는 지침을 제공합니다. WorkSpaces

자세한 정보는 다음 리소스를 참조하세요.

- Microsoft Teams: 가상화된 데스크톱 인프라용 Teams
- Zoom Meetings: Managing the user experience for incompatible VDI plugins
- Webex: Deployment guide for Webex App for Virtual Desktop Infrastructure (VDI) - Manage and troubleshoot Webex App for VDI [Webex App]
- Google Meet: VDI 사용

양방향 오디오 및 웹캠 리디렉션 활성화

Amazon은 기본적으로 비디오 WorkSpaces 입력을 통한 오디오 입력, 오디오 출력 및 카메라 리디렉션을 지원합니다. 하지만 특정 이유로 이러한 기능이 비활성화된 경우 제공된 지침에 따라 리디렉션을 다시 활성화할 수 있습니다. 자세한 내용은 Amazon 관리 안내서의 WSP에 대한 비디오 입력 리디렉션 활성화 또는 비활성화를 참조하십시오. WorkSpaces 사용자는 연결 후 세션에서 사용할 카메라를 선택해야 합니다. 자세한 내용은 WorkSpaces 사용자가 Amazon 사용 설명서의 웹캠 및 기타 비디오 장치를 참조하십시오.

최대 웹캠 해상도 제한

Power 또는 화상 회의를 사용하는 사용자의 PowerPro WorkSpaces 경우 리디렉션 웹캠의 최대 해상도를 제한하는 것이 좋습니다. 의 PowerPro 경우 권장 최대 해상도는 너비 640픽셀 x 높이 480픽셀입니다. Power의 경우 권장 최대 해상도는 너비 320픽셀, 높이 240픽셀입니다.

최대 웹캠 해상도를 구성하려면 다음 단계를 수행합니다.

1. Windows 레지스트리 편집기를 엽니다.
2. 다음 레지스트리 경로로 이동합니다.

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. 이름이 `max-resolution`인 문자열 값을 만들고 `(X,Y)` 형식의 원하는 해상도로 설정합니다. 여기서 `X`는 가로 픽셀 수(너비)를 나타내고 `Y`는 세로 픽셀 수(높이)를 나타냅니다. 예를 들어, `(640,480)`으로 지정하면 너비 640픽셀, 높이 480픽셀의 해상도를 나타냅니다.

음성 최적화 오디오 구성 활성화

기본적으로 클라이언트에서 7.1 하이파이 오디오를 WorkSpaces 전달하도록 설정되어 있어 뛰어난 음악 재생 품질을 보장합니다. WorkSpaces 하지만 주 사용 사례에 오디오 또는 화상 회의가 포함되는 경우 오디오 코덱 프로필을 음성 최적화 설정으로 수정하면 CPU 및 네트워크 리소스를 절약할 수 있습니다.

오디오 프로필을 음성 최적화로 설정하려면 다음 단계를 완료하세요.

1. Windows 레지스트리 편집기를 엽니다.
2. 다음 레지스트리 경로로 이동합니다.

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

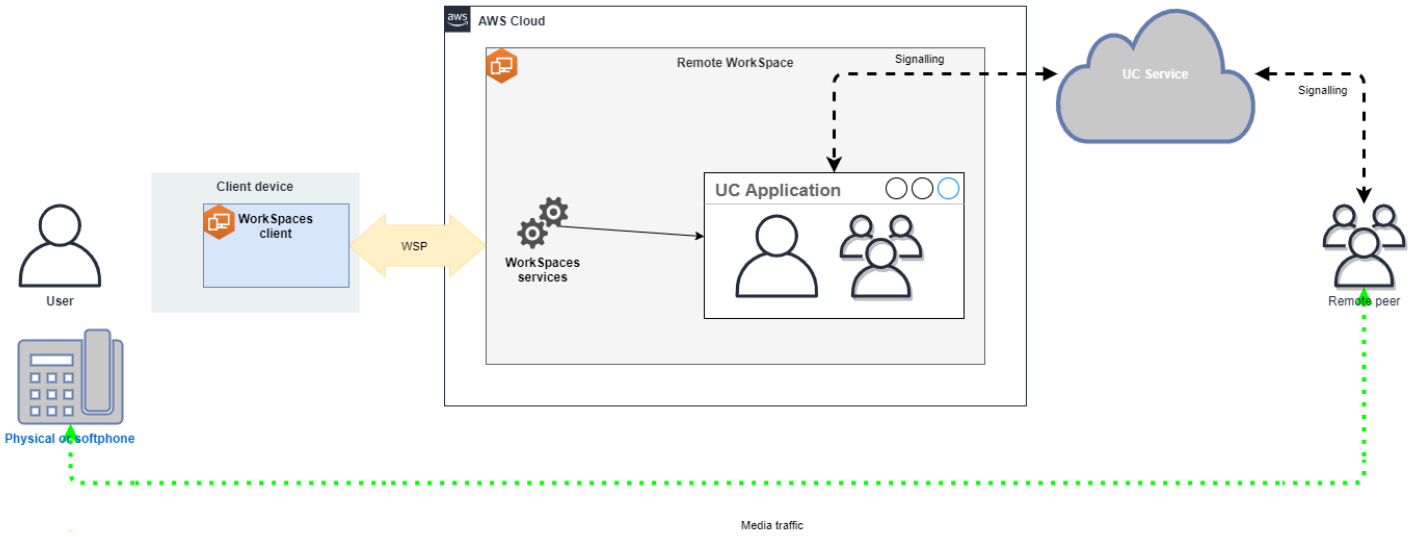
3. 이름이 `default-profile`인 문자열 값을 만들고 `voice`로 설정합니다.

음성 및 영상 통화에 고품질 헤드셋을 사용

오디오 경험을 향상시키고 울림을 방지하려면 고품질 헤드셋을 사용하는 것이 중요합니다. 데스크톱 스피커를 사용하면 원격 통화의 상대방에게 울림 문제가 발생할 수 있습니다.

직접 RTC 구성

Direct RTC 모드의 구성은 특정 통합 통신 (UC) 응용 프로그램에 따라 달라지며 구성을 변경할 필요가 없습니다. WorkSpaces 다음 목록은 다양한 UC 애플리케이션에 대한 최적화를 정리한 것이며 모든 최적화가 포함되지는 않았습니다.



- Microsoft Teams:
  - SIP 게이트웨이 계획
  - Microsoft 365에서의 오디오 회의
  - Teams 음성 솔루션 계획
- Zoom Meetings:
  - Enabling or disabling toll call dial-in numbers
  - Using desk phone call control
  - Desk phone companion mode
- Webex
  - Webex App | Make calls with your desk phone
  - Webex App | Supported calling options
- BlueJeans:
  - Dialing into a Meeting from a Desk Telephone
- Genesys:
  - Genesys Cloud WebRTC 미디어 도우미
- Amazon Connect:
  - 아마존을 위한 아마존 커넥트 최적화 WorkSpaces
- Google Meet:
  - 화상 회의에서 휴대전화를 오디오 기기로 사용

WorkSpace 실행 모드 관리

WorkSpace의 실행 모드에 따라 즉각적인 가용성과 지불 방법(월별 또는 시간별)이 결정됩니다. WorkSpace를 생성할 때 다음 실행 모드 중에서 선택할 수 있습니다.

- AlwaysOn - WorkSpaces를 무제한 사용하며 고정 월 요금을 지불할 때 사용합니다. 이 모드는 WorkSpaces를 기본 데스크톱으로 상시 사용하는 사용자에게 가장 적합합니다.
- AutoStop - WorkSpaces에 대해 시간 단위 요금을 지불할 때 사용합니다. 이 모드에서는 지정된 기간 동안 연결 해제 상태이면 WorkSpaces가 중지되고 앱 상태와 데이터가 저장됩니다.

자세한 내용은 WorkSpaces 요금을 참조하세요.

AutoStop WorkSpaces

자동 중지 시간을 설정하려면 Amazon WorkSpaces 콘솔에서 WorkSpaces를 선택하고 작업, 실행 모드 속성 수정을 선택한 다음 AutoStop 시간(시간)을 설정합니다. 기본적으로 AutoStop 시간(시간)은 1시간으로 설정되어 있습니다. 즉, WorkSpace의 연결이 끊긴 후 한 시간 후에 WorkSpaces가 자동으로 중지됩니다.

WorkSpace의 연결이 끊기고 AutoStop 시간이 만료된 후 WorkSpaces가 자동으로 중지되는 데 몇 분이 더 걸릴 수 있습니다. 하지만 청구는 AutoStop 시간이 만료되는 즉시 중단되며 추가 시간에 대해서는 요금이 청구되지 않습니다.

가능한 경우 데스크톱의 상태가 WorkSpaces의 루트 볼륨에 저장됩니다. 사용자가 로그인하면 WorkSpaces가 재개되고, 모든 열려 있는 문서와 실행 중인 프로그램이 저장된 상태로 반환됩니다.

AutoStop Graphics.g4dn, GraphicsPro.g4dn, Graphics 및 GraphicsPro WorkSpaces는 중지된 데이터 및 프로그램의 상태를 보존하지 않습니다. 이러한 Autostop WorkSpaces의 경우 매번 사용을 완료한 후 작업을 저장하는 것이 좋습니다.

기존 보유 라이선스 사용(BYOL) AutoStop WorkSpaces의 경우 동시 로그인 수가 많으면 WorkSpaces를 사용할 수 있기까지 시간이 오래 걸릴 수 있습니다. 많은 사용자가 동시에 BYOL AutoStop WorkSpaces에 로그인할 것으로 예상되는 경우 계정 관리자에게 조언을 구하세요.

> **Important**
>
> AutoStop WorkSpaces는 WorkSpaces 연결이 끊긴 경우에만 자동으로 중지됩니다.

WorkSpace는 다음과 같은 경우에만 연결이 끊깁니다.

- 사용자가 WorkSpace와의 연결을 수동으로 끊거나 Amazon WorkSpaces 클라이언트 애플리케이션을 종료하는 경우
- 클라이언트 디바이스가 종료된 경우
- 클라이언트 디바이스와 WorkSpace가 20분 이상 연결되지 않은 경우

가장 좋은 방법은 AutoStop WorkSpace 사용자가 매일 WorkSpaces를 사용하고 나면 해당 WorkSpaces와의 연결을 수동으로 끊는 것입니다. 수동으로 연결을 끊으려면 Linux, macOS 또는 Windows용 WorkSpaces 클라이언트 애플리케이션의 Amazon WorkSpaces 메뉴에서 WorkSpace 연결 해제 또는 Amazon WorkSpaces 종료를 선택합니다. Android 또는 iPad의 경우 사이드바 메뉴에서 연결 해제를 선택합니다.

AutoStop WorkSpaces는 다음과 같은 경우에 자동으로 중지되지 않을 수 있습니다.

- 클라이언트 디바이스가 종료되지 않고 잠기거나 휴면 상태이거나 비활성 상태인 경우(예: 노트북 덮개가 닫힌 경우) WorkSpaces 애플리케이션이 백그라운드에서 계속 실행되고 있을 수 있습니다. WorkSpaces 애플리케이션이 계속 실행되고 있는 동안에는 WorkSpace의 연결이 끊어지지 않을 수 있으며, 따라서 WorkSpace가 자동으로 중지되지 않을 수 있습니다.
- WorkSpaces는 사용자가 WorkSpaces 클라이언트를 사용하는 경우에만 연결 해제를 감지할 수 있습니다. 사용자가 서드 파티 클라이언트를 사용하는 경우 WorkSpaces가 연결 해제를 감지하지 못하여 WorkSpaces가 자동으로 중지되지 않고 청구가 일시 중단되지 않을 수 있습니다.

실행 모드 수정

언제라도 실행 모드를 전환할 수 있습니다.

WorkSpaces 실행 모드를 수정하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. 수정할 WorkSpace를 선택하고 작업, 실행 모드 속성 수정을 선택합니다.
4. 새 실행 모드를 선택하고 AlwaysOn 또는 AutoStop을 선택한 다음 수정을 선택합니다.

AWS CLI를 사용하여 WorkSpaces 실행 모드를 수정하는 방법

modify-workspace-properties 명령을 사용합니다.

AutoStop WorkSpaces 중지 및 시작

AutoStop WorkSpaces가 연결 해제되면 지정된 연결 해제 기간이 지난 후 자동으로 중지되고 시간별 청구가 일시 중지됩니다. 비용 최적화를 위해 AutoStop WorkSpaces와 연결된 시간당 요금을 수동으로 일시 중지할 수 있습니다. 그러면 WorkSpace가 중지되고 사용자가 WorkSpace에 다음에 로그인할 때에 대비하여 모든 앱과 데이터가 저장됩니다.

사용자가 중지된 WorkSpace에 다시 연결하면 일반적으로 90초 이내에 중단된 위치부터 재개됩니다.

사용 가능하거나 오류 상태인 AutoStop WorkSpaces를 재부팅(다시 시작)할 수 있습니다.

AutoStop WorkSpaces를 중지하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. 중지할 WorkSpace를 선택하고 작업, WorkSpaces 중지를 선택합니다.
4. 확인 메시지가 표시되면 WorkSpace 중지를 선택합니다.

AutoStop WorkSpaces를 시작하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. 시작할 WorkSpaces를 선택하고 작업, WorkSpaces 시작을 선택합니다.
4. 확인 메시지가 표시되면 WorkSpace 시작을 선택합니다.

AutoStop WorkSpaces와 연결된 고정 인프라 비용을 제거하려면 계정에서 WorkSpace를 제거합니다. 자세한 내용은 WorkSpace 삭제 섹션을 참조하세요.

AWS CLI를 사용하여 AutoStop WorkSpaces를 중지 및 시작하는 방법

stop-WorkSpaces 및 start-WorkSpaces 명령을 사용합니다.

애플리케이션 관리

WorkSpacea를 실행하면 WorkSpaces 콘솔에서 와 관련된 모든 애플리케이션 번들 목록을 볼 수 있습니다 WorkSpace .

해당 제품과 관련된 모든 애플리케이션 번들 목록을 보려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 선택합니다 WorkSpaces.
3. 를 WorkSpace 선택하고 세부 정보 보기를 선택합니다.
4. 애플리케이션에서 이와 WorkSpace 관련된 애플리케이션 목록과 해당 설치 상태를 확인할 수 있습니다.

다음과 같은 방법으로 WorkSpace 에서 애플리케이션 번들을 업데이트할 수 있습니다.

- 에 애플리케이션 번들을 설치하십시오. WorkSpace
- 에서 애플리케이션 번들 제거 WorkSpace
- 애플리케이션 번들을 설치하고 사용자 디바이스에서 다른 애플리케이션 번들 세트를 제거하세요. WorkSpace

> **Note**
>
> - 애플리케이션 번들을 업데이트하려면 의 상태가 또는 WorkSpace 상태여야 합니다. `AVAILABLE` `STOPPED`
> - 애플리케이션 관리는 WorkSpaces Windows에서만 사용할 수 있습니다.
> - 애플리케이션 관리는 AWS를 통해 구독한 애플리케이션 번들에서만 가능합니다.

애플리케이션 관리가 지원되는 번들

응용 프로그램 관리를 사용하면 사용자 컴퓨터에 다음 응용 프로그램을 설치 및 제거할 수 WorkSpaces 있습니다. Microsoft Office 2016 번들 및 Microsoft Office 2019의 경우 제거만 가능합니다.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021

- Microsoft Project Standard 2021

다음 표에는 지원되는 애플리케이션과 지원되지 않는 애플리케이션 및 운영 체제 조합의 목록이 나와 있습니다.

	Microsoft Office Professional Plus 2016(32비트)	Microsoft Office Professional Plus 2019(64비트)	Microsoft LTSC Office Professional Plus / Standard 2021(64비트)	Microsoft Project Professional / Standard 2021(64비트)	Microsoft LTSC Visio Professional / Standard 2021(64비트)
Windows Server 2016	제거	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음
Windows Server 2019	지원되지 않음	제거	설치/제거	설치/제거	설치/제거
Windows Server 2022	지원되지 않음	제거	설치/제거	설치/제거	설치/제거
Windows 10	제거	제거	설치/제거	설치/제거	설치/제거
Windows 11	제거	제거	설치/제거	설치/제거	설치/제거

Important

- 이러한 애플리케이션은 동일한 에디션을 따라야 합니다. 예를 들어, Standard 애플리케이션과 Professional 애플리케이션을 함께 사용할 수 없습니다.

- 이러한 애플리케이션은 동일한 버전을 따라야 합니다. 예를 들어, 2019 애플리케이션과 2021 애플리케이션을 함께 사용할 수 없습니다.
- Microsoft Office/Visio/Project 2021 스탠다드/프로페셔널은 밸류, 그래픽 및 번들에 대해 지원되지 않습니다. GraphicsPro WorkSpaces
- Microsoft Office 2016용 Plus 애플리케이션 번들을 사용자 WorkSpaces 제품에서 제거하면 해당 Amazon WorkSpaces 번들의 일부로 포함된 모든 트렌드마이크로 솔루션에 액세스할 수 없게 됩니다. WorkSpacesAmazon에서 트렌드마이크로 솔루션을 계속 사용하려면 AWS 마켓플레이스에서 별도로 구매할 수 있습니다.
- Microsoft 365 앱을 설치/제거하려면 자체 도구 및 설치 프로그램을 사용해야 합니다. 애플리케이션 워크플로 관리로는 Microsoft 365 앱을 설치/제거할 수 없습니다.
- 애플리케이션 관리를 통해 애플리케이션이 WorkSpaces 설치된 사용자 지정 이미지를 생성할 수는 없지만 애플리케이션 관리를 사용하여 애플리케이션 번들을 제거하는 사용자 지정 이미지를 생성할 수 있습니다. WorkSpaces
- 애플리케이션 관리를 사용하려면 DNS 확인을 활성화해야 합니다.
- 아프리카 (케이프타운) 와 같은 옵트인 지역의 경우 디렉터리 수준에서 WorkSpaces 인터넷 연결을 활성화해야 합니다.

에서 애플리케이션 번들을 업데이트하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 를 WorkSpace 선택하고 작업, 애플리케이션 관리를 선택합니다.
4. 현재 응용 프로그램 아래에는 이미 설치된 응용 프로그램 번들 목록이 표시되고 응용 프로그램 선택에는 여기에 WorkSpace 설치할 수 있는 응용 프로그램 번들 목록이 있습니다. WorkSpace
5. 여기에 애플리케이션 번들을 설치하려면: WorkSpace
   a. 여기에 WorkSpace 설치할 애플리케이션 번들을 선택하고 [Associate] 를 선택합니다.
   b. 이전 단계를 반복하여 다른 애플리케이션 번들을 설치합니다.
   c. 애플리케이션 번들이 설치되는 동안 현재 애플리케이션에 `Pending install deployment` 상태로 애플리케이션 번들이 표시됩니다.
6. 여기에서 애플리케이션 번들을 제거하려면: WorkSpace
   a. 애플리케이션 선택에서 제거하려는 애플리케이션 번들을 선택하고 연결 해제를 선택합니다.

b. 이전 단계를 반복하여 다른 애플리케이션 번들을 제거합니다.

c. 애플리케이션 번들이 제거되는 동안 현재 애플리케이션에 `Pending uninstall deployment` 상태로 애플리케이션 번들이 표시됩니다.

7. 번들 설치 또는 설치 상태를 되돌리려면 다음 중 하나를 수행하세요.

- 번들을 `Pending uninstall deployment` 상태에서 되돌리려면 되돌릴 애플리케이션을 선택한 다음 연결을 선택합니다.
- 번들을 `Pending install deployment` 상태에서 되돌리려면 되돌릴 애플리케이션을 선택한 다음 연결 해제를 선택합니다.

8. 설치 또는 제거하기로 선택한 애플리케이션 번들이 보류 상태로 전환되면 애플리케이션 배포를 선택합니다.

> **Important**
>
> 애플리케이션 배포를 선택하면 애플리케이션을 설치하거나 제거하는 동안에는 최종 사용자 세션이 종료되고 WorkSpaces 액세스할 수 없게 됩니다.

9. 작업을 확인하려면 확인을 입력합니다. 오류 상태인 애플리케이션 번들을 설치하거나 제거하려면 강제를 선택합니다.

10. 애플리케이션 번들 진행 상황을 모니터링하는 방법:

a. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.

b. 탐색 창에서 WorkSpaces를 선택합니다. 상태에서 다음과 같은 상태를 확인할 수 있습니다.

- 업데이트 중 - 애플리케이션 번들 업데이트가 아직 진행 중입니다.
- 사용 가능/ 중지됨 - 애플리케이션 번들 업데이트가 WorkSpace 완료되어 원래 상태로 돌아왔습니다.

c. 애플리케이션 번들의 설치 또는 제거 상태를 모니터링하려면 를 WorkSpace 선택하고 세부 정보 보기를 선택합니다. 애플리케이션에서 상태 아래에서 `Pending install`, `Pending uninstall`, `Installed` 등의 상태를 확인할 수 있습니다.

> **Note**
>
> Managed Applications를 통해 새로 설치한 애플리케이션 번들에 라이선스가 활성화되지 않은 것을 사용자가 발견하면 수동 재부팅을 수행할 수 있습니다. WorkSpace 사용자는 재

부팅 후 해당 애플리케이션을 사용하기 시작할 수 있습니다. 추가 지원이 필요하면 AWS Support에 문의하세요.

애플리케이션 관리를 사용하여 관리, WorkSpaces 수정됨

에서 애플리케이션 번들을 설치 또는 제거한 후 다음과 같은 조치가 기존 구성에 영향을 미칠 수 있습니다. WorkSpaces

- a WorkSpace - 복원 a를 WorkSpace 복원하면 정상 상태일 때 생성된 해당 볼륨의 최신 스냅샷을 기반으로 루트 볼륨과 사용자 볼륨이 모두 다시 생성됩니다. WorkSpace 전체 WorkSpace 스냅샷은 12시간마다 촬영됩니다. 자세한 내용은 복원 WorkSpace a를 참조하십시오. 애플리케이션 관리를 사용하여 WorkSpaces 수정한 데이터를 복원하려면 12시간 이상 기다려야 합니다. 애플리케이션 관리를 사용하여 수정한 다음 전체 스냅샷을 WorkSpaces 복원하기 전에 복원하면 다음과 같은 결과가 나타납니다.
  - 애플리케이션 관리 WorkSpaces 워크플로를 사용하여 설치한 애플리케이션 번들은 사용자 계정에서 WorkSpaces 제거되지만 라이선스는 계속 활성화되며 해당 애플리케이션에 대한 WorkSpaces 요금이 청구됩니다. 이러한 애플리케이션 번들을 다시 가져오려면 애플리케이션 관리 워크플로를 다시 실행하고 애플리케이션을 WorkSpaces 제거하여 새로 시작한 다음 다시 설치해야 합니다.
  - 애플리케이션 관리 WorkSpaces 워크플로를 사용하여 제거된 애플리케이션 번들은 다시 다시 사용할 수 있습니다. WorkSpaces 하지만 라이선스 활성화가 누락되므로 이러한 애플리케이션 번들은 제대로 작동하지 않습니다. 이러한 애플리케이션 번들을 제거하려면 사용자 애플리케이션에서 해당 애플리케이션 번들을 수동으로 제거해 보세요. WorkSpaces
- 재구축 a WorkSpace - a를 재구축하면 루트 볼륨이 WorkSpace 다시 생성됩니다. 자세한 내용은 a 재구축을 참조하십시오. WorkSpace 애플리케이션 관리를 사용하여 WorkSpaces 수정한 데이터를 다시 빌드하면 다음과 같은 결과가 나타납니다.
  - 애플리케이션 관리 워크플로를 WorkSpaces 사용하여 설치한 애플리케이션 번들은 에서 제거되고 비활성화됩니다. WorkSpaces 이러한 애플리케이션을 다시 실행하려면 애플리케이션 관리 워크플로를 다시 실행해야 합니다. WorkSpaces
  - 애플리케이션 관리 워크플로를 WorkSpaces 통해 제거된 애플리케이션 번들은 에 설치되고 활성화됩니다. WorkSpaces 에서 이러한 애플리케이션 번들을 제거하려면 애플리케이션 관리 워크플로를 다시 실행해야 합니다. WorkSpaces
- 마이그레이션 a WorkSpace - 마이그레이션 프로세스는 대상 번들 이미지의 새 루트 볼륨과 원본의 마지막 사용 가능한 스냅샷의 사용자 볼륨을 사용하여 를 다시 생성합니다. WorkSpace WorkSpace 새 WorkSpace ID를 WorkSpace 가진 새 ID가 생성됩니다. 자세한 내용은 WorkSpace마이그레이션

을 참조하십시오. 애플리케이션 관리를 사용하여 수정한 계정을 WorkSpaces 마이그레이션하면 다음과 같은 결과가 나타납니다.

- 소스의 모든 애플리케이션 번들이 제거되고 WorkSpaces 비활성화됩니다. 새 대상은 대상 WorkSpaces 번들의 애플리케이션을 상속합니다. WorkSpaces 소스 WorkSpaces 애플리케이션 번들에 대해서는 한 달 동안 요금이 청구되지만 대상 번들의 애플리케이션 번들에는 비례 할당으로 계산된 요금이 적용됩니다.

a 수정 WorkSpace

WorkSpacea를 시작한 후 다음 세 가지 방법으로 구성을 수정할 수 있습니다.

- 루트 볼륨(Windows의 경우 C 드라이브, Linux의 경우 /) 및 사용자 볼륨(Windows의 경우 D 드라이브, Linux의 경우 /home의 경우)의 크기를 변경할 수 있습니다.
- 컴퓨팅 유형을 변경하여 새 번들을 선택할 수 있습니다.
- PCoIP WorkSpace 번들로 생성한 경우 AWS CLI 또는 Amazon WorkSpaces API를 사용하여 스트리밍 프로토콜을 수정할 수 있습니다.

a의 현재 수정 상태를 보려면 화살표를 선택하여 이에 WorkSpace 대한 세부 정보를 표시합니다. WorkSpace State(상태)에 가능한 값은 Modifying Compute(컴퓨팅 수정), Modifying Storage(스토리지 수정) 및 None(없음)입니다.

WorkSpacea를 수정하려면 상태가 또여야 합니다`STOPPED`. `AVAILABLE` 볼륨 크기와 컴퓨팅 유형을 동시에 변경할 수 없습니다.

a의 볼륨 크기 또는 컴퓨팅 유형을 WorkSpace 변경하면 의 청구 요금이 변경됩니다 WorkSpace.

사용자가 볼륨 및 컴퓨팅 유형을 직접 수정할 수 있도록 하려면 사용자를 위한 셀프 서비스 WorkSpace 관리 기능 활성화 단원을 참조하십시오.

볼륨 크기 수정

루트 볼륨과 사용자 볼륨의 크기를 각각 최대 2000GB까지 늘릴 수 있습니다. WorkSpace WorkSpace 루트 볼륨과 사용자 볼륨은 세트 그룹으로 구성되며 변경할 수 없습니다. 사용 가능한 그룹은 다음과 같습니다.

[루트(GB), 사용자(GB)]
[80, 10]
[80, 50]
[80, 100]
[175~2000, 100~2000]

루트 및 사용자 볼륨은 암호화되어 있든 암호화되어 있지 않든 상관없이 확장할 수 있으며 두 볼륨 모두 6시간 내에 한 번 확장할 수 있습니다. 하지만 루트 및 사용자 볼륨의 크기를 동시에 늘릴 수는 없습니다. 자세한 내용은 볼륨 증가의 제한을 참조하십시오.

> **Note**
>
> 의 볼륨을 확장하면 Windows 또는 Linux 내에서 볼륨의 파티션이 WorkSpaces 자동으로 확장됩니다. WorkSpace 프로세스가 끝나면 를 다시 부팅해야 변경 내용이 적용됩니다. WorkSpace

데이터를 보존하려면 를 실행한 후에는 루트 또는 사용자 볼륨의 크기를 줄일 수 없습니다 WorkSpace. 대신 를 실행할 때 이러한 볼륨의 최소 크기를 지정해야 WorkSpace 합니다. Value, Standard, Performance, Power 또는 PowerPro WorkSpace 루트 볼륨은 최소 80GB, 사용자 볼륨은 10GB 이상으로 실행할 수 있습니다. 그래픽.G4DN, GraphicsPro .g4dn, Graphics를 실행하거나 GraphicsPro WorkSpace 루트 볼륨의 경우 최소 100GB, 사용자 볼륨의 경우 100GB 이상으로 실행할 수 있습니다.

WorkSpace 디스크 크기가 커지는 동안에도 사용자는 자신의 디스크에서 대부분의 작업을 수행할 수 있습니다. WorkSpace 하지만 WorkSpace 컴퓨팅 유형을 변경하거나, WorkSpace 실행 모드를 전환하거나, 재구축하거나 WorkSpace, 재부팅 (재시작) 할 WorkSpace 수는 없습니다.

> **Note**
>
> 디스크 크기가 커지는 WorkSpaces 동안에도 사용자가 해당 디스크를 사용할 수 있게 하려면 볼륨 크기를 `STOPPED` 조정하기 전에 상태가 `AVAILABLE` 대신 으로 설정되어 WorkSpaces

있어야 합니다. WorkSpaces 그럴 경우 디스크 크기를 늘리는 동안에는 시작할 수 없습니다. WorkSpaces STOPPED

대부분의 경우 디스크 크기 증가 프로세스에는 최대 2시간이 걸릴 수 있습니다. 그러나 대량의 볼륨 크기를 수정할 경우 프로세스 시간이 상당히 오래 걸릴 수 있습니다. WorkSpaces 수정해야 할 개수가 많으면 WorkSpaces AWS Support 문의하여 도움을 받는 것이 좋습니다.

볼륨 증가의 제한 사항

- SSD 볼륨만 크기를 조정할 수 있습니다.
- 를 WorkSpace 실행할 때는 6시간을 기다려야 볼륨 크기를 수정할 수 있습니다.
- 루트 및 사용자 볼륨의 크기를 동시에 늘릴 수는 없습니다. 루트 볼륨을 늘리려면 먼저 사용자 볼륨을 100GB로 변경해야 합니다. 이와 같이 변경한 후, 루트 볼륨을 175 ~ 2000GB 사이의 값으로 업데이트할 수 있습니다. 루트 볼륨을 175 ~ 2000GB 사이의 값으로 변경한 후에는 사용자 볼륨을 100 ~ 2000GB 사이의 값으로 추가로 업데이트할 수 있습니다.

  > **Note**
  >
  > 두 볼륨을 모두 늘리려면 첫 번째 작업이 완료될 때까지 20 ~ 30분을 기다려야 두 번째 작업을 시작할 수 있습니다.

- 그래픽.g4dn, GraphicsPro .g4dn, Graphics 또는 GraphicsPro WorkSpace 사용자 볼륨이 100GB인 경우 루트 볼륨이 175GB 미만인 경우를 제외하고 루트 WorkSpace 볼륨은 175GB 미만일 수 없습니다. 그래픽.g4dn, GraphicsPro .g4dn, 그래픽 및 루트 볼륨과 사용자 볼륨 모두 최소 100GB로 설정할 수 있습니다. GraphicsPro WorkSpaces
- 사용자 볼륨이 50GB인 경우 루트 볼륨을 80GB 이외의 다른 값으로 업데이트할 수 없습니다. 루트 볼륨이 80GB인 경우 사용자 볼륨은 10, 50 또는 100GB만 될 수 있습니다.

의 루트 볼륨을 수정하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 를 WorkSpace 선택하고 작업, 루트 볼륨 수정을 선택합니다. .
4. 루트 볼륨 크기에서 볼륨 크기를 선택하거나 사용자 지정을 선택하여 사용자 지정 볼륨 크기를 입력합니다.

5. 변경 사항 저장을 선택합니다.
6. 디스크 크기 증가가 끝나면 를 다시 부팅해야 변경 사항이 적용됩니다. WorkSpace 데이터 손실을 방지하려면 를 다시 부팅하기 전에 사용자가 열려 있는 파일을 모두 저장했는지 확인하십시오 WorkSpace.

의 사용자 볼륨을 수정하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 를 WorkSpace 선택하고 작업, 사용자 볼륨 수정을 선택합니다. .
4. 사용자 볼륨 크기에서 볼륨 크기를 선택하거나 사용자 지정을 선택하여 사용자 지정 볼륨 크기를 입력합니다.
5. 변경 사항 저장을 선택합니다.
6. 디스크 크기 증가가 끝나면 를 다시 부팅해야 변경 사항이 적용됩니다. WorkSpace 데이터 손실을 방지하려면 를 다시 부팅하기 전에 사용자가 열려 있는 파일을 모두 저장했는지 확인하십시오 WorkSpace.

의 볼륨 크기를 변경하려면 WorkSpace

modify-workspace-properties명령을 `RootVolumeSizeGib` or `UserVolumeSizeGib` 속성과 함께 사용합니다.

컴퓨팅 유형 수정

a를 표준, 전력, 성능 및 PowerPro 컴퓨팅 유형 WorkSpace 간에 전환할 수 있습니다. 이러한 컴퓨팅 유형에 대한 자세한 내용은 Amazon WorkSpaces Bundles를 참조하십시오.

> **Note**
>
> - 컴퓨팅 유형을 Graphics.G4dn에서 .g4dn으로 변경하거나.g4dn에서 Graphics.G4dn으로 변경할 수 있습니다 GraphicsPro. GraphicsPro 그래픽.G4DN과 GraphicsPro .g4dn의 컴퓨팅 유형을 다른 값으로 변경할 수 없습니다.
> - 2023년 11월 30일 이후에는 Graphics 번들이 더 이상 지원되지 않습니다. Graphics.G4dn 번들로 마이그레이션하는 것이 좋습니다. WorkSpaces 자세한 설명은 마이그레이션 a WorkSpace 섹션을 참조하세요.

- 그래픽의 컴퓨팅 유형을 다른 값으로 변경할 수 없습니다. GraphicsPro

컴퓨팅 변경을 요청하면 새 컴퓨팅 유형을 WorkSpace 사용하여 WorkSpaces 를 재부팅합니다. WorkSpaces 의 운영 체제, 애플리케이션, 데이터 및 스토리지 설정을 보존합니다. WorkSpace

더 큰 컴퓨팅 유형을 6시간마다 한 번 요청하거나 더 작은 컴퓨팅 유형을 30일마다 한 번 요청할 수 있습니다. 새로 시작한 WorkSpace 경우 더 큰 컴퓨팅 유형을 요청하려면 6시간을 기다려야 합니다.

WorkSpace 컴퓨팅 유형 변경이 진행 중인 경우 사용자는 해당 WorkSpace 사용자와의 연결이 끊어져 사용하거나 변경할 수 없습니다. WorkSpace 컴퓨팅 유형 변경 프로세스 중에 WorkSpace 가 자동으로 재부팅됩니다.

Important

데이터 손실을 방지하려면 WorkSpace 컴퓨팅 유형을 변경하기 전에 사용자가 열려 있는 문서 및 기타 애플리케이션 파일을 모두 저장하도록 하십시오.

컴퓨팅 유형 변경 프로세스는 최대 한 시간까지 걸릴 수 있습니다.

의 컴퓨팅 유형을 변경하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 를 WorkSpace 선택하고 작업, 컴퓨팅 유형 수정을 선택합니다.
4. 컴퓨팅 유형에서 컴퓨팅 유형을 선택합니다.
5. 변경 사항 저장을 선택합니다.

a의 컴퓨팅 유형을 변경하려면 WorkSpace

modify-workspace-properties명령을 `ComputeTypeName` 속성과 함께 사용합니다.

프로토콜 수정

PCoIP 번들로 생성한 경우 AWS CLI 또는 Amazon WorkSpace API를 사용하여 스트리밍 프로토콜을 수정할 수 있습니다. WorkSpaces 이렇게 하면 마이그레이션 기능을 사용하지 WorkSpace 않고도 기

존 프로토콜을 사용하여 프로토콜을 마이그레이션할 수 있습니다. WorkSpace 또한 WorkSpaces 스트리밍 프로토콜 (WSP) 을 사용하여 마이그레이션 프로세스 WorkSpaces 중에 기존 PCoIP를 다시 만들지 않고도 루트 볼륨을 유지할 수 있습니다.

- PCoIP WorkSpace 번들로 프로토콜을 생성한 경우에만 프로토콜을 수정할 수 있습니다.
- 프로토콜을 WSP로 수정하기 전에 WSP에 대한 다음 요구 WorkSpace 사항을 충족하는지 확인하십시오. WorkSpace
  - WorkSpaces 클라이언트가 WSP를 지원합니다.
  - 배포된 WorkSpace 지역은 WSP를 지원합니다.
  - WSP에 대한 IP 주소 및 포트가 공개되어야 합니다. 자세한 내용은 의 IP 주소 및 포트 요구 사항을 참조하십시오 WorkSpaces.
  - 현재 번들을 WSP에서 사용할 수 있는지 확인하세요.
  - 최상의 화상 회의 경험을 위해 Power 또는 PowerPro Bundles만 사용하는 것이 좋습니다.

> **Note**
>
> - 프로토콜 변경을 WorkSpaces 시작하기 전에 비프로덕션 환경에서 테스트해 보는 것이 좋습니다.
> - 프로토콜을 PCoIP에서 WSP로 수정한 다음 프로토콜을 다시 PCoIP로 수정하면 웹 액세스를 통해 연결할 수 없습니다. WorkSpaces

의 프로토콜을 변경하려면 WorkSpace

1. [선택 사항] 프로토콜을 수정하기 전에 WorkSpace 재부팅하고 `AVAILABLE` 상태가 될 때까지 기다리십시오.
2. [선택 사항] `describe-workspaces` 명령을 사용하여 WorkSpace 속성을 나열합니다. 상태가 `AVAILABLE`이고 현재 `Protocol`이 올바른지 확인합니다.
3. `modify-workspace-properties` 명령을 사용하여 `Protocols` 속성을 `PCOIP`에서 `WSP`로 또는 그 반대로 수정합니다.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> `Protocols` 속성은 대소문자를 구분합니다. 반드시 `PCOIP` 또는 `WSP`를 사용해야 합니다.

4. 명령을 실행한 후 를 재부팅하고 필요한 구성을 WorkSpace 완료하는 데 최대 20분이 걸릴 수 있습니다.
5. `describe-workspaces`명령을 다시 사용하여 WorkSpace 속성을 나열하고 속성이 정상이고 현재 `Protocols` 속성이 올바른 프로토콜로 변경되었는지 확인합니다. `AVAILABLE`

> **Note**
>
> - WorkSpace의 프로토콜을 수정해도 콘솔의 번들 설명은 업데이트되지 않습니다. 번들 시작 설명은 변경되지 않습니다.
> - 20분 후에도 `UNHEALTHY` 상태가 WorkSpace 유지되면 WorkSpace 콘솔에서 다시 부팅하십시오.

6. 이제 컴퓨터에 연결할 수 있습니다 WorkSpace.

WorkSpace 브랜딩 맞춤 설정

WorkSpaces Amazon에서는 API를 사용하여 자체 브랜드 로고, IT 지원 정보, 비밀번호 분실 링크 및 로그인 메시지로 로그인 페이지의 모양을 사용자 지정하여 사용자에게 친숙한 WorkSpaces 경험을 제공할 수 있습니다. WorkSpace 브랜딩은 기본 브랜딩이 아닌 사용자의 WorkSpace 로그인 페이지에 표시됩니다. WorkSpaces

다음 클라이언트가 지원됩니다.

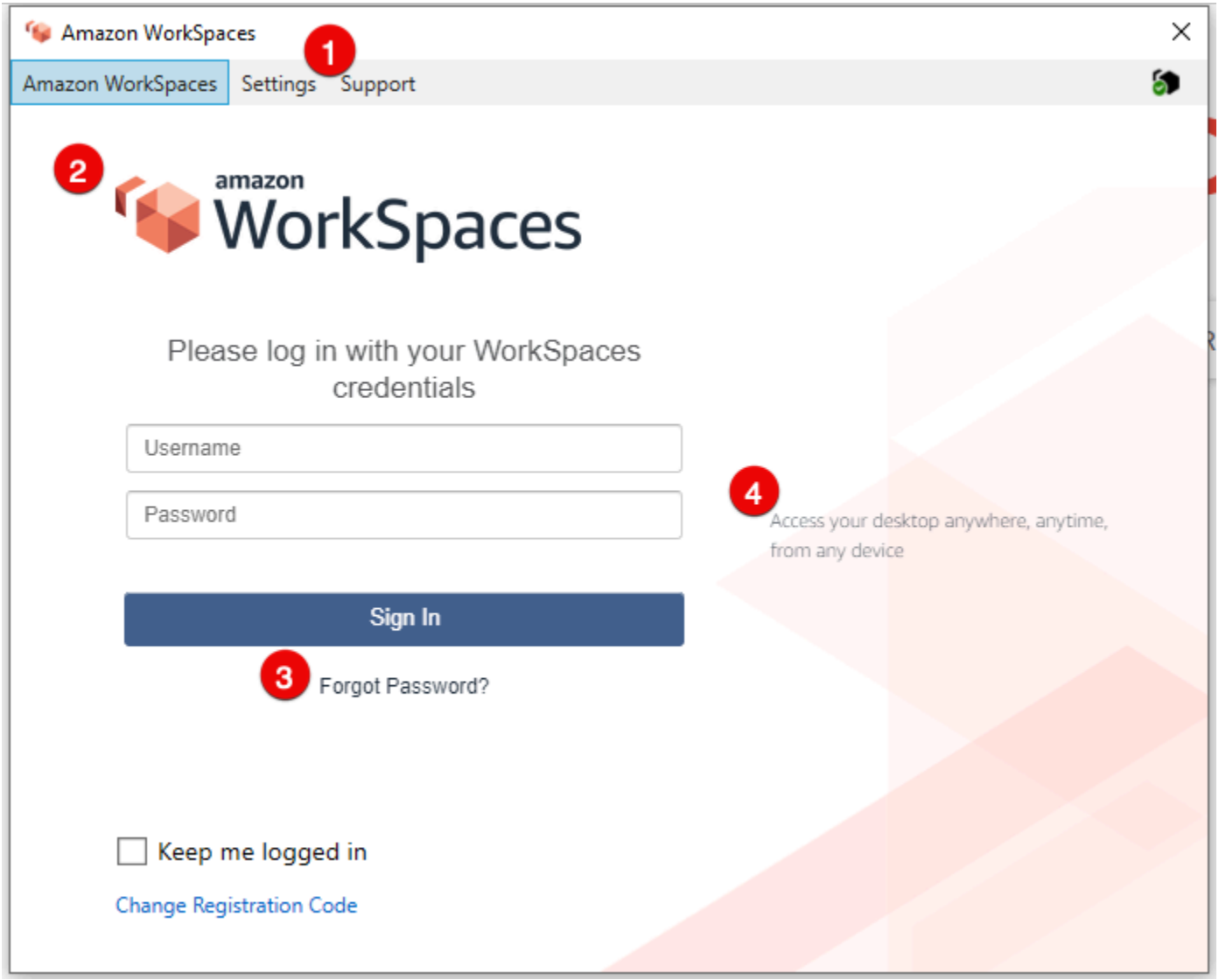
- Windows
- Linux
- Android
- MacOS
- iOS
- 웹 액세스

> **Note**
>
> 의 ClientBranding API를 사용하여 브랜딩 요소를 수정하려면 AWS GovCloud (US) Region 5.10.0인 WorkSpaces 클라이언트 버전을 사용하십시오.

사용자 지정 브랜딩 가져오기

클라이언트 브랜딩 사용자 지정을 가져오려면 다음 요소가 포함된 `ImportClientBranding` 작업을 사용하세요. 자세한 내용은 ImportClientBranding API 참조를 참조하십시오.

> **Important**
>
> 클라이언트 브랜딩 속성은 공개용입니다. 민감한 정보를 저장하지 마세요.



1. 지원 링크
2. 로고
3. 암호 찾기 링크
4. 로그인 메시지

사용자 지정 브랜딩 요소

브랜딩 요소	설명	요구 사항 및 권장 사항
지원 링크	사용자가 도움을 요청하기 위해 연락할 수 있는 지원 이메일 링크를 지정할 수 있습니	• 각 플랫폼 유형에서 `SupportEmail` 및 `SupportLink` 파라미터는

브랜딩 요소	설명	요구 사항 및 권장 사항
	다 WorkSpaces. `SupportEmail` 속성을 사용하거나 `SupportLink` 속성을 사용하여 지원 페이지 링크를 제공할 수 있습니다.	상호 배타적입니다. 각 플랫폼 유형에 파라미터를 하나만 지정할 수 있습니다. 두 파라미터를 모두 지정할 수는 없습니다. • 기본 이메일은 `workspaces-feedback@amazon.com` 입니다. • 길이 제한: 최소 길이는 1입니다. 최대 길이는 200.

로고	`Logo` 속성을 사용하여 조직의 로고를 사용자 지정할 수 있습니다.	• 허용되는 유일한 이미지 형식은 `.png` 파일에서 변환된 바이너리 데이터 객체입니다.
		• 권장 해상도:
		  • Android: 978 x 190
		  • 데스크톱: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1,650 x 300

암호 찾기 링크	속성을 사용하여 웹 주소를 추가할 수 있습니다. 이 ForgotPasswordLink 속성은 사용자가 비밀번호를 잊은 경우 해당 주소로 이동할 수 WorkSpace 있습니다.	길이 제약: 최소 길이 1자. 최대 길이는 200.

브랜딩 요소	설명	요구 사항 및 권장 사항
로그인 메시지	로그인 화면에서 LoginMessage 속성을 사용하여 메시지를 사용자 지정할 수 있습니다.	• 길이 제약: 최소 길이는 0입니다. HTML 태그 및 다양한 글꼴 크기와의 통합을 위한 최대 길이는 2,000자입니다. HTML 태그가 없는 기본 케이스의 경우 로그인 메시지를 600자 미만으로 유지하는 것이 좋습니다. • 지원되는 HTML 태그: a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul

다음은 사용할 수 있는 샘플 코드 스니펫입니다. ImportClientBranding

AWS CLI 버전 2

> **Warning**
>
> 사용자 지정 브랜딩을 가져오면 해당 플랫폼 내에서 사용자 지정 데이터로 지정한 속성을 덮어씁니다. 또한 지정하지 않은 속성을 기본 사용자 지정 브랜딩 속성 값으로 덮어씁니다. 덮어쓰지 않으려는 모든 속성의 데이터를 포함해야 합니다.

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

가져오기 JSON 파일은 다음 샘플 코드와 유사합니다.

```
{
```

```
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

다음 샘플 Java 코드 스니펫은 로고 이미지를 base64로 인코딩된 문자열로 변환합니다.

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

다음 샘플 Python 코드 스니펫은 로고 이미지를 base64로 인코딩된 문자열로 변환합니다.

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> 사용자 지정 브랜딩을 가져오면 해당 플랫폼 내에서 사용자 지정 데이터로 지정한 속성을 덮어씁니다. 또한 지정하지 않은 속성을 기본 사용자 지정 브랜딩 속성 값으로 덮어씁니다. 덮어쓰지 않으려는 모든 속성의 데이터를 포함해야 합니다.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> 사용자 지정 브랜딩을 가져오면 해당 플랫폼 내에서 사용자 지정 데이터로 지정한 속성을 덮어씁니다. 또한 지정하지 않은 속성을 기본 사용자 지정 브랜딩 속성 값으로 덮어씁니다. 덮어쓰지 않으려는 모든 속성의 데이터를 포함해야 합니다.

```
import boto3

# Read logo into bytearray
```

```
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

로그인 페이지를 미리 보려면 애플리케이션 또는 웹 로그인 페이지를 실행하세요. WorkSpaces

> **Note**
>
> 변경 사항이 표시되는 데 최대 1분이 소요될 수 있습니다.

사용자 지정 브랜딩 설명

현재 사용하고 있는 클라이언트 브랜딩 사용자 지정의 세부 정보를 보려면 `DescribeCustomBranding` 작업을 사용하세요. 다음은 사용하기 위한 샘플 스크립트입니다 DescribeClientBranding. 자세한 내용은 DescribeClientBranding API 참조를 참조하십시오.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

사용자 지정 브랜딩 삭제

클라이언트 브랜딩 사용자 지정을 삭제하려면 `DeleteCustomBranding` 작업을 사용하세요. 다음은 사용을 위한 샘플 스크립트입니다 DeleteClientBranding. 자세한 내용은 DeleteClientBranding API 참조를 참조하십시오.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> 변경 사항이 표시되는 데 최대 1분이 소요될 수 있습니다.

WorkSpaces 리소스 태그 지정

자체 메타데이터를 태그 형태로 각 리소스에 지정하여 WorkSpaces 리소스를 구성하고 관리할 수 있습니다. 각 태그에 대한 키 및 값을 지정합니다. 키는 "project", "owner" 또는 "environment" 등의 특정 연결 값을 가진 일반 범주일 수 있습니다. 태그를 사용하면 간단하면서도 효과적으로 AWS 리소스를 관리하고 결제 데이터를 포함하여 데이터를 구성할 수 있습니다.

기존 리소스에 태그를 추가하면 해당 태그는 다음 달 첫날까지 비용 할당 보고서에 표시되지 않습니다. 예를 들어 7월 15일에 기존 WorkSpaces에 태그를 추가하면 8월 1일까지 태그가 비용 할당 보고서에 표시되지 않습니다. 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

> **Note**
>
> Cost Explorer에서 WorkSpaces 리소스 태그를 보려면 AWS Billing 사용 설명서의 사용자 정의 비용 할당 태그 활성화에 나와 있는 지침에 따라 WorkSpaces 리소스에 적용한 태그를 활성화해야 합니다.
> 태그는 활성화 후 24시간 후에 나타나지만 해당 태그와 관련된 값이 Cost Explorer에 표시되는 데 4~5일이 걸릴 수 있습니다. 또한 Cost Explorer에서 비용 데이터를 표시하고 제공하려면 태그가 지정된 WorkSpaces 리소스에 해당 기간 동안 요금이 발생해야 합니다. Cost Explorer에는 태그가 활성화된 시점 이후의 비용 데이터만 표시됩니다. 현재로서는 과거 데이터가 제공되지 않습니다.

태그 지정이 가능한 리소스

- WorkSpaces, 가져온 이미지, IP 액세스 제어 그룹과 같은 리소스에 태그를 추가할 수 있습니다.
- WorkSpaces, 등록된 디렉터리, 사용자 지정 번들, 이미지, IP 액세스 제어 그룹 등의 기존 리소스에 태그를 추가할 수 있습니다.

태그 제한

- 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 AWS용이므로 태그 이름이나 값에 사용하지 마세요. 이러한 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다.

콘솔을 사용하여 기존 리소스의 태그를 업데이트하는 방법(디렉터리, WorkSpaces 또는 IP 액세스 제어 그룹)

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 리소스 유형으로 디렉터리, WorkSpaces 또는 IP 액세스 제어 중 하나를 선택합니다.
3. 리소스를 선택하여 세부 정보 페이지를 엽니다.
4. 다음 중 한 개 이상을 수행할 수 있습니다.

- 태그를 업데이트하려면 [Key] 및 [Value] 값을 수정합니다.
- 태그를 추가하려면 [Add Tag]를 선택한 다음 [Key] 및 [Value] 값을 편집합니다.
- 태그를 삭제하려면 해당 태그 옆의 삭제 아이콘(X)을 선택합니다.

5. 태그 업데이트를 마쳤으면 [Save]를 선택합니다.

콘솔을 사용하여 기존 리소스의 태그를 업데이트하는 방법(이미지 또는 번들)

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 리소스 유형으로 번들 또는 이미지 중 하나를 선택합니다.
3. 리소스를 선택하여 세부 정보 페이지를 엽니다.
4. 태그에서 태그 관리를 선택합니다.
5. 다음 중 한 개 이상을 수행할 수 있습니다.

- 태그를 업데이트하려면 [Key] 및 [Value] 값을 수정합니다.
- 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
- 태그를 삭제하려면 태그 옆의 제거를 선택합니다.

6. 태그 업데이트를 마쳤으면 변경 사항 저장을 선택합니다.

AWS CLI를 사용하여 기존 리소스의 태그를 업데이트하려면

create-tags 및 delete-tags 명령을 사용합니다.

WorkSpace 유지 관리

정기적으로 WorkSpaces를 유지 관리하는 것이 좋습니다. WorkSpaces는 WorkSpaces의 기본 유지 관리 기간을 예약합니다. 유지 관리 기간 동안 WorkSpace는 Amazon WorkSpaces에서 중요 업데이트를 설치하고 필요에 따라 재부팅합니다. 사용 가능한 경우, WorkSpace가 사용하도록 구성된 OS 업데이트 서버에서도 운영 체제 업데이트가 설치됩니다. 이 유지 관리 기간 동안 WorkSpaces를 사용하지 못할 수 있습니다.

기본적으로 Windows WorkSpaces는 Windows Update에서 업데이트를 받도록 구성됩니다. Windows용 자체 자동 업데이트 메커니즘을 구성하려면 Windows Server Update Services(WSUS) 및 구성 관리자에 대한 설명서를 참조하십시오.

요구 사항

운영 체제 및 배포 애플리케이션에 대한 업데이트를 설치할 수 있도록 WorkSpaces에서 인터넷에 액세스할 수 있어야 합니다. 자세한 내용은 the section called “인터넷 액세스” 섹션을 참조하세요.

AlwaysOn WorkSpaces의 유지 관리 기간

AlwaysOn WorkSpaces의 경우 유지 관리 기간은 운영 체제 설정에 따라 결정됩니다. 기본값은 WorkSpace의 시간대로 매주 일요일 아침 00h00부터 04h00까지 4시간입니다. 기본적으로 AlwaysOn WorkSpace의 시간대는 WorkSpace의 AWS 리전 시간대입니다. 그러나 다른 리전에서 연결하고 시간대 리디렉션을 활성화한 다음 연결을 해제하면 WorkSpace의 시간대가 연결된 리전의 시간대로 업데이트됩니다.

그룹 정책을 사용하여 Windows WorkSpaces에 대한 시간대 리디렉션을 비활성화할 수 있습니다. PCoIP 에이전트 구성을 사용하여 Linux WorkSpaces에 대한 시간대 리디렉션을 비활성화할 수 있습니다.

Windows WorkSpaces의 경우 그룹 정책을 사용하여 유지 관리 기간을 구성할 수 있습니다. 자세한 내용은 자동 업데이트에 대한 그룹 정책 설정 구성을 참조하십시오. Linux WorkSpaces의 경우 유지 관리 기간을 구성할 수 없습니다.

AutoStop Workspaces의 유지 관리 기간

AutoStop WorkSpaces는 중요 업데이트를 설치하기 위해 한 달에 한 번 자동으로 시작됩니다. 매월 세 번째 월요일부터 최대 2주 동안 유지 관리 기간이 WorkSpace의 AWS 리전 시간대로 매일 0시부터 오전 5시 사이에 시작됩니다. 유지 관리 기간 중에는 어느 날이든 하루에 WorkSpace를 유지 관리할 수 있습니다. 이 기간 동안에는 7일이 지난 WorkSpaces만 유지 관리됩니다.

WorkSpace가 유지 관리를 수행하는 기간 동안 WorkSpace의 상태가 `MAINTENANCE`로 설정됩니다.

AutoStop WorkSpaces를 유지 관리하는 데 사용되는 시간대를 수정할 수는 없지만, 다음과 같이 AutoStop WorkSpaces의 유지 관리 기간을 비활성화할 수 있습니다. 유지 관리 모드를 비활성화하면 WorkSpaces가 재부팅되지 않고 `MAINTENANCE` 상태로 설정되지 않습니다.

유지 관리 모드를 비활성화하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Directories]를 선택합니다.
3. 디렉터리를 선택하고 [Actions], [Update Details]를 선택합니다.
4. [Maintenance Mode]를 확장합니다.

5. 자동 업데이트를 사용하려면 활성을 선택합니다. 수동으로 업데이트를 관리하려면 비활성을 선택합니다.
6. [Update and Exit]를 선택합니다.

수동 유지 관리

원하는 경우 WorkSpaces를 원하는 일정대로 유지 관리할 수 있습니다. 유지 관리 작업을 수행할 때는 Workspace의 상태를 유지 관리로 변경하는 것이 좋습니다. 작업이 끝나면 WorkSpace의 상태를 사용 가능으로 변경하세요.

WorkSpace가 유지 관리 상태인 경우 다음 동작이 발생합니다.

- WorkSpace가 재부팅, 중지, 시작 또는 재구축 요청에 응답하지 않습니다.
- 사용자가 WorkSpace에 로그인할 수 없습니다.
- AutoStop WorkSpace가 최대 절전 모드가 아닙니다.

콘솔을 사용하여 WorkSpace의 상태를 변경하려면

> **Note**
>
> WorkSpace 상태를 변경하려면 WorkSpace 상태가 사용 가능이어야 합니다. WorkSpaces가 사용 가능 상태가 아닌 경우 상태 수정 설정을 사용할 수 없습니다.

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. WorkSpace를 선택하고 작업, WorkSpace 수정을 선택합니다.
4. 상태 수정에서 사용 가능 또는 유지 관리를 선택합니다.
5. Save를 선택합니다.

AWS CLI를 사용하여 WorkSpace의 상태를 변경하려면

modify-workspace-state 명령을 사용합니다.

암호화된 WorkSpaces

WorkSpaces가 AWS Key Management Service(AWS KMS)와 통합되어 있습니다. 이 경우 AWS KMS 키를 사용하여 WorkSpaces의 스토리지 볼륨을 암호화할 수 있습니다. WorkSpace를 시작할 때 루트 볼륨(Microsoft Windows의 경우 C 드라이브, Linux의 경우 /)과 사용자 볼륨(Windows의 경우 D 드라이브, Linux의 경우 /home)을 암호화할 수 있습니다. 이렇게 하면 유휴 상태인 저장 데이터, 볼륨에 대한 디스크 I/O 및 볼륨에서 생성된 스냅샷이 모두 암호화됩니다.

> **Note**
>
> WorkSpaces를 암호화하는 것 외에도 특정 AWS 미국 리전에서 FIPS 엔드포인트 암호화를 사용할 수 있습니다. 자세한 내용은 FedRAMP 승인 또는 DoD SRG 준수를 위해 Amazon WorkSpaces 설정 섹션을 참조하세요.

목차

필수 조건

암호화 프로세스를 시작하려면 AWS KMS 키가 필요합니다. 이 KMS 키는 Amazon WorkSpaces용 AWS 관리형 KMS 키(aws/workspaces)이거나 대칭형 고객 관리형 KMS 키일 수 있습니다.

- AWS 관리형 KMS 키 - 리전의 WorkSpaces 콘솔에서 암호화되지 않은 WorkSpace를 처음 시작할 때 Amazon WorkSpaces는 계정에 AWS 관리형 KMS 키(aws/workspaces)를 자동으로 생성합니다. 이 AWS 관리형 KMS 키를 선택하여 WorkSpaces의 사용자 및 루트 볼륨을 암호화할 수 있습니다. 자세한 내용은 AWS KMS를 사용한 WorkSpaces 암호화 개요 섹션을 참조하세요.

  정책 및 권한 부여를 포함하여 이 AWS 관리형 KMS 키를 확인하고 AWS CloudTrail 로그에서 키 사용을 추적할 수 있지만 이 KMS 키를 사용하거나 관리할 수는 없습니다. Amazon WorkSpaces

가 이 KMS 키를 생성하고 관리합니다. Amazon WorkSpaces만 이 KMS 키를 사용할 수 있으며 WorkSpaces는 계정의 WorkSpaces 리소스를 암호화하는 데만 이 키를 사용할 수 있습니다.

Amazon WorkSpaces가 지원하는 키를 포함한 AWS 관리형 KMS 키는 3년마다 교체됩니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 Rotating AWS KMS Key를 참조하세요.

- 고객 관리형 KMS 키 - 또는 AWS KMS를 사용하여 생성한 대칭형 고객 관리형 KMS 키를 선택할 수도 있습니다. 정책 설정을 포함하여 이 KMS 키를 확인, 사용 및 관리할 수 있습니다. KMS 키 생성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 생성을 참조하세요. AWS KMS API를 사용하여 KMS 키를 생성하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 작업을 참조하세요.

  자동 키 교체를 활성화하지 않는 한 고객 관리형 KMS 키는 자동으로 교체되지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 Rotating AWS KMS Key를 참조하세요.

> **Important**
>
> KMS 키를 수동으로 교체할 때는 원래 KMS 키가 암호화한 WorkSpaces를 AWS KMS가 해독할 수 있도록 원래 KMS 키와 새 KMS 키를 모두 활성화한 상태로 유지해야 합니다. 원래 KMS 키를 활성화한 상태로 유지하지 않으려면 WorkSpaces를 다시 생성하고 새 KMS 키를 사용하여 암호화해야 합니다.

AWS KMS 키를 사용하여 WorkSpaces를 암호화하려면 다음 요구 사항을 충족해야 합니다.

- KMS 키는 대칭이어야 합니다. Amazon WorkSpaces는 비대칭 KMS 키를 지원하지 않습니다. 대칭 KMS 키와 비대칭 KMS 키를 구분하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 대칭 및 비대칭 KMS 키 식별을 참조하세요.
- KMS 키를 활성화해야 합니다. KMS 키의 활성화 여부를 확인하려면 AWS Key Management Service 개발자 안내서의 KMS 키 세부 정보 표시를 참조하세요.
- 올바른 권한과 정책이 KMS 키에 연결되어 있어야 합니다. 자세한 내용은 2부: IAM 정책을 사용하여 WorkSpaces 관리자에게 추가 권한 부여 섹션을 참조하세요.

제한

- 기존 WorkSpace는 암호화할 수 없습니다. WorkSpace를 시작할 때 암호화해야 합니다.
- 암호화된 WorkSpaces에서 사용자 정의 이미지를 생성하는 기능은 지원되지 않습니다.

- 암호화된 WorkSpaces에 대해 암호화를 비활성화하는 기능은 현재 지원되지 않습니다.
- 루트 볼륨 암호화를 활성화한 상태로 시작된 WorkSpaces를 프로비저닝하는 데 최대 1시간이 소요될 수 있습니다.
- 암호화된 WorkSpace를 재부팅하거나 재구축하려면 먼저 AWS KMS 키가 활성화되어 있는지 확인합니다. 활성화되어 있지 않으면 WorkSpace를 사용할 수 없습니다. KMS 키의 활성화 여부를 확인하려면 AWS Key Management Service 개발자 안내서의 KMS 키 세부 정보 표시를 참조하세요.

AWS KMS를 사용한 WorkSpaces 암호화 개요

암호화된 볼륨으로 WorkSpaces를 만들면 WorkSpaces가 Amazon Elastic Block Store(Amazon EBS)를 이용해 이러한 볼륨을 만들고 관리합니다. Amazon EBS는 산업 표준 AES-256 알고리즘을 사용하여 데이터 키로 볼륨을 암호화합니다. Amazon EBS와 Amazon WorkSpaces는 모두 KMS 키를 사용하여 암호화된 볼륨으로 작업합니다. EBS 볼륨 암호화에 대한 자세한 내용은 Amazon EC2 Linux 인스턴스용 사용 설명서의 Amazon EBS 암호화를 참조하세요.

암호화된 볼륨으로 WorkSpaces를 시작하면 종단 간 프로세스는 다음과 같습니다.

1. 암호화에 사용할 KMS 키와 WorkSpace의 사용자와 디렉터리를 지정합니다. 이 작업은 WorkSpaces가 이 WorkSpace에 대해서만, 즉 지정된 사용자 및 디렉터리와 연결된 WorkSpace에 대해서만 KMS 키를 사용할 수 있도록 허용하는 권한을 생성합니다.
2. WorkSpaces는 WorkSpace에 사용할 암호화된 EBS 볼륨을 생성하고, 사용할 KMS 키와 볼륨의 사용자 및 디렉터리를 지정합니다. 이 작업은 Amazon EBS가 이 WorkSpace 및 볼륨에 대해서만, 즉 지정된 사용자 및 디렉터리와 연결된 WorkSpace에 대해서만 지정된 볼륨에 대해서만 KMS 키를 사용할 수 있도록 허용하는 권한을 생성합니다.
3. Amazon EBS는 KMS 키를 사용하여 암호화된 볼륨 데이터 키를 요청하고 WorkSpace 사용자의 Active Directory 보안 식별자(SID) 및 AWS Directory Service 디렉터리 ID, Amazon EBS 볼륨 ID를 암호화 컨텍스트로 지정합니다.
4. AWS KMS가 새 데이터 키를 생성하고 KMS 키를 사용하여 암호화한 후, 암호화된 데이터 키를 모두 Amazon EBS로 보냅니다.
5. WorkSpaces는 Amazon EBS를 사용하여 암호화된 볼륨을 WorkSpace Space에 연결합니다. Amazon EBS는 `Decrypt` 요청과 함께 암호화된 데이터 키를 AWS KMS에 보내고 WorkSpace 사용자의 SID, 디렉터리 ID 및 암호화 컨텍스트로 사용되는 볼륨 ID를 지정합니다.
6. AWS KMS는 KMS 키를 이용해 데이터 키를 해독한 후 일반 텍스트 데이터 키를 Amazon EBS로 보냅니다.

7. Amazon EBS에서는 일반 텍스트 데이터 키를 이용해 암호화된 볼륨으로 들어오거나 나가는 모든 데이터를 암호화합니다. 볼륨이 WorkSpace Space에 연결되어 있는 동안에는 Amazon EBS는 일반 텍스트 데이터 키를 메모리에 유지합니다.
8. Amazon EBS는 나중에 WorkSpace를 재부팅하거나 다시 빌드할 때 사용할 볼륨 메타데이터로 암호화된 데이터 키(Step 4에서 수신)를 저장합니다.
9. AWS Management Console을 사용하여 WorkSpace를 제거하거나 WorkSpaces API에서 `TerminateWorkspaces` 작업을 사용하면 WorkSpaces 및 Amazon EBS는 해당 WorkSpace에 대해 KMS 키를 사용할 수 있도록 허용한 권한을 폐기합니다.

WorkSpaces 암호화 컨텍스트

WorkSpaces는 암호화 작업(예: `Encrypt`, `Decrypt`, `GenerateDataKey` 등)에 KMA 키를 직접 사용하지 않습니다. 즉, WorkSpaces는 암호화 컨텍스트가 포함된 요청을 AWS KMS에 보내지 않습니다. 그러나 Amazon EBS가 WorkSpaces의 암호화된 볼륨(AWS KMS를 사용한 WorkSpaces 암호화 개요의 Step 3)에 대해 암호화된 데이터 키를 요청하고 해당 데이터 키(Step 5)의 일반 텍스트 사본을 요청할 때 요청에 암호화 컨텍스트를 포함합니다.

암호화 컨텍스트는 AWS KMS가 데이터 무결성을 보장하기 위해 사용하는 추가 인증 데이터(AAD)를 제공합니다. 암호화 컨텍스트는 AWS CloudTrail 로그 파일에도 기록되어, 해당 KMS 키가 사용된 이유를 이해하는 데 도움을 줍니다. Amazon EBS는 암호화 컨텍스트에 대해 다음을 사용합니다.

- WorkSpace와 연결된 Active Directory 사용자의 보안 식별자(SID)
- WorkSpace에 연결된 AWS Directory Service 디렉터리의 디렉터리 ID
- 암호화된 볼륨의 Amazon EBS 볼륨 ID

다음 예는 Amazon EBS가 사용하는 암호화 컨텍스트의 JSON 표시를 보여줍니다.

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces에 사용자 대신 KMS 키를 사용할 수 있는 권한 부여

WorkSpaces용 AWS 관리형 KMS 키(aws/workspaces) 또는 고객 관리형 KMS 키를 사용하여 WorkSpace 데이터를 보호할 수 있습니다. 고객 관리형 KMS 키를 사용하는 경우, 계정의 WorkSpaces

관리자를 대신해 WorkSpaces에 KMS 키를 사용할 수 있는 권한을 부여해야 합니다. WorkSpaces용 AWS 관리형 KMS 키에는 기본적으로 필요한 권한이 있습니다.

WorkSpaces에서 사용하도록 고객 관리형 KMS 키를 준비하려면 다음 절차를 따르세요.

1. KMS 키의 키 정책에 있는 키 사용자 목록에 WorkSpaces 관리자 추가
2. WorkSpaces 관리자에게 IAM 정책 관련 추가 권한 부여

WorkSpaces 관리자는 WorkSpaces를 사용할 수 있는 권한도 필요합니다. 이러한 권한에 대한 자세한 내용은 WorkSpaces의 Identity and Access Management 섹션을 참조하세요.

1부: 키 사용자에 WorkSpaces 관리자 추가

WorkSpaces 관리자에게 필요한 권한을 제공하기 위해 AWS Management Console 또는 AWS KMS API를 사용할 수 있습니다.

WorkSpaces 관리자를 KMS 키의 키 사용자로 추가하는 방법(콘솔)

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/kms에서 AWS Key Management Service(AWS KMS) 콘솔을 엽니다.
2. AWS 리전을 변경하려면 페이지의 오른쪽 상단 모서리에 있는 리전 선택기를 사용합니다.
3. 탐색 창에서 고객 관리형 키(Customer managed keys)를 선택합니다.
4. 선호하는 고객 관리형 KMS 키의 키 ID 또는 별칭을 선택합니다.
5. 키 정책(Key policy) 탭을 선택합니다. 키 사용자에서 추가(Add)를 선택합니다.
6. IAM 사용자 및 역할 목록에서 WorkSpaces 관리자에 해당하는 사용자와 역할을 선택한 후 추가를 선택합니다.

WorkSpaces 관리자를 KMS 키의 키 사용자로 추가하는 방법(API)

1. GetKeyPolicy 작업을 이용해 기존 키 정책을 검색한 다음, 이 정책 문서를 파일에 저장합니다.
2. 원하는 텍스트 편집기에서 정책 문서를 엽니다. WorkSpaces 관리자에 해당하는 IAM 사용자와 역할을 키 사용자에게 권한을 부여하는 정책 문에 추가합니다. 그런 다음 파일을 저장합니다.
3. PutKeyPolicy 작업을 이용해 KMS 키에 키 정책을 적용합니다.

2부: IAM 정책을 사용하여 WorkSpaces 관리자에게 추가 권한 부여

암호화에 사용할 고객 관리형 KMS 키를 선택한 경우, 암호화된 WorkSpaces를 시작하는 계정의 IAM 사용자를 대신해 Amazon WorkSpaces가 해당 KMS 키를 사용할 수 있도록 허용하는 IAM 정책을 설정해야 합니다. 또한 해당 사용자에게는 Amazon WorkSpaces 사용 권한이 필요합니다. IAM 사용자 정책 생성 및 편집에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 관리 및 WorkSpaces의 Identity and Access Management 섹션을 참조하세요.

WorkSpaces 암호화에는 KMS 키에 대한 제한된 액세스가 필요합니다. 다음은 사용 가능한 샘플 키 정책입니다. 이 정책은 AWS KMS KMS 키를 관리할 수 있는 보안 주체와 이 키를 사용할 수 있는 보안 주체를 구분합니다. 이 샘플 키 정책을 사용하기 전에 예시 계정 ID와 IAM 사용자 이름을 계정의 실제 값으로 바꿉니다.

첫 번째 문은 기본 AWS KMS 키 정책과 일치합니다. 이는 KMS 키에 대한 액세스를 제어할 수 있도록 IAM 정책을 사용할 수 있는 계정 권한을 부여합니다. 두 번째 및 세 번째 문은 각각 키를 관리 및 사용할 수 있는 AWS 보안 주체를 정의합니다. 네 번째 문은 AWS KMS와 통합된 AWS 서비스에서 지정된 보안 주체를 대신하여 키를 사용할 수 있도록 해줍니다. 이 문을 사용하여 AWS 서비스에서 권한을 생성 및 관리할 수 있습니다. 이 문은 KMS 키에 대한 권한 부여를 계정의 사용자를 대신해 AWS 서비스가 제공하는 권한 부여로 제한하는 조건 요소를 사용합니다.

> **Note**
>
> WorkSpaces 관리자가 AWS Management Console을 사용하여 암호화된 볼륨으로 WorkSpaces를 생성하는 경우에는 관리자에게 별칭 및 키를 나열할 수 있는 권한("kms:ListAliases" 및 "kms:ListKeys" 권한)이 필요합니다. WorkSpaces 관리자가 콘솔이 아닌 Amazon WorkSpaces API만 사용하는 경우, "kms:ListAliases" 및 "kms:ListKeys" 권한을 생략할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

WorkSpace를 암호화 중인 사용자 또는 역할에 대한 IAM 정책은 고객 관리형 KMS 키에 대한 사용 권한 및 WorkSpaces에 대한 액세스 권한을 포함해야 합니다. IAM 사용자 또는 역할에 WorkSpaces 권한을 부여하려면 다음 샘플 정책을 IAM 사용자 또는 역할에 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

다음 IAM 정책은 사용자가 AWS KMS를 사용하기 위해 필요합니다. 이 정책은 권한 부여 생성 가능과 더불어 KMS 키에 대한 읽기 전용 액세스 권한을 사용자에게 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

정책에 KMS 키를 지정하려면 다음과 유사한 IAM 정책을 사용하세요. 예시에서 KMS 키 ARN을 유효한 ARN으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

WorkSpace 암호화

WorkSpaces를 암호화하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. [Launch WorkSpaces]를 선택하고 처음 세 단계를 완료합니다.
3. [WorkSpaces Configuration] 단계에서 다음을 수행합니다.
   a. 암호화할 볼륨을 선택합니다. [Root Volume], [User Volume] 또는 두 볼륨 모두.
   b. 암호화 키에서 Amazon WorkSpaces에서 생성한 AWS 관리형 KMS 키 또는 직접 생성한 KMS 키 중 하나로 AWS KMS 키를 선택합니다. 선택하는 KMS 키는 대칭이어야 합니다. Amazon WorkSpaces는 비대칭 KMS 키를 지원하지 않습니다.
   c. 다음 단계(Next Step)를 선택합니다.
4. [Launch WorkSpaces]를 선택합니다.

암호화된 WorkSpaces 보기

WorkSpaces 콘솔에서 어느 WorkSpaces 및 볼륨이 암호화되었는지 확인하려면 왼쪽에 있는 탐색 모음에서 WorkSpaces를 선택합니다. [Volume Encryption] 열에는 각 WorkSpaces에서 암호화가 활성화 또는 비활성화되었는지 여부가 표시됩니다. 특정 볼륨이 암호화되었는지 확인하려면 WorkSpaces 항목을 확장하여 [Encrypted Volumes] 필드를 확인하십시오.

재부팅 a WorkSpace

경우에 따라 WorkSpace 수동으로 재부팅 (재시작) 해야 할 수도 있습니다. 를 재부팅하면 사용자 WorkSpace 연결이 끊긴 다음 사용자가 종료되고 재부팅됩니다. WorkSpace 데이터 손실을 방지하려면 를 재부팅하기 전에 사용자가 열려 있는 문서 및 기타 응용 프로그램 파일을 모두 저장했는지 확인하십시오. WorkSpace 사용자 데이터, 운영 체제 및 시스템 설정은 영향을 받지 않습니다.

> **Warning**
>
> WorkSpace암호화된 파일을 재부팅하려면 먼저 키가 활성화되어 있는지 확인하십시오. 그렇지 않으면 AWS KMS 키를 사용할 수 WorkSpace 없게 됩니다. KMS 키의 활성화 여부를 확인하려면 AWS Key Management Service 개발자 안내서의 KMS 키 세부 정보 표시를 참조하세요.

재부팅하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. WorkSpaces 재부팅할 항목을 선택하고 작업, 재부팅을 선택합니다 WorkSpaces.
4. 확인 메시지가 표시되면 재부팅을 선택합니다 WorkSpaces.

를 WorkSpace 사용하여 재부팅하려면 AWS CLI

reboot-workspaces 명령을 사용하세요.

대량 재부팅하려면 WorkSpaces

를 사용하십시오 amazon-workspaces-admin-module.

재구축 a WorkSpace

를 재구축하면 WorkSpace 실행된 번들의 가장 최근 이미지, 사용자 볼륨 및 기본 Elastic network 인터페이스의 루트 볼륨이 WorkSpace 다시 생성됩니다. 재구축은 a를 복원하는 것보다 더 많은 데이터를 WorkSpace 삭제하지만 사용자 볼륨의 스냅샷만 있으면 됩니다. WorkSpace a를 WorkSpace 복원하려면 을 참조하십시오. WorkSpace 복원

a를 WorkSpace 재구축하면 다음과 같은 결과가 발생합니다.

- 루트 볼륨 (Microsoft Windows의 경우 C 드라이브, Linux의 경우/) 이 WorkSpace 생성된 번들의 최신 이미지로 새로 고쳐집니다. 설치된 모든 애플리케이션 또는 생성 후 변경된 시스템 설정은 손실됩니다. WorkSpace
- 사용자 볼륨(Microsoft Windows의 경우 D 드라이브, Linux의 경우 /home)이 가장 최근 스냅샷에서 다시 생성됩니다. 데이터 볼륨의 현재 내용을 덮어씁니다.

  a를 재구축할 때 사용할 자동 스냅샷은 12시간마다 WorkSpace 예약됩니다. 사용자 볼륨의 이러한 스냅샷은 상태 여부에 관계없이 생성됩니다. WorkSpace 작업, 재구축/복원을 WorkSpace 선택하면 가장 최근 스냅샷의 날짜와 시간이 표시됩니다.

  a를 재구축하면 재구축이 완료된 직후 (보통 30분 이내) 새 스냅샷도 생성됩니다. WorkSpace
- 기본 탄력적 네트워크 인터페이스가 다시 생성됩니다. 는 새 사설 IP 주소를 WorkSpace 받습니다.

> **Important**
>
> 2020년 1월 14일 이후에는 퍼블릭 Windows 7 번들로 WorkSpaces 만든 번들을 더 이상 다시 빌드할 수 없습니다. Windows WorkSpaces 7을 Windows 10으로 마이그레이션하는 것을 고려해 볼 수 있습니다. 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.

다음 조건이 충족되는 WorkSpace 경우에만 a를 다시 빌드할 수 있습니다.

- 의 상태는`AVAILABLE`,, `ERROR` `UNHEALTHY`또는 `STOPPED`, 또는 WorkSpace `REBOOTING` 이어야 합니다. `REBOOTING`상태에서 를 다시 빌드하려면 RebuildWorkspacesAPI 작업 또는 AWS CLI rebuild-workspaces 명령을 사용해야 합니다. WorkSpace
- 사용자 볼륨의 스냅샷이 있어야 합니다.

다시 빌드하려면 WorkSpace

> **Warning**
>
> WorkSpace암호화된 키를 재구축하려면 먼저 키가 활성화되어 있는지 확인하십시오. 그렇지 않으면 AWS KMS 키를 사용할 수 WorkSpace 없게 됩니다. KMS 키의 활성화 여부를 확인하려면 AWS Key Management Service 개발자 안내서의 KMS 키 세부 정보 표시를 참조하세요.

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. WorkSpace 재빌드할 항목을 선택하고 작업, 재구축/복원을 선택합니다. WorkSpace
4. 스냅샷에서 스냅샷의 타임스탬프를 선택합니다.
5. Rebuild(재구축)를 선택합니다.

를 사용하여 재구축하려면 WorkSpace AWS CLI

rebuild-workspaces 명령을 사용합니다.

문제 해결

Active Directory에서 사용자의 SaM AccountName 사용자 이름 지정 속성을 변경한 WorkSpace 후 a를 다시 빌드하면 다음과 같은 오류 메시지가 표시될 수 있습니다.

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

이 문제를 해결하려면 원래 사용자 이름 지정 속성으로 되돌아간 다음 재구축을 다시 시작하거나 해당 사용자를 위해 새 이름을 만드십시오. WorkSpace

WorkSpace 복원

WorkSpace를 복구하면 WorkSpace가 정상일 때 생성된 볼륨의 가장 최근 스냅샷을 기반으로 루트 볼륨과 사용자 볼륨이 모두 다시 생성됩니다. WorkSpace를 복원하면 WorkSpace를 재구축하는 것보다 삭제되는 데이터가 적습니다. 그러나 WorkSpace를 재구축하려면 사용자 볼륨의 스냅샷만 필요한 반면, WorkSpace를 복원하려면 루트 볼륨과 사용자 볼륨의 스냅샷이 필요합니다. WorkSpace를 재구축하려면 재구축 a WorkSpace 섹션을 참조하세요.

WorkSpace를 복원하면 다음과 같이 됩니다.

- 루트 볼륨(Microsoft Windows의 경우 C 드라이브, Linux의 경우 /)이 가장 최근의 스냅샷으로 복원됩니다. 가장 최근 스냅샷이 생성된 이후에 변경된 시스템 설정 또는 설치된 애플리케이션이 손실됩니다.
- 사용자 볼륨(Microsoft Windows의 경우 D 드라이브, Linux의 경우 /home)이 가장 최근 스냅샷에서 다시 생성됩니다. 데이터 볼륨의 현재 내용을 덮어씁니다.

스냅샷을 촬영한 시점

루트 및 사용자 볼륨의 스냅샷은 다음과 같은 기준으로 생성됩니다. 작업, WorkSpaces 재구축/복원을 선택하면 가장 최근 스냅샷의 날짜와 시간이 표시됩니다.

- WorkSpace가 처음 생성된 후 - 일반적으로 루트 및 사용자 볼륨의 초기 스냅샷은 WorkSpace가 생성된 직후(보통 30분 이내) 생성됩니다. 일부 AWS 리전에서는 WorkSpace를 생성한 후 초기 스냅샷을 생성하는 데 몇 시간이 걸릴 수 있습니다.

  초기 스냅샷을 생성하기 전에 WorkSpace가 비정상 상태가 되면 WorkSpace를 복원할 수 없습니다. 이 경우 WorkSpace를 재구축하거나 AWS Support에 문의하여 도움을 받을 수 있습니다.
- 규칙적인 사용 중 - WorkSpace를 복원할 때 사용할 자동 스냅샷이 12시간마다 예약됩니다. WorkSpace가 정상이면 루트 볼륨과 사용자 볼륨의 스냅샷이 거의 동시에 생성됩니다. WorkSpace가 정상이 아니면 사용자 볼륨의 스냅샷만 생성됩니다.
- WorkSpace가 복원된 후 - WorkSpace를 복원하면 복원이 완료된 직후(보통 30분 이내) 새 스냅샷이 생성됩니다. 일부 AWS 리전에서는 WorkSpace를 복원한 후 스냅샷을 생성하는 데 몇 시간이 걸릴 수 있습니다.

  WorkSpace가 복원된 후 새 스냅샷을 생성하기 전에 WorkSpace가 비정상 상태가 되면 WorkSpace를 다시 복원할 수 없습니다. 이 경우 WorkSpace를 재구축하거나 AWS Support에 문의하여 도움을 받을 수 있습니다.

WorkSpace는 다음 조건이 충족될 때만 복원할 수 있습니다.

- WorkSpace 상태는`AVAILABLE`, `ERROR`, `UNHEALTHY` 또는 `STOPPED`여야 합니다.
- 루트 및 사용자 볼륨의 스냅샷이 있어야 합니다.

WorkSpace를 복원하려면

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. 복원할 WorkSpace를 선택하고 작업, WorkSpace 재구축/복원을 선택합니다.
4. 스냅샷에서 스냅샷의 타임스탬프를 선택합니다.
5. 복원(Restore)을 선택합니다.

AWS CLI를 사용하여 WorkSpaces를 복원하는 방법

restore-workspace 명령을 사용합니다.

Microsoft 365 기존 보유 라이선스 사용(BYOL)

WorkSpaces Amazon에서는 Microsoft의 라이선스 요구 사항을 충족하는 경우 자체 Microsoft 365 라이선스를 가져올 수 있도록 허용합니다. 이러한 라이선스를 통해 다음 운영 체제에서 WorkSpaces 구동되는 Microsoft 365 Apps for 엔터프라이즈 소프트웨어를 설치하고 활성화할 수 있습니다.

- Windows 10(기존 보유 라이선스 사용)
- Windows 11(기존 보유 라이선스 사용)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

엔터프라이즈용 Microsoft 365 앱을 사용하려면 마이크로소프트 365 E3/E5 WorkSpaces, 마이크로소프트 365 A3/A5 또는 마이크로소프트 365 비즈니스 프리미엄에 가입해야 합니다.

WorkSpaces Amazon에서는 Microsoft 365 라이선스를 사용하여 다음과 같은 엔터프라이즈용 Microsoft 365 앱을 설치하고 활성화할 수 있습니다.

- Microsoft Word
- Microsoft Excel
- 마이크로소프트 PowerPoint
- Microsoft Outlook
- 마이크로소프트 OneDrive

자세한 내용은 엔터프라이즈용 Microsoft 365 앱의 전체 목록을 참조하세요.

Microsoft Project, Microsoft Visio, Microsoft Power Automate와 같이 Microsoft 365에 포함되지 않은 Microsoft 응용 프로그램을 설치할 수도 WorkSpaces 있지만 추가 라이선스를 가져와야 합니다.

다중 지역 복구를 사용하여 Microsoft 365 및 기타 Microsoft 애플리케이션을 기본 WorkSpaces 및 페일오버에 설치하고 WorkSpaces 사용할 수 있습니다.

내용

- 마이크로소프트 365 엔터프라이즈용 WorkSpaces 앱으로 제작하세요
- 기존 앱을 WorkSpaces 마이그레이션하여 엔터프라이즈용 Microsoft 365 앱을 사용할 수 있습니다.
- 엔터프라이즈용 Microsoft 365 앱을 업데이트하세요 WorkSpaces

마이크로소프트 365 엔터프라이즈용 WorkSpaces 앱으로 제작하세요

Microsoft 365 Apps for Enterprise를 사용하여 생성하려면 애플리케이션이 설치된 사용자 지정 이미지를 만들고 WorkSpaces 이를 사용하여 사용자 지정 번들을 만들어야 합니다. 번들을 사용하여 애플리케이션이 설치된 새 WorkSpaces 번들을 시작할 수 있습니다. WorkSpaces 기업용 Microsoft 365 앱과 함께 제공되는 공개 번들을 제공하지 않습니다.

엔터프라이즈용 Microsoft 365 앱을 WorkSpaces 사용하여 만들려면:

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 다른 Microsoft 응용 프로그램의 이미지로 사용할 이미지를 실행합니다 WorkSpaces. WorkSpace 여기에서 Microsoft 애플리케이션을 설치합니다. 실행에 대한 자세한 내용은 를 WorkSpace 사용하여 가상 데스크톱 시작을 참조하십시오 WorkSpaces.
3. https://clients.amazonworkspaces.com/에서 클라이언트 애플리케이션을 시작하고 초대 이메일에 있는 등록 코드를 입력한 다음 등록을 선택합니다.
4. 로그인하라는 메시지가 표시되면 사용자의 로그인 보안 인증 정보를 입력한 다음 로그인을 선택합니다.
5. 엔터프라이즈용 Microsoft 365 Apps를 설치하고 구성합니다.
6. 에서 사용자 지정 이미지를 만들고 이를 사용하여 사용자 지정 번들을 생성합니다. WorkSpace 사용자 지정 이미지 및 번들 생성에 대한 자세한 내용은 사용자 지정 WorkSpaces 이미지 및 번들 생성을 참조하십시오.
7. 생성한 사용자 지정 번들을 WorkSpaces 사용하여 실행하십시오. 여기에는 WorkSpaces 기업용 Microsoft 365 앱이 설치되어 있습니다.

기존 앱을 WorkSpaces 마이그레이션하여 엔터프라이즈용 Microsoft 365 앱을 사용할 수 있습니다.

Microsoft Office 라이선스가 WorkSpaces 없는 경우 엔터프라이즈용 Microsoft 365 앱을 설치하고 구성할 수 있습니다 WorkSpaces. AWS

Microsoft Office 라이선스를 AWS 보유한 경우 엔터프라이즈용 Microsoft 365 앱을 설치하기 전에 먼저 Microsoft Office 라이선스의 등록을 취소해야 합니다. WorkSpaces

Important

Microsoft Office 응용 프로그램을 제거해도 라이선스 등록은 WorkSpaces 취소되지 않습니다. Microsoft Office 라이선스에 대한 요금이 부과되지 않도록 하려면 다음 중 하나를 AWS 수행하여 Microsoft Office WorkSpaces 애플리케이션에서 등록을 취소하십시오.

- 응용 프로그램 관리 (권장) - 귀하의 WorkSpaces 응용 프로그램에서 Microsoft Office 2016 및 2019를 제거할 수 있습니다. 자세한 내용은 Manage applications를 참조하세요. 제거한 후에는 기업용 Microsoft 365 앱을 사용자 WorkSpaces 컴퓨터에 설치할 수 있습니다.
- a 마이그레이션 WorkSpace - 사용자 볼륨의 WorkSpace 데이터를 유지하면서 한 번들에서 다른 번들로 마이그레이션할 수 있습니다.
  - Microsoft WorkSpaces Office를 구독하지 않는 이미지가 포함된 번들로 마이그레이션하세요. 마이그레이션이 완료되면 엔터프라이즈용 Microsoft 365 앱을 사용자 컴퓨터에 설치할 수 있습니다 WorkSpaces.
  - 또는 WorkSpaces 이미지에 Microsoft 365 Apps for Enterprise가 이미 설치되어 있는 사용자 지정 이미지와 번들을 만든 다음 이 새 사용자 지정 번들로 WorkSpaces 마이그레이션할 수 있습니다. 마이그레이션이 완료되면 WorkSpaces 사용자는 엔터프라이즈용 Microsoft 365 앱을 사용하기 시작할 수 있습니다.
  - 마이그레이션 방법에 대한 자세한 내용은 마이그레이션 WorkSpaces a를 참조하십시오 WorkSpace.

엔터프라이즈용 Microsoft 365 앱을 업데이트하세요 WorkSpaces

기본적으로 Microsoft Windows 운영 체제에서 WorkSpaces 실행 중인 사용자는 Windows Update에서 업데이트를 받도록 구성되어 있습니다. 그러나 엔터프라이즈용 Microsoft 365 Apps의 업데이트는 Windows Update를 사용하여 수행할 수 없습니다. Office CDN에서 자동으로 실행되도록 업데이트를 설정하거나 Microsoft Configuration Manager와 함께 Windows Server Update

Services(WSUS)를 사용하여 엔터프라이즈용 Microsoft 365 Apps를 업데이트할 수 있습니다. 자세한 내용은 Microsoft Manage updates to Microsoft 365 Apps with Microsoft Configuration Manager를 참조하세요. Microsoft 365 응용 프로그램 업데이트 빈도를 설정하려면 업데이트 채널을 지정하고 Microsoft 365 WorkSpaces 라이선스 정책을 준수하도록 현재 또는 월간 엔터프라이즈로 설정합니다.

윈도우 BYOL 업그레이드 WorkSpaces

Windows BYOL (기존 보유 라이선스 사용) WorkSpaces 에서 전체 업그레이드 프로세스를 사용하여 새 버전의 Windows로 업그레이드할 수 있습니다. 업그레이드하려면 이 항목의 지침을 따르십시오.

인플레이스 업그레이드 프로세스는 Windows 10 및 11 BYOL에만 적용됩니다. WorkSpaces

> **Important**
>
> 업그레이드된 버전에서는 Sysprep을 실행하지 마십시오. WorkSpace 이렇게 하면 Sysprep 완료를 방해하는 오류가 발생할 수 있습니다. Sysprep을 실행하려는 경우 업그레이드되지 않은 시스템에서만 실행하십시오. WorkSpace

> **Note**
>
> 이 프로세스를 사용하여 Windows 10 및 11을 최신 버전으로 WorkSpaces 업그레이드할 수 있습니다. 그러나 이 프로세스를 사용하여 Windows 10을 Windows 11로 WorkSpaces 업그레이드할 수는 없습니다.

내용

필수 조건

- 그룹 정책 또는 SCCM (시스템 센터 구성 관리자) 을 사용하여 Windows 10 및 11 업그레이드를 연기하거나 일시 중지한 경우 Windows 10 및 11의 운영 체제 업그레이드를 사용하도록 설정합니다. WorkSpaces
- AutoStop WorkSpace인 경우 업데이트가 적용되는 동안 자동으로 중지되지 않도록 전체 업그레이드 프로세스 AlwaysOn WorkSpace 전으로 변경하십시오. WorkSpace 자세한 정보는 실행 모드 수정을 참조하세요. WorkSpace 설정을 그대로 유지하려면 업그레이드가 진행되는 동안 AutoStop 시간을 3시간 이상으로 변경하십시오. AutoStop
- 인플레이스 업그레이드 프로세스는 Default User(`C:\Users\Default`)라는 특수 프로필의 사본을 복사하여 사용자 프로필을 다시 생성합니다. 사용자 지정을 수행하는 데 이 기본 사용자 프로필을 사용하지 마십시오. 그룹 정책 객체(GPO)를 통해 사용자 프로필을 사용자 지정하는 것이 좋습니다. GPO를 통한 사용자 지정은 쉽게 수정하거나 롤백할 수 있으며 오류가 발생할 가능성이 낮습니다.
- 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.

고려 사항

전체 업그레이드 프로세스에서는 두 개의 레지스트리 스크립트 (`enable-inplace-upgrade.ps1`및`update-pvdrivers.ps1`) 를 사용하여 Windows Update 프로세스를 실행할 수 WorkSpaces 있도록 필요한 변경 작업을 수행합니다. 이러한 변경에는 D 드라이브 대신에 C 드라이브에 (임시) 사용자 프로필을 생성하는 작업이 포함됩니다. 사용자 프로필이 이미 D 드라이브에 있는 경우 원래 사용자 프로필의 데이터는 D 드라이브에 남아있게 됩니다.

기본적으로 에서 `D:\Users\%USERNAME%` 사용자 프로필을 WorkSpaces 만듭니다. `enable-inplace-upgrade.ps1` 스크립트는 새 사용자 프로필을 `C:\Users\%USERNAME%`에 생성하도록 Windows를 구성하고 사용자 셸 폴더를 `D:\Users\%USERNAME%`로 리디렉션합니다. 이 새 사용자 프로필은 사용자가 처음 로그온할 때 생성됩니다.

인플레이스 업그레이드 후, 사용자가 나중에 Windows Update 프로세스를 사용하여 시스템을 업그레이드할 수 있도록 사용자 프로필을 C 드라이브에 그대로 둘 수도 있습니다. 하지만 C 드라이브에 저장된 프로필은 데이터를 직접 백업하고 복원하지 않는 한 사용자 프로필의 모든 데이터를 손실하지 않고 다시 빌드하거나 마이그레이션할 수 없다는 WorkSpaces 점에 유의하십시오. 프로필을 C 드라이브에 그대로 두려면 이 항목의 뒷부분에서 설명하는 대로 UserShellFoldersRedirection레지스트리 키를 사용하여 사용자 셸 폴더를 D 드라이브로 리디렉션할 수 있습니다.

을 (를) 다시 빌드하거나 마이그레이션할 수 WorkSpaces 있고 사용자 셸 폴더 리디렉션과 관련된 잠재적 문제를 방지하려면 전체 업그레이드 후 드라이브 D에 사용자 프로필을 복원하도록 선택하는 것이 좋습니다. 이 항목의 뒷부분에서 설명하는 대로 PostUpgradeRestoreProfileOnD 레지스트리 키를 사용하여 이 작업을 수행할 수 있습니다.

알려진 제한 사항

- WorkSpace 재구축 또는 마이그레이션 중에는 D 드라이브에서 C 드라이브로 사용자 프로필 위치가 변경되지 않습니다. Windows 10 또는 11 WorkSpace BYOL에서 전체 업그레이드를 수행한 다음 다시 빌드하거나 마이그레이션하는 경우 새 드라이브에는 D 드라이브에 사용자 WorkSpace 프로필이 있습니다.

  > **Warning**
  >
  > 인플레이스 업그레이드 후에 사용자 프로필을 C 드라이브에 그대로 두는 경우, 다시 빌드하거나 마이그레이션하기 전에 사용자 프로필 데이터를 수동으로 백업하고 프로세스를 다시 빌드하거나 마이그레이션한 후 사용자 프로필 데이터를 수동으로 복원하지 않으면 다시 빌드하거나 마이그레이션하는 중에 C 드라이브에 저장된 사용자 프로필 데이터가 손실됩니다.

- 기본 BYOL 번들에 Windows 10 및 11의 이전 릴리스를 기반으로 하는 이미지가 포함되어 있는 경우 다시 빌드하거나 마이그레이션한 후에 전체 업그레이드를 다시 수행해야 합니다. WorkSpace

레지스트리 키 설정 요약

인플레이스 업그레이드 프로세스를 활성화하고 업그레이드 후 사용자 프로필을 배치할 위치를 지정하려면 여러 레지스트리 키를 설정해야 합니다.

레지스트리 경로: HKL M:\Software\Amazon\WorkSpacesConfig\ .ps1 enable-inplace-upgrade

레지스트리 키	유형	값
활성화됨	DWORD	0 - (기본값) 인플레이스 업그레이드를 비활성화합니다. 1 - 인플레이스 업그레이드를 활성화합니다.

레지스트리 키	유형	값
PostUpgradeRestoreProfileOnD	DWORD	0 - (기본값) 인플레이스 업그레이드 후 사용자 프로필 경로 복원을 시도하지 않습니다. 1 — 전체 업그레이드 후 사용자 프로필 경로 (ProfileImagePath) 를 복원합니다.
UserShellFoldersRedirection	DWORD	0 - 사용자 쉘 폴더의 리디렉션을 활성화하지 않습니다. 1 - (기본값) 사용자 프로필이 `C:\Users\%USERNAME%` 에 다시 생성된 후 `D:\Users\%USERNAME%` 으로의 사용자 쉘 폴더 리디렉션을 활성화합니다.
NoReboot	DWORD	0 - (기본값) 사용자 프로필에 대한 레지스트리를 수정한 후 재부팅하는 시간을 제어할 수 있습니다. 1 - 사용자 프로필의 레지스트리를 WorkSpace 수정한 후 스크립트를 재부팅할 수 없습니다.

레지스트리 경로: HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

레지스트리 키	유형	값
활성화됨	DWORD	0 — (기본값) PV 드라이버 업데이트를 비활성화합니다. AWS

레지스트리 키	유형	값
		1 — AWS PV 드라이버 업데이트 활성화

현재 위치 업그레이드 수행

WorkSpacesBYOL에서 Windows 전체 업그레이드를 활성화하려면 다음 절차에 설명된 대로 특정 레지스트리 키를 설정해야 합니다. 인플레이스 업그레이드를 완료한 후 사용자 프로필이 위치할 드라이브(C 또는 D)를 가리키는 데에도 특정 레지스트리 키를 설정해야 합니다.

이러한 레지스트리를 수동으로 변경할 수 있습니다. 업데이트할 항목이 여러 개 WorkSpaces 있는 경우 그룹 정책 또는 SCCM을 사용하여 스크립트를 푸시할 수 있습니다. PowerShell 샘플 PowerShell 스크립트는 을 참조하십시오. 스크립트를 사용하여 WorkSpace 레지스트리를 업데이트하세요. PowerShell

Windows 10 및 11의 전체 업그레이드를 수행하려면

1. 업데이트하려는 Windows 10 및 11 WorkSpaces BYOL에서 현재 실행 중인 Windows 버전을 메모해 둔 다음 다시 부팅하십시오.
2. 다음 Windows 시스템 레지스트리 키를 업데이트하여 Enabled 값 데이터를 0에서 1로 변경합니다. 이러한 레지스트리 변경을 통해 을 (를) 전체 업그레이드할 수 있습니다. WorkSpace

   - HKEY_LOCAL_MACHINE\ 소프트웨어\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ 소프트웨어\ 아마존\\ update-pvdrivers.ps1 WorkSpacesConfig

   > **Note**
   >
   > 이러한 키가 없는 경우 를 재부팅하십시오. WorkSpace 시스템을 재부팅할 때 이러한 키가 추가되어야 합니다.

   (선택 사항) SCCM Task Sequences 같은 관리형 워크플로를 사용하여 업그레이드를 수행하는 경우, 다음 키 값을 1로 설정하여 컴퓨터 재부팅을 방지합니다.

HKEY_LOCAL_MACHINE\ 소프트웨어\ 아마존\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. 인플레이스 업그레이드 프로세스(자세한 내용은 고려 사항 섹션 참조) 후에 사용자 프로필이 위치할 드라이브를 결정하고 다음과 같이 레지스트리 키를 설정합니다.

   - 업그레이드 후 사용자 프로필을 C 드라이브에 위치시키려는 경우 설정:

     HKEY_LOCAL_MACHINE\ 소프트웨어\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     키 이름 PostUpgradeRestoreProfileOn: D

     키 값: 0

     키 이름: UserShellFoldersRedirection

     키 값: 1

   - 업그레이드 후 사용자 프로필을 D 드라이브에 위치시키려는 경우 설정:

     HKEY_LOCAL_MACHINE\ 소프트웨어\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     키 이름 PostUpgradeRestoreProfileOn: D

     키 값: 1

     키 이름: UserShellFoldersRedirection

     키 값: 0

4. 레지스트리에 변경 내용을 저장한 후 WorkSpace 다시 부팅하여 변경 내용이 적용되도록 합니다.

> **Note**
>
> - 다시 부팅한 후 에 WorkSpace 로그인하면 새 사용자 프로필이 생성됩니다. 시작 메뉴에서 자리 표시자 아이콘을 볼 수 있습니다. 이 동작은 인플레이스 업그레이드가 완료되면 자동으로 해결됩니다.
> - WorkSpace 차단이 해제될 때까지 10분 정도 기다려 주세요.

(선택 사항) 다음 키 값이 1로 설정되어 있는지 확인합니다. 그러면 업데이트 차단이 WorkSpace 해제됩니다.

HKEY_LOCAL_MACHINE\ 소프트웨어\ Amazon\\ .ps1\ 삭제됨 WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. 인플레이스 업그레이드를 수행합니다. SCCM, ISO, Windows 업데이트(WU) 등과 같은 원하는 방법을 사용할 수 있습니다. 원래 Windows 10 및 11 버전과 설치된 앱 수에 따라 이 프로세스는 40분에서 120분까지 걸릴 수 있습니다.

> **Note**
>
> 인플레이스 업그레이드 프로세스에는 최소 한 시간이 걸릴 수 있습니다. WorkSpace 인스턴스 상태는 업그레이드 UNHEALTHY 중과 같이 표시될 수 있습니다.

6. 업데이트 프로세스가 완료되면 Windows 버전이 업데이트되었는지 확인합니다.

> **Note**
>
> 전체 업그레이드가 실패하는 경우 Windows는 업그레이드를 시작하기 전에 사용하던 Windows 10 및 11 버전을 사용하도록 자동으로 롤백됩니다. 문제 해결에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

(선택 사항) 업데이트 스크립트가 성공적으로 실행되었는지 확인하려면 다음 키 값이 1로 설정되었는지 확인합니다.

HKEY_LOCAL_MACHINE\ 소프트웨어\ 아마존\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. 전체 업그레이드 프로세스가 중단 없이 실행될 수 있도록 기간을 AlwaysOn 설정하거나 AutoStop 기간을 변경하여 의 실행 모드를 수정한 경우 실행 모드를 원래 설정으로 다시 설정하십시오. WorkSpace 자세한 정보는 실행 모드 수정을 참조하세요.

PostUpgradeRestoreProfileOnD 레지스트리 키를 1로 설정하지 않은 경우 사용자 프로필은 Windows에서 다시 생성되어 전체 업그레이드 C:\Users\%USERNAME% 후에 삽입되므로 향후 Windows 10 및 11 전체 업그레이드 시 위 단계를 다시 거치지 않아도 됩니다. 기본적으로 enable-inplace-upgrade.ps1 스크립트는 다음 셸 폴더를 D 드라이브로 리디렉션합니다.

- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates

셸 폴더를 내 다른 위치로 리디렉션하는 경우 전체 WorkSpaces 업그레이드 WorkSpaces 후에 필요한 작업을 수행하십시오.

문제 해결

업데이트와 관련된 문제가 발생하는 경우, 다음 항목을 확인하면 문제를 해결하는 데 도움이 될 수 있습니다.

- Windows 로그(기본적으로 다음 위치에 있음)

  C:\Program Files\Amazon\WorkSpacesConfig\Logs\

  C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED
- Windows 이벤트 뷰어

  윈도우 로그 > 애플리케이션 > 출처: Amazon WorkSpaces

> **Tip**
>
> 전체 업그레이드 프로세스 중에 바탕 화면의 일부 아이콘 바로 가기가 더 이상 작동하지 않는 경우 업그레이드를 준비하기 위해 D 드라이브에 있는 모든 사용자 프로필을 C 드라이브로 WorkSpaces 이동했기 때문입니다. 업그레이드가 완료되면 바로 가기가 작동합니다.

스크립트를 사용하여 WorkSpace 레지스트리를 업데이트하세요. PowerShell

다음 샘플 PowerShell 스크립트를 사용하여 레지스트리를 업데이트하여 전체 업그레이드를 WorkSpaces 활성화할 수 있습니다. 을 따르되현재 위치 업그레이드 수행, 각 WorkSpace 스크립트에서 레지스트리를 업데이트하려면 이 스크립트를 사용하십시오.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
```

```
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

마이그레이션 a WorkSpace

> **Note**
>
> 를 통해 Microsoft Office 버전 라이선스를 구독 취소하거나 제거하려는 경우 AWS 응용 프로그램 관리를 사용하는 것이 좋습니다. WorkSpace

사용자 볼륨의 WorkSpace 데이터를 유지하면서 한 번들에서 다른 번들로 a를 마이그레이션할 수 있습니다. 다음은 예시 시나리오입니다.

- Windows 7 데스크톱 환경에서 Windows 10 데스크톱 WorkSpaces 환경으로 마이그레이션할 수 있습니다.
- PCoIP WorkSpaces 프로토콜에서 WorkSpaces 스트리밍 프로토콜 (WSP) 으로 마이그레이션할 수 있습니다.
- Windows Server 2016 기반 32비트 Microsoft Office 지원 번들에서 Windows Server 2019의 64비트 Microsoft Office 및 Windows Server 2022 기반 WorkSpaces 번들로 WorkSpaces 마이그레이션할 수 있습니다. WorkSpaces

- 공용 또는 사용자 지정 번들 간에 WorkSpaces 마이그레이션할 수 있습니다. 예를 들어 GPU 지원 (Graphics.g4dn) 에서 마이그레이션할 수 있습니다. GraphicsPro.g4dn, 그래픽 및 GraphicsPro) 번들을 GPU를 지원하지 않는 번들로, 또는 그 반대로도 가능합니다.
- 윈도우 10 WorkSpaces BYOL에서 윈도우 11 BYOL로 마이그레이션할 수 있지만 윈도우 11에서 윈도우 10으로의 마이그레이션은 지원되지 않습니다.
- Windows 11에서는 Value 번들이 지원되지 않습니다. Windows 7 또는 10 밸류 번들을 Windows WorkSpaces 11로 마이그레이션하려면 먼저 밸류를 더 큰 번들 WorkSpaces 오퍼링으로 전환해야 합니다.
- Windows WorkSpaces 7에서 Windows 11로 마이그레이션하기 전에 먼저 Windows 10으로 마이그레이션해야 합니다. Windows 11로 마이그레이션하기 전에 Windows 10에 한 번 WorkSpace 이상 로그인하세요. Windows 7에서 Windows 11로 WorkSpaces 직접 마이그레이션하는 것은 지원되지 않습니다.
- Microsoft Office를 사용하는 Windows를 Microsoft 365 응용 프로그램이 WorkSpaces 포함된 사용자 지정 WorkSpaces 번들로 AWS 마이그레이션할 수 있습니다. 마이그레이션 후에는 Microsoft Office WorkSpaces 구독이 취소됩니다.
- Microsoft Office를 사용하는 WorkSpaces Windows를 Office 2016/2019 구독 없이 WorkSpaces 번들로 AWS 마이그레이션할 수 있습니다. 마이그레이션 후에는 Microsoft Office WorkSpaces 구독이 취소됩니다.

Amazon WorkSpaces 번들에 대한 자세한 내용은 을 참조하십시오WorkSpace 번들 및 이미지.

마이그레이션 프로세스는 대상 번들 이미지의 새 루트 볼륨과 원본의 마지막 사용 가능한 스냅샷의 사용자 볼륨을 사용하여 를 다시 생성합니다. WorkSpace WorkSpace 호환성을 높이기 위해 마이그레이션 중에 새 사용자 프로필이 생성됩니다. 이전 사용자 프로필의 이름이 바뀌고 이전 사용자 프로필의 특정 파일이 새 사용자 프로필로 이동됩니다. 이동되는 항목에 대한 자세한 내용은 마이그레이션 중에 발생하는 일 단원을 참조하십시오.

마이그레이션 프로세스에는 각각 최대 WorkSpace 1시간이 소요됩니다. 마이그레이션 프로세스를 시작하면 새 프로세스가 WorkSpace 생성됩니다. 마이그레이션에 실패할 수 있는 오류가 발생하는 경우 WorkSpace 원본은 복구되어 원래 상태로 돌아가고 새 WorkSpace 버전은 종료됩니다.

목차

- 모범 사례
- 문제 해결
- 결제에 미치는 영향
- 마이그레이션: WorkSpace

마이그레이션 제한 사항

- 퍼블릭 또는 사용자 지정 Windows 7 데스크톱 환경 번들로는 마이그레이션할 수 없습니다. 또한 기존 보유 라이선스 사용(BYOL) Windows 7 번들로 마이그레이션할 수 없습니다.
- BYOL은 다른 BYOL WorkSpaces 번들로만 마이그레이션할 수 있습니다. WorkSpace PCoIP에서 WSP로 BYOL을 마이그레이션하려면 먼저 WSP 프로토콜을 사용하여 BYOL 번들을 만들어야 합니다. 그런 다음 PCoIP BYOL을 해당 WSP BYOL 번들로 마이그레이션할 수 있습니다. WorkSpaces
- 공개 또는 사용자 지정 번들에서 WorkSpace 만든 번들은 BYOL 번들로 마이그레이션할 수 없습니다.
- Graphics.g4dn, GraphicsPro .g4dn, 그래픽 및 GraphicsPro 번들은 현재 PCoIP 프로토콜에서만 사용할 수 있으므로 Graphics.g4dn, .g4dn, Graphics는 아직 WSP로 마이그레이션할 수 없습니다. GraphicsPro GraphicsPro WorkSpaces
- WorkSpaces Linux 마이그레이션은 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 둘 이상의 언어를 지원하는 리전에서는 언어가 서로 다르다면 동일한 Windows 10 번들로 마이그레이션할 수 있습니다. 동일한 번들을 WorkSpace 사용하여 새로 고치려면 대신 번들을 다시 빌드하세요. WorkSpace
- 지역 간에는 WorkSpaces 마이그레이션할 수 없습니다.
- 경우에 따라, 마이그레이션을 성공적으로 완료할 수 없을 때 오류 메시지가 나타나지 않을 수 있으며 마이그레이션 프로세스가 시작되지 않은 것처럼 보일 수 있습니다. 마이그레이션을 시도한 지 한 시간이 지난 후에도 WorkSpace 번들이 동일하게 유지되면 마이그레이션이 실패합니다. AWS Support Center에 문의하여 지원을 받으세요.

마이그레이션 시나리오

다음 표에서는 가능한 마이그레이션 시나리오를 보여 줍니다.

소스 OS	대상 OS	가능 여부
퍼블릭 또는 사용자 지정 번들 Windows 7	퍼블릭 또는 사용자 지정 번들 Windows 10	예
사용자 지정 번들 Windows 7	퍼블릭 번들 Windows 7	아니요
사용자 지정 번들 Windows 7	사용자 지정 번들 Windows 7	아니요
퍼블릭 번들 Windows 7	사용자 지정 번들 Windows 7	아니요
퍼블릭 또는 사용자 지정 번들 Windows 10	퍼블릭 또는 사용자 지정 번들 Windows 7	아니요
퍼블릭 또는 사용자 지정 번들 Windows 10	사용자 지정 번들 Windows 10	예
Windows 7 BYOL 번들	Windows 7 BYOL 번들	아니요
Windows 7 BYOL 번들	Windows 10 BYOL 번들	예
Windows 10 BYOL 번들	Windows 7 BYOL 번들	아니요
Windows 10 BYOL 번들	Windows 10 BYOL 번들	예
Windows Server 2016 기반 퍼블릭 Windows 10 번들	Windows Server 2019 기반 퍼블릭 Windows 10 번들 	예
Windows Server 2019 기반 퍼블릭 Windows 10 번들 	Windows Server 2016 기반 퍼블릭 Windows 10 번들	예
Windows 10 BYOL 번들	Windows 11 BYOL 번들	예

소스 OS	대상 OS	가능 여부
Windows 11 BYOL 번들	Windows 10 BYOL 번들	아니요
Windows Server 2016 기반 사용자 지정 Windows 10 번들	Windows Server 2019 기반 퍼블릭 Windows 10 번들	예
Windows Server 2016 기반 사용자 지정 Windows 10 번들	Windows Server 2022 기반 퍼블릭 Windows 10 번들	예
Windows Server 2019 기반 사용자 지정 Windows 10 번들	Windows Server 2022 기반 퍼블릭 Windows 10 번들	예

Note

Windows Server 2019 기반 퍼블릭 Windows 10 번들 PCoIP 브랜치에서는 웹 액세스를 사용할 수 없습니다.

Important

Windows Server 2016 기반 퍼블릭 Windows 10 Plus 번들에는 Microsoft Office 2016과 Trend Micro Worry-Free Business Security Service가 포함되어 있습니다. Windows Server 2019 기반 퍼블릭 Windows 10 Plus 번들에는 Microsoft Office 2019만 포함되어 있으며 Trend Micro Service는 포함되어 있지 않습니다.

마이그레이션 중에 발생하는 일

마이그레이션 과정에서 사용자 볼륨(D 드라이브)의 데이터는 유지되지만 루트 볼륨(C 드라이브)의 모든 데이터는 잃게 됩니다. 즉, 설치된 애플리케이션, 설정 및 레지스트리 변경 사항은 유지되지 않습니다. 이전 사용자 프로필 폴더의 이름이 `.NotMigrated` 접미사를 사용하여 바뀌고 새 사용자 프로필이 생성됩니다.

마이그레이션 과정에서 원래 사용자 볼륨의 마지막 스냅샷을 기반으로 D 드라이브가 재생성됩니다. 새 WorkSpace 폴더를 처음 부팅할 때 마이그레이션 프로세스는 원래 `D:\Users\%USERNAME%` 폴더

를 이름이 지정된 폴더로 이동합니다. D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 새 OS에서 새 D:\Users\%USERNAME%\ 폴더가 생성됩니다.

새 사용자 프로필이 생성되면 다음 사용자 셸 폴더의 파일이 이전 .NotMigrated 프로필에서 새 프로필로 이동됩니다.

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

> **Important**
>
> 마이그레이션 프로세스는 이전 사용자 프로필에서 새 프로필로 파일을 이동합니다. 마이그레이션 과정에서 이동되지 않은 파일은 모두 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 폴더에 남아 있습니다. 마이그레이션이 성공하면 이동된 파일을 C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs에서 확인할 수 있습니다. 자동으로 이동되지 않은 파일은 수동으로 이동할 수 있습니다.
> 기본적으로 퍼블릭 번들에는 로컬 검색 인덱싱이 비활성화되어 있습니다. 활성화하려는 경우 기본값은 D:\Users가 아닌 C:\Users 검색이므로 이 역시 조정해야 합니다. 로컬 검색 인덱싱을 D:\Users가 아닌 D:\Users*username*으로 특별히 설정한 경우 마이그레이션 후에는 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 폴더에 있는 사용자 파일에 대해 로컬 검색 인덱싱이 작동하지 않을 수 있습니다.

WorkSpace 원본에 할당된 모든 태그는 마이그레이션 중에 그대로 유지되며 의 실행 WorkSpace 모드는 유지됩니다. 하지만 새 버전에는 새 WorkSpace WorkSpace ID, 컴퓨터 이름 및 IP 주소가 부여됩니다.

모범 사례

마이그레이션하기 전에 WorkSpace 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 확인할 수 있습니다. 마지막 스냅샷 이후에 생성된 모든 데이터는 마이그레이션 중에 손실됩니다.
- 잠재적 데이터 손실을 방지하려면 마이그레이션 프로세스가 완료될 때까지 사용자가 WorkSpaces 로그아웃하고 다시 로그인하지 않도록 하십시오. 단, `ADMIN_MAINTENANCE` 모드 상태에서는 마이그레이션할 수 WorkSpaces 없습니다.
- WorkSpaces 마이그레이션하려는 상태가 `AVAILABLESTOPPED`, 또는 `ERROR` 인지 확인하십시오.
- 마이그레이션하려는 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.

문제 해결

- 사용자가 마이그레이션 후 누락된 파일을 보고하는 경우 마이그레이션 과정에서 해당 사용자 프로필 파일이 이동되지 않았는지 확인합니다. 이동된 파일은 `C:\Program Files\Amazon \WorkspacesConfig\Logs\MigrationLogs`에서 확인할 수 있습니다. 이동되지 않은 파일은 `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` 폴더에 있습니다. 자동으로 이동되지 않은 파일은 수동으로 이동할 수 있습니다.
- API를 사용하여 WorkSpaces 마이그레이션하고 있는데 마이그레이션에 실패하는 경우 API에서 반환한 대상 WorkSpace ID는 사용되지 않으며 원래 WorkSpace WorkSpace ID는 그대로 유지됩니다.
- 마이그레이션이 성공적으로 완료되지 않는 경우 Active Directory가 적절히 정리되었는지 확인합니다. 더 이상 필요하지 않은 WorkSpaces 것은 수동으로 제거해야 할 수도 있습니다.

결제에 미치는 영향

마이그레이션이 발생하는 달에는 새 버전과 원래 버전 모두에 대해 비례 할당으로 계산된 금액이 청구됩니다. 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.

> **Note**
>
> A를 다른 번들 유형 (예: 성능에서 전원으로 또는 Value to Standard) 으로 마이그레이션하는 경우 마이그레이션 프로세스 중에 루트 볼륨 (C 드라이브) 과 사용자 볼륨 (D 드라이브) 의 크기가 증가할 수 있습니다. WorkSpace 필요한 경우 루트 볼륨이 새 번들의 기본 루트 볼륨 크기와 일치하도록 증가합니다. 그러나 사용자 볼륨에 원래 번들의 기본값과 다른 크기(더 크거나 작음)를 이미 지정한 경우에는 마이그레이션 과정에서 동일한 사용자 볼륨 크기가 유지됩니다. 그렇지 않으면 새 번들의 소스 WorkSpace 사용자 볼륨 크기와 기본 사용자 볼륨 크기 중 더 큰 크기가 마이그레이션 프로세스에 사용됩니다.

마이그레이션: WorkSpace

Amazon WorkSpaces 콘솔, AWS CLI 또는 Amazon WorkSpaces API를 WorkSpaces 통해 마이그레이션할 수 있습니다.

마이그레이션하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. 원하는 항목을 WorkSpace 선택하고 작업, 마이그레이션을 선택합니다 WorkSpaces.
4. 번들 아래에서 WorkSpace 마이그레이션하려는 번들을 선택합니다.

   > **Note**
   >
   > WorkSpace PCoIP에서 WSP로 BYOL을 마이그레이션하려면 먼저 WSP 프로토콜을 사용하여 BYOL 번들을 만들어야 합니다. 그런 다음 PCoIP BYOL을 해당 WSP BYOL 번들로 마이그레이션할 수 있습니다. WorkSpaces

5. 마이그레이션을 WorkSpaces 선택합니다.

   Amazon WorkSpace WorkSpaces 콘솔에 상태가 인 새 항목이 `PENDING` 나타납니다. 마이그레이션이 완료되면 WorkSpace 원본은 종료되고 새 WorkSpace 항목의 상태는 로 `AVAILABLE` 설정됩니다.

6. (선택 사항) 더 이상 필요하지 않은 사용자 지정 번들 및 이미지를 삭제하려면 사용자 지정 WorkSpaces 번들 또는 이미지 삭제 단원을 참조하십시오.

를 WorkSpaces 통해 마이그레이션하려면 migrate-workspace 명령을 사용하십시오. AWS CLI Amazon API를 WorkSpaces 통해 마이그레이션하려면 Amazon WorkSpaces WorkSpaces API 레퍼런스를 참조하십시오 MigrateWorkSpace.

WorkSpace 삭제

사용을 마친 WorkSpaces를 삭제할 수 있습니다. 관련 리소스도 삭제할 수 있습니다.

> **Warning**
>
> WorkSpace 삭제는 영구 작업이며 실행 취소할 수 없습니다. WorkSpace 사용자의 데이터는 유지되지 않고 삭제됩니다. 사용자 데이터를 백업하는 데 도움이 필요한 경우 AWS Support에 문의하세요.

> **Note**
>
> Simple AD 및 AD Connector는 WorkSpaces에 무료로 제공됩니다. 연속 30일 동안 Simple AD 또는 AD Connector 디렉터리에 사용 중인 WorkSpaces가 없는 경우 이 디렉터리는 Amazon WorkSpaces에서의 사용이 자동으로 등록 취소되며, AWS Directory Service 요금 조건에 따라 이 디렉터리에 대한 요금이 부과됩니다.
> 빈 디렉터리를 삭제하려면 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요. Simple AD 또는 AD Connector 디렉터리를 삭제한 경우 WorkSpaces를 다시 사용하고 싶을 때 언제든지 새 디렉터리를 생성할 수 있습니다.

WorkSpaces를 삭제하려면

일시 중단됨을 제외한 모든 상태의 WorkSpace를 삭제할 수 있습니다.

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [WorkSpaces]를 선택합니다.
3. WorkSpace를 선택하고 삭제를 선택합니다.
4. 확인 메시지가 나타나면 WorkSpace 삭제를 선택합니다. WorkSpace를 삭제하는 데 약 5분이 소요됩니다. 삭제 중에는 WorkSpace의 상태가 종료 중으로 설정됩니다. 삭제가 완료되면 WorkSpace가 콘솔에서 사라집니다.

5. (선택 사항) 사용을 마친 사용자 지정 번들 및 이미지를 삭제하려면 사용자 지정 WorkSpaces 번들 또는 이미지 삭제 단원을 참조하십시오.
6. (선택 사항) 디렉터리에서 모든 WorkSpaces를 삭제한 후 해당 디렉터리를 삭제할 수 있습니다. 자세한 내용은 WorkSpaces용 디렉터리 삭제 섹션을 참조하세요.
7. (선택 사항) 디렉터리의 가상 사설 클라우드(VPC)에서 모든 리소스를 삭제한 후 해당 VPC를 삭제하고 NAT 게이트웨이에 사용된 탄력적 IP 주소를 해제할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 삭제 및 탄력적 IP 주소 작업을 참조하세요.

AWS CLI를 사용하여 WorkSpaces를 삭제하는 방법

terminate-workspaces 명령을 사용하세요.

WorkSpace 번들 및 이미지

WorkSpace 번들은 운영 체제와 스토리지, 컴퓨팅, 소프트웨어 리소스의 조합입니다. 를 WorkSpace 실행할 때 요구 사항에 맞는 번들을 선택합니다. 에서 사용할 수 있는 기본 번들을 퍼블릭 WorkSpaces 번들이라고 합니다. 에서 사용할 수 있는 다양한 퍼블릭 번들에 대한 자세한 내용은 Amazon WorkSpaces Bundles를 WorkSpaces 참조하십시오.

Windows 또는 WorkSpace Linux를 시작하고 사용자 지정한 경우 해당 이미지로 사용자 지정 이미지를 생성할 수 있습니다. WorkSpace

사용자 지정 이미지에는 의 OS, 소프트웨어 및 설정만 포함됩니다 WorkSpace. 사용자 지정 번들은 해당 사용자 지정 이미지와 a를 실행할 WorkSpace 수 있는 하드웨어의 조합입니다.

사용자 지정 이미지를 만든 후 사용자 지정 이미지와 선택한 기본 컴퓨팅 및 스토리지 구성을 결합하는 사용자 지정 WorkSpace 번들을 빌드할 수 있습니다. 그런 다음 새로 시작할 때 이 사용자 지정 번들을 WorkSpaces 지정하여 새 번들이 동일한 일관된 구성 (하드웨어 및 소프트웨어) 을 WorkSpaces 갖도록 할 수 있습니다.

소프트웨어 업데이트를 수행하거나 에 추가 소프트웨어를 설치해야 하는 경우 사용자 지정 번들을 업데이트하고 이를 사용하여 소프트웨어를 다시 빌드할 수 있습니다 WorkSpaces. WorkSpaces

WorkSpaces 다양한 운영 체제 (OS), 스트리밍 프로토콜 및 번들을 지원합니다. 다음 표에는 각 OS에서 지원하는 라이선스, 스트리밍 프로토콜 및 번들에 대한 정보가 나와 있습니다.

운영 체제	라이선스	스트리밍 프로토콜	지원되는 번들	라이프사이클 정책/은퇴일
Windows Server 2016	포함	WSP, PCoIP	가치, 표준, 성능, 전력, 그래픽 (더 이상 사용되지 않음) PowerPro, 그래픽.g4dn, .g4dn GraphicsPro GraphicsPro	2027년 1월 12일
Windows Server 2019	포함	WSP, PCoIP	가치, 표준, 성능, 전력, 그래픽 (더 이상 사용되지 않음) PowerPro, 그래픽.g4dn, .g4dn GraphicsPro GraphicsPro	2029년 1월 9일

운영 체제	라이선스	스트리밍 프로토콜	지원되는 번들	라이프사이클 정책/은퇴일
Windows Server 2022	포함	WSP, PCoIP	표준, 성능, 전원, 그래픽 (더 이상 사용되지 않음) PowerPro, 그래픽.g4dn, .g4dn GraphicsPro GraphicsPro	2013년 10월 14일
Windows 10	기존 보유 라이선스 사용 (BYOL)	WSP, PCoIP	가치, 표준, 성능, 전력, 그래픽 (더 이상 사용되지 않음) PowerPro, 그래픽.g4dn, .g4dn GraphicsPro GraphicsPro	지원 중
Windows 11	기존 보유 라이선스 사용 (BYOL)	WSP	표준, 성능, 전력, PowerPro	지원 중
Amazon Linux 2	포함	WSP, PCoIP	가치, 표준, 성능, 전력, PowerPro	2025년 6월 30일
Ubuntu 22.04 LTS	포함	WSP	가치, 표준, 성능, 전력, 그래픽.g4dn PowerPro, .g4dn GraphicsPro	2032년 6월

Note

- 공급업체에서 더 이상 지원하지 않는 운영 체제 버전은 작동이 보장되지 않으며 지원 부서에서 AWS 지원하지 않습니다.
- Windows 운영 체제에서 WorkSpaces 실행하는 경우 그래픽 번들은 PCoIP 스트리밍 프로토콜만 지원합니다.

내용

- 사용자 지정 WorkSpaces 이미지 및 번들 생성
- 사용자 지정 WorkSpaces 번들 업데이트
- 사용자 지정 WorkSpaces 이미지 복사
- 사용자 지정 WorkSpaces 이미지 공유 또는 공유 해제
- 사용자 지정 WorkSpaces 번들 또는 이미지 삭제
- 기존 보유 Windows 데스크톱 라이선스 사용

번들 옵션

번들을 선택하기 전에 선택하려는 번들이 WorkSpaces의 프로토콜, 운영 체제, 네트워크 및 컴퓨팅 유형과 호환되는지 확인하세요. 프로토콜에 대한 자세한 내용은 Protocols for Amazon WorkSpaces를 참조하세요. 네트워크에 대한 자세한 내용은 Amazon WorkSpaces 클라이언트 네트워크 요구 사항을 참조하세요.

> **Note**
>
> - PCoIP WorkSpaces의 경우 네트워크 지연 시간은 최대 250밀리초를 초과하지 않는 것이 좋습니다. 최상의 PCoIP WorkSpaces 사용자 경험을 얻으려면 네트워크 지연 시간을 100밀리초 미만으로 유지하는 것이 좋습니다. 왕복 시간(RTT)이 375ms를 초과하면 WorkSpaces 클라이언트 연결이 종료됩니다. 최상의 WorkSpaces 스트리밍 프로토콜(WSP) 사용자 경험을 위해 RTT를 250밀리초 미만으로 유지하는 것이 좋습니다. RTT가 250~400밀리초인 경우 사용자가 WorkSpaces에 액세스할 수는 있지만 성능이 크게 저하됩니다.
> - 사용자의 일상 작업을 복제하는 애플리케이션을 실행하고 사용하여 테스트 환경에서 선택하려는 번들의 성능을 테스트하는 것이 좋습니다.

> **Important**
>
> - 2023년 11월 30일 이후에는 Graphics 번들이 더 이상 지원되지 않습니다. Graphics 번들을 사용하는 WorkSpaces를 Graphics.g4dn 번들로 전환하는 것이 좋습니다.
> - Graphics 및 GraphicsPro 번들은 현재 아시아 태평양(뭄바이) 리전에서 사용할 수 없습니다.

다음은 WorkSpaces에서 제공하는 번들입니다. WorkSpaces의 번들에 대한 자세한 내용은 Amazon WorkSpaces 번들을 참조하세요.

Value 번들

이 번들은 다음과 같은 경우에 적합합니다.

- 기본 텍스트 편집 및 데이터 입력
- 사용량이 적은 웹 브라우징
- 인스턴트 메시징

이 번들은 워드 프로세싱, 오디오 및 화상 회의, 화면 공유, 소프트웨어 개발 도구, 비즈니스 인텔리전스 애플리케이션, 그래픽 애플리케이션에는 권장되지 않습니다.

Standard 번들

이 번들은 다음과 같은 경우에 적합합니다.

- 기본 텍스트 편집 및 데이터 입력
- 웹 브라우징
- 인스턴트 메시징
- 이메일

이 번들은 오디오 및 화상 회의, 화면 공유, 워드 프로세싱, 소프트웨어 개발 도구, 비즈니스 인텔리전스 애플리케이션, 그래픽 애플리케이션에는 권장되지 않습니다.

Performance 번들

이 번들은 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 인스턴트 메시징
- 이메일
- 스프레드시트
- 오디오 프로세싱
- 코스웨어

이 번들은 화상 회의, 화면 공유, 소프트웨어 개발 도구, 비즈니스 인텔리전스 애플리케이션, 그래픽 애플리케이션에는 권장되지 않습니다.

Power 번들

이 번들은 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 이메일
- 인스턴트 메시징
- 스프레드시트
- 오디오 프로세싱
- 소프트웨어 개발(통합 개발 환경(IDE))
- 초급에서 중급 수준의 데이터 프로세싱
- 오디오 및 화상 회의

이 번들은 화면 공유, 소프트웨어 개발 도구, 비즈니스 인텔리전스 애플리케이션, 그래픽 애플리케이션에는 권장되지 않습니다.

PowerPro 번들

이 번들은 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 이메일
- 인스턴트 메시징
- 스프레드시트
- 오디오 프로세싱
- 소프트웨어 개발(통합 개발 환경(IDE))
- 데이터 웨어하우징
- 비즈니스 인텔리전스 애플리케이션
- 오디오 및 화상 회의

이 번들은 기계 학습 모델 훈련 및 그래픽 애플리케이션에는 권장되지 않습니다.

GraphicsPro 번들

이 번들은 WorkSpaces를 위한 기본 수준의 그래픽 성능과 높은 수준의 CPU 성능 및 메모리를 제공합니다. 이 번들은 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 이메일
- 인스턴트 메시징
- 스프레드시트
- 오디오 회의
- 소프트웨어 개발(통합 개발 환경(IDE))
- 데이터 웨어하우징
- 비즈니스 인텔리전스 애플리케이션
- 그래픽 디자인
- 이미지 프로세싱

이 번들은 오디오 및 화상 회의, 3D 렌더링 및 실사 수준의 디자인에는 권장되지 않습니다.

Graphics.g4dn 번들

이 번들은 WorkSpaces를 위한 높은 수준의 그래픽 성능과 보통 수준의 CPU 성능 및 메모리를 제공하며 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 이메일
- 스프레드시트
- 인스턴트 메시징
- 오디오 회의
- 소프트웨어 개발(통합 개발 환경(IDE))
- 초급에서 중급 수준의 데이터 프로세싱

- 데이터 웨어하우징
- 비즈니스 인텔리전스 애플리케이션
- 그래픽 디자인
- 컴퓨터 지원 설계/컴퓨터 지원 제조(CAD/CAM)

이 번들은 오디오 및 화상 회의, 3D 렌더링 및 실사 수준의 디자인 및 기계 학습 모델 훈련에는 권장되지 않습니다.

GraphicsPro.g4dn

GraphicsPro.g4dn 번들

이 번들은 WorkSpaces를 위한 높은 수준의 그래픽 성능과 CPU 성능, 메모리를 제공하며 다음과 같은 경우에 적합합니다.

- 웹 브라우징
- 워드 프로세싱
- 이메일
- 스프레드시트
- 인스턴트 메시징
- 오디오 회의
- 소프트웨어 개발(통합 개발 환경(IDE))
- 초급에서 중급 수준의 데이터 프로세싱
- 데이터 웨어하우징
- 비즈니스 인텔리전스 애플리케이션
- 그래픽 디자인
- 컴퓨터 지원 설계/컴퓨터 지원 제조(CAD/CAM)
- 비디오 트랜스코딩
- 3D 렌더링
- 실사 수준의 디자인
- 게임 스트리밍
- 기계 학습(ML) 모델 훈련 및 ML 추론

이 번들은 오디오 및 비디오 컨퍼런싱에는 권장되지 않습니다.

사용자 지정 WorkSpaces 이미지 및 번들 생성

Windows 또는 WorkSpace Linux를 시작하고 사용자 지정한 경우 해당 이미지로 사용자 지정 이미지와 사용자 지정 번들을 만들 수 있습니다. WorkSpace

사용자 지정 이미지에는 에 대한 OS, 소프트웨어 및 설정만 포함됩니다. WorkSpace 사용자 지정 번들은 해당 사용자 지정 이미지와 a를 실행할 WorkSpace 수 있는 하드웨어의 조합입니다.

> **Note**
>
> 번들을 삭제한 후 이름이 같은 새 번들을 생성하려면 최소 2시간 이상 기다려야 합니다.

사용자 지정 이미지를 생성한 후, 사용자 지정 이미지와 선택한 스토리지 구성 및 기본 컴퓨팅을 결합하는 사용자 지정 번들을 빌드할 수 있습니다. 그런 다음 새로 시작할 때 이 사용자 지정 번들을 WorkSpaces 지정하여 새 번들이 동일한 일관된 구성 (하드웨어 및 소프트웨어) 을 WorkSpaces 갖도록 할 수 있습니다.

동일한 사용자 지정 이미지를 이용해 각 번들에 대해 서로 다른 컴퓨팅 및 스토리지 옵션을 선택하여 다양한 사용자 지정 번들을 생성할 수 있습니다.

> **Important**
>
> - Windows 10에서 이미지를 만들려는 경우 한 버전의 Windows WorkSpace 10에서 최신 버전의 Windows 10으로 업그레이드 (Windows 기능/버전 업그레이드) 된 Windows 10 시스템에서는 이미지 생성이 지원되지 않는다는 점에 유의하십시오. 하지만 Windows 누적 업데이트 또는 보안 업데이트는 이미지 생성 프로세스에서 지원됩니다. WorkSpaces
> - 2020년 1월 14일 이후에는 퍼블릭 Windows 7 번들에서 이미지를 생성할 수 없습니다. Windows WorkSpaces 7을 Windows 10으로 마이그레이션하는 것을 고려해 볼 수 있습니다. 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.
> - 2023년 11월 30일 이후에는 Graphics 번들이 더 이상 지원되지 않습니다. Graphics.G4dn 번들로 마이그레이션하는 WorkSpaces 것이 좋습니다. 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.
> - 그래픽 및 GraphicsPro 번들은 현재 아시아 태평양 (뭄바이) 지역에서 사용할 수 없습니다.
> - 사용자 지정 번들 스토리지 볼륨은 이미지 스토리지 볼륨보다 작을 수 없습니다.

사용자 지정 번들은 생성된 퍼블릭 번들과 같은 비용이 듭니다. 요금에 대한 자세한 내용은 Amazon WorkSpaces 요금을 참조하십시오.

내용

Windows 사용자 지정 이미지 생성 시 적용되는 요구 사항

> **Note**
>
> Windows는 현재 1GB를 1,073,741,824바이트로 정의합니다. A 이미지를 생성하려면 고객은 C 드라이브에 12,884,901,888바이트 (또는 12GiB) 이상의 여유 공간이 있어야 하고 사용자 프로필이 10,737,418,240바이트 (또는 10GiB) 미만인지 확인해야 합니다. WorkSpace

- 상태는 [사용 가능] 이고 수정 상태는 [없음] 이어야 합니다. WorkSpace
- WorkSpaces 이미지에 있는 모든 응용 프로그램 및 사용자 프로필은 Microsoft Sysprep과 호환되어야 합니다.
- 이미지에 포함할 모든 애플리케이션을 C 드라이브에 설치해야 합니다.
- Windows WorkSpaces 7의 경우 전체 크기 (파일 및 데이터) 가 10GB 미만이어야 합니다.
- Windows 7의 WorkSpaces 경우 C 드라이브에 12GB 이상의 사용 가능한 공간이 있어야 합니다.
- 에서 실행되는 모든 응용 프로그램 서비스는 도메인 사용자 자격 증명 대신 로컬 시스템 계정을 WorkSpace 사용해야 합니다. 예를 들어 도메인 사용자의 자격 증명을 사용하여 Microsoft SQL Server Express 설치를 실행할 수 없습니다.
- WorkSpace 암호화해서는 안 됩니다. 암호화된 이미지를 이용한 이미지 WorkSpace 생성은 현재 지원되지 않습니다.

- 다음 구성 요소가 이미지에 필요합니다. 이러한 구성 요소가 없으면 이미지에서 시작한 구성 요소가 제대로 작동하지 않습니다. WorkSpaces 자세한 정보는 the section called “필수 구성”을 참조하세요.
  - 윈도우 PowerShell 버전 3.0 이상
  - 원격 데스크톱 서비스
  - AWS PV 드라이버
  - Windows 원격 관리(WinRM)
  - Teradici PCoIP 에이전트 및 드라이버
  - STXHD 에이전트 및 드라이버
  - AWS 및 인증서 WorkSpaces
  - Skylight 에이전트

Linux 사용자 지정 이미지 생성 시 적용되는 요구 사항

- 상태는 사용 WorkSpace 가능이어야 하고 수정 상태는 없음이어야 합니다.
- 이미지에 포함할 모든 애플리케이션은 사용자 볼륨(/home 디렉터리) 외부에 설치되어야 합니다.
- 루트 볼륨(/)은 97%보다 작아야 합니다.
- WorkSpace 암호화해서는 안 됩니다. 암호화된 이미지를 이용한 이미지 WorkSpace 생성은 현재 지원되지 않습니다.
- 다음 구성 요소가 이미지에 필요합니다. 다음과 같은 구성 요소가 없으면 이미지에서 시작한 구성 요소가 제대로 작동하지 않습니다. WorkSpaces
  - Cloud-init
  - Teradici PCoIP 또는 WSP 에이전트 및 드라이버
  - Skylight 에이전트

모범 사례

WorkSpacea에서 이미지를 생성하기 전에 다음을 수행하십시오.

- 프로덕션 환경에 연결되지 않은 별도의 VPC를 사용합니다.
- 프라이빗 WorkSpace 서브넷에 배포하고 아웃바운드 트래픽에 NAT 인스턴스를 사용하십시오.
- 작은 Simple AD 디렉터리를 사용합니다.

- 소스에 가장 작은 볼륨 크기를 사용한 다음 WorkSpace 사용자 지정 번들을 생성할 때 필요에 따라 볼륨 크기를 조정합니다.
- 모든 운영 체제 업데이트 (Windows 기능/버전 업데이트 제외) 와 모든 애플리케이션 업데이트를 에 설치합니다. WorkSpace 자세한 내용은 이 주제의 시작 부분에 있는 중요 참고 사항을 참조하십시오.
- 번들에 포함해서는 안 WorkSpace 되는 캐시된 데이터 (예: 브라우저 기록, 캐시된 파일, 브라우저 쿠키) 에서 삭제하십시오.
- 번들에 포함해서는 안 WorkSpace 되는 구성 설정 (예: 이메일 프로필) 에서 구성 설정을 삭제합니다.
- DHCP를 사용하여 동적 IP 주소 설정으로 전환합니다.
- 지역에 허용된 WorkSpace 이미지 할당량을 초과하지 않았는지 확인하세요. 기본적으로 지역당 40 개의 WorkSpace 이미지가 허용됩니다. 이 할당량에 도달한 경우 이미지를 생성하려고 시도하면 실패합니다. 할당량 증가를 요청하려면 WorkSpaces 제한 양식을 사용하세요.
- 암호화된 이미지로 이미지를 만들려고 하지 않았는지 확인하세요 WorkSpace. 암호화된 이미지를 이용한 이미지 WorkSpace 생성은 현재 지원되지 않습니다.
- 에서 바이러스 백신 소프트웨어를 실행 중인 경우 이미지를 만들려고 시도하는 동안 해당 소프트웨어를 사용하지 않도록 설정하십시오. WorkSpace
- 방화벽이 활성화되어 있는 경우 필요한 포트를 차단하고 있지 않은지 확인하세요. WorkSpace 자세한 정보는 IP 주소 및 포트 요구 사항 WorkSpaces을 참조하세요.
- WorkSpacesWindows의 경우 이미지를 만들기 전에 그룹 정책 개체 (GPO) 를 구성하지 마십시오.
- WorkSpacesWindows의 경우 이미지를 만들기 전에 기본 사용자 프로필 (`C:\Users\Default`) 을 사용자 지정하지 마십시오. 이미지 생성 후에 GPO를 통해 사용자 프로필을 사용자 지정하고 적용하는 것이 좋습니다. GPO는 쉽게 수정하거나 롤백할 수 있으므로 기본 사용자 프로필에 수행된 사용자 지정보다 오류가 발생할 가능성이 낮습니다.
- WorkSpacesLinux의 경우 “ WorkSpaces Linux용 Amazon 이미지 준비 모범 사례” 백서도 참조하십시오.
- WorkSpaces 스트리밍 프로토콜 (WSP) 이 WorkSpaces 활성화된 Linux에서 스마트 카드를 사용하려면 이미지를 WorkSpace 생성하기 전에 인증에 스마트 카드 사용 Linux에 적용해야 하는 사용자 지정을 참조하십시오.
- ENA, NVMe, PV 드라이버와 같은 네트워킹 종속성 드라이버를 반드시 업데이트하십시오. WorkSpaces 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 Windows 인스턴스용 ENA (엘라스틱 네트워크 어댑터) 드라이버 설치 또는 업그레이드 및 Windows 인스턴스의 PV 드라이버 업그레이드를 참조하십시오.AWS NVMe 드라이버

- EC2Config, EC2Launch 및 EC2Launch V2 에이전트를 정기적으로 최신 버전으로 업데이트하십시오. 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 EC2Config 및 EC2Launch 업데이트를 참조하십시오.

(선택 사항) 1단계: 이미지에 사용자 지정 컴퓨터 이름 형식 지정

사용자 지정 또는 BYOL (Bring Your Own License) 이미지에서 시작하는 경우 기본 컴퓨터 이름 형식을 사용하는 대신 컴퓨터 이름 형식에 사용자 지정 접두사를 지정할 수 있습니다. WorkSpaces 사용자 지정 접두사를 지정하려면 이미지 유형에 맞는 적절한 절차를 따르세요.

사용자 지정 이미지에 사용자 지정 컴퓨터 이름 형식을 지정하는 방법

> **Note**
>
> 기본적으로 Windows 10의 컴퓨터 이름 형식은 Windows WorkSpaces `DESKTOP-XXXXX` 10이고 Windows 11의 컴퓨터 이름 형식은 입니다. WorkSpaces `WORKSPA-XXXXX`

1. 사용자 지정 이미지를 만드는 데 사용하는 이미지를 메모장이나 다른 텍스트 `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` 편집기에서 엽니다. WorkSpace `Unattend.xml` 파일 작업에 대한 자세한 내용은 Microsoft 설명서의 Answer files (unattend.xml)를 참조하세요.

   > **Note**
   >
   > 의 Windows 파일 탐색기에서 C: 드라이브에 액세스하려면 주소 표시줄에 를 입력합니다**`C:\`**. WorkSpace

2. `<settings pass="specialize">` 섹션에서 `<ComputerName>`을 별표(*)로 설정하세요. `<ComputerName>`을 다른 값으로 설정하면 사용자 지정 컴퓨터 이름 설정이 무시됩니다. `<ComputerName>`설정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오. ComputerName
3. `<settings pass="specialize">` 섹션에서 `<RegisteredOrganization>` 및 `<RegisteredOwner>`를 원하는 값으로 설정합니다.

   Sysprep 중에 `<RegisteredOwner>` 및 `<RegisteredOrganization>`에 지정한 값과 값이 결합되며, 결합된 문자열의 처음 7자가 컴퓨터 이름을 만드는 데 사용됩니다. 예를 들어 `<RegisteredOrganization>` for와 **`EC2`** for를 지정하는 **`Amazon.com`** 경우 사용

자 지정 번들로 WorkSpaces 만든 컴퓨터 이름은 EC2AMAZ- *xxxxxxxxx#* 시작합니다.
<RegisteredOwner>

> **Note**
>
> Sysprep은 <settings pass="oobeSystem"> 섹션의
> <RegisteredOrganization> 및 <RegisteredOwner> 값을 무시합니다.

4. Unattend.xml 파일에 대한 변경 사항을 저장합니다.

BYOL 이미지에 사용자 지정 컴퓨터 이름 형식을 지정하는 방법

1. Windows 10을 사용하는 경우 메모장이나 다른 텍스트 편집기에서 C:\Program Files \Amazon\Ec2ConfigService\Sysprep2008.xml을 엽니다. Windows 11을 사용하는 경우 C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml을 엽니다.
2. <settings pass="specialize"> 섹션에서 <ComputerName>*</ComputerName>의 코멘트를 삭제하고 <ComputerName>을 별표(*)로 설정하세요. <ComputerName>을 다른 값으로 설정하면 사용자 지정 컴퓨터 이름 설정이 무시됩니다. <ComputerName>설정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오. ComputerName
3. <settings pass="specialize"> 섹션에서 <RegisteredOrganization> 및 <RegisteredOwner>를 원하는 값으로 설정합니다.

   Sysprep 중에 <RegisteredOwner> 및 <RegisteredOrganization>에 지정한 값과 값이 결합되며, 결합된 문자열의 처음 7자가 컴퓨터 이름을 만드는 데 사용됩니다. 예를 들어 <RegisteredOrganization> for와 **EC2** for를 지정하는 **Amazon.com** 경우 사용자 지정 번들로 WorkSpaces 만든 컴퓨터 이름은 EC2AMAZ- *xxxxxxxxx#* 시작합니다.
   <RegisteredOwner>

   > **Note**
   >
   > Sysprep은 <settings pass="oobeSystem"> 섹션의
   > <RegisteredOrganization> 및 <RegisteredOwner> 값을 무시합니다.

4. Windows 10을 사용하는 경우 변경 사항을 Sysprep2008.xml 파일에 저장하세요. Windows 11을 사용하는 경우 변경 사항을 OOBE_unattend.xml에 저장하세요.

2단계: 이미지 검사기 실행

> **Note**
>
> 이미지 검사기는 Windows에서만 사용할 수 있습니다. WorkSpaces WorkSpaceLinux에서 이미지를 생성하는 경우 으로 건너뛰십시오. 3단계: 사용자 지정 이미지 및 사용자 지정 번들 생성

Windows가 이미지 생성 요구 사항을 WorkSpace 충족하는지 확인하려면 이미지 검사기를 실행하는 것이 좋습니다. 이미지 검사기는 이미지를 만드는 데 사용할 항목에 대해 일련의 테스트를 수행하고 발견된 문제를 해결하는 방법에 대한 지침을 제공합니다. WorkSpace

> **Important**
>
> - 이미지 생성에 사용하려면 먼저 이미지 검사기에서 실행하는 모든 테스트를 WorkSpace 통과해야 합니다.
> - 이미지 검사기를 실행하기 전에 최신 Windows 보안 및 누적 업데이트가 컴퓨터에 설치되어 있는지 확인하십시오. WorkSpace

이미지 검사기를 가져오려면 다음 중 하나를 수행합니다.

- 를 재부팅하십시오. WorkSpace 이미지 검사기는 재부팅하는 동안 자동으로 다운로드되고 `C:\Program Files\Amazon\ImageChecker.exe`에 설치됩니다.
- https://tools.amazonworkspaces.com/ ImageChecker .zip 아마존 WorkSpaces 이미지 검사기를 다운로드하고 파일을 추출하십시오. `ImageChecker.exe` 이 파일을 `C:\Program Files\Amazon\`에 복사합니다.

이미지 검사기를 실행하려면

1. `C:\Program Files\Amazon\ImageChecker.exe` 파일을 엽니다.
2. Amazon WorkSpaces 이미지 검사기 대화 상자에서 실행을 선택합니다.
3. 각 테스트가 완료된 후 테스트의 상태를 볼 수 있습니다.

테스트의 상태가 FAILED(실패)인 경우 Info(정보)를 선택하여 실패의 원인이 된 문제를 해결하는 방법에 대한 정보를 표시합니다. 이러한 문제를 해결하는 방법에 대한 자세한 내용은 이미지 검사기에서 감지한 문제 해결을 위한 팁 단원을 참조하십시오.

테스트가 WARNING(경고) 상태를 표시하는 경우 Fix All Warnings(모든 경고 수정) 버튼을 선택합니다.

이 도구는 이미지 검사기가 위치해 있는 동일한 디렉터리에 출력 로그 파일을 생성합니다. 이 파일의 기본 위치는 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`입니다.

> **Tip**
>
> 이 로그 파일을 삭제하지 마십시오. 문제가 발생하는 경우 이러한 로그 파일이 문제 해결에 도움이 될 수 있습니다.

4. 해당하는 경우 테스트 실패 및 경고를 유발하는 모든 문제를 해결하고 모든 테스트를 WorkSpace 통과할 때까지 이미지 검사기 실행 프로세스를 반복합니다. 이미지를 생성하기 전에 모든 실패 및 경고를 해결해야 합니다.
5. 모든 테스트를 WorkSpace 통과하면 검증 성공 메시지가 표시됩니다. 이제 사용자 지정 번들을 생성할 준비가 되었습니다.

이미지 검사기에서 감지한 문제 해결을 위한 팁

이미지 검사기에서 감지한 문제를 해결하기 위한 다음 팁을 고려하는 것 외에도 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`에서 이미지 검사기 로그 파일을 검토해야 합니다.

PowerShell 버전 3.0 이상을 설치해야 합니다.

최신 버전의 마이크로소프트 윈도우를 설치합니다 PowerShell.

> **Important**
>
> 에 대한 PowerShell 실행 정책을 RemoteSigned스크립트를 허용하도록 WorkSpace 설정해야 합니다. 실행 정책을 확인하려면 Get- ExecutionPolicy PowerShell 명령을 실행합니다. 실행 정책이 Unrestricted RemoteSignedor로 설정되지 않은 경우 Set- ExecutionPolicy — ExecutionPolicy RemoteSigned 명령을 실행하여 실행 정책 값을 변경하십시오. 이

RemoteSigned설정을 통해 Amazon에서 스크립트를 실행할 수 있으며 WorkSpaces, 이 스크립트는 이미지를 생성하는 데 필요합니다.

C 및 D 드라이브만 있을 수 있습니다.

이미징에 사용되는 A에는 C WorkSpace 및 D 드라이브만 있을 수 있습니다. 가상 드라이브를 포함한 기타 모든 드라이브를 제거합니다.

Windows Update로 인해 보류 중인 재부팅을 감지할 수 없음

- 보안 또는 누적 업데이트 설치를 완료하기 위해 Windows를 재부팅할 때까지 이미지 생성 프로세스를 실행할 수 없습니다. Windows를 재부팅하여 이러한 업데이트를 적용하고 보류 중인 기타 Windows 보안 또는 누적 업데이트를 설치할 필요가 없는지 확인합니다.
- 한 버전의 Windows 10에서 더 최신 버전의 Windows 10으로 업그레이드(Windows 기능/버전 업그레이드)를 수행한 Windows 10 시스템에서는 이미지 생성이 지원되지 않습니다. 하지만 Windows 누적 업데이트 또는 보안 업데이트는 WorkSpaces 이미지 생성 프로세스에서 지원됩니다.

Sysprep 파일이 있어야 하며 비워 둘 수 없습니다.

Sysprep 파일에 문제가 있는 경우 AWS Support Center에 문의하여 EC2Config 또는 EC2Launch를 복구합니다.

사용자 프로필 크기는 10GB 미만이어야 합니다.

Windows 7의 WorkSpaces 경우 사용자 프로필 (`D:\Users\`*`username`*) 은 총 10GB 미만이어야 합니다. 필요에 따라 파일을 제거하여 사용자 프로필의 크기를 줄입니다.

C 드라이브에는 충분한 사용 가능한 공간이 있어야 합니다.

Windows 7의 WorkSpaces 경우 드라이브에 최소 12GB의 여유 공간이 있어야 C 합니다. 필요에 따라 파일을 제거하여 C 드라이브의 공간을 확보합니다. Windows WorkSpaces 10의 경우 FAILED 메시지가 표시되고 디스크 공간이 2GB를 초과하면 무시하세요.

도메인 계정에서 서비스를 실행할 수 없습니다.

이미지 만들기 프로세스를 실행하려면 의 어떤 서비스도 도메인 계정으로 실행할 WorkSpace 수 없습니다. 모든 서비스는 로컬 계정에서 실행해야 합니다.

로컬 계정에서 서비스를 실행하려면

1. `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`를 열고 도메인 계정에서 실행 중인 서비스 목록을 찾습니다.
2. Windows 검색 상자에 **`services.msc`**를 입력하여 Windows Services Manager를 엽니다.
3. [Log On As]에서, 도메인 계정에서 실행 중인 서비스를 찾습니다. (Local System, Local Service 또는 Network Service로 실행 중인 서비스는 이미지 생성을 방해하지 않습니다.)
4. 도메인 계정에서 실행 중인 서비스를 선택한 다음 [Action], [Properties]를 선택합니다.
5. [Log On] 탭을 엽니다. [Log On As]에서 [Local System account]를 선택합니다.
6. 확인을 선택합니다.

DHCP를 사용하도록 WorkSpace 구성해야 합니다.

의 모든 네트워크 어댑터가 고정 IP 주소 대신 WorkSpace DHCP를 사용하도록 구성해야 합니다.

DHCP를 사용하도록 모든 네트워크 어댑터를 설정하려면

1. Windows 검색 상자에 **`control panel`**을 입력하여 제어판을 엽니다.
2. [Network and Internet]을 선택합니다.
3. [Network and Sharing Center]를 선택합니다.
4. [Change adapter settings]를 선택하고 어댑터를 선택합니다.
5. [Change settings of this connection]을 선택합니다.
6. [Networking] 탭에서 [Internet Protocol Version 4 (TCP/IPv4)]를 선택한 다음 [Properties]를 선택합니다.
7. [Internet Protocol Version 4 (TCP/IPv4) Properties] 대화 상자에서 [Obtain an IP address automatically]를 선택합니다.
8. 확인을 선택합니다.
9. 의 모든 네트워크 어댑터에 대해 이 프로세스를 반복합니다. WorkSpace

원격 데스크톱 서비스가 활성화되어 있어야 합니다.

이미지 생성 프로세스를 수행하려면 원격 데스크톱 서비스를 활성화해야 합니다.

원격 데스크톱 서비스를 활성화하려면

1. Windows 검색 상자에 **`services.msc`**를 입력하여 Windows Services Manager를 엽니다.

2. [Name] 열에서 [Remote Desktop Services]를 찾습니다.
3. [Remote Desktop Services]를 선택한 다음 [Action], [Properties]를 선택합니다.
4. [General] 탭에서, [Startup type]에 대해 [Manual] 또는 [Automatic]을 선택합니다.
5. 확인을 선택합니다.

사용자 프로필이 있어야 합니다.

이미지를 만드는 WorkSpace 데 사용하는 이미지에는 사용자 프로필 (`D:\Users\username`) 이 있어야 합니다. 이 테스트가 실패하면 AWS Support Center에 문의하여 도움을 받으세요.

환경 변수 경로가 올바르게 구성되어 있어야 합니다.

로컬 시스템의 환경 변수 경로에 System32와 PowerShell Windows의 경우 항목이 누락되었습니다. 이러한 항목은 이미지 생성을 실행하는 데 필요합니다.

환경 변수 경로를 구성하려면

1. Windows 검색 상자에 **`environment variables`**를 입력한 다음 [Edit the system environment variables]를 선택합니다.
2. [System Properties] 대화 상자에서 [Advanced] 탭을 선택한 다음 [Environment Variables]를 선택합니다.
3. [Environment Variables] 대화 상자의 [System variables]에서 [Path] 항목을 선택한 다음 [Edit]를 선택합니다.
4. [New]를 선택하고 다음 경로를 추가합니다.

   ```
   C:\Windows\System32
   ```
5. [New]를 다시 선택하고 다음 경로를 추가합니다.

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. 확인을 선택합니다.
7. 를 다시 시작합니다. WorkSpace

> **Tip**
>
> 환경 변수 경로에 항목이 표시되는 순서가 중요합니다. 올바른 순서를 결정하려면 의 환경 변수 경로를 새로 만든 환경 변수 WorkSpace 경로나 새 Windows 인스턴스의 WorkSpace 경로와 비교하는 것이 좋습니다.

Windows 모듈 설치 관리자가 활성화되어 있어야 합니다.

이미지 생성 프로세스를 수행하려면 Windows 모듈 설치 관리자 서비스를 활성화해야 합니다.

Windows 모듈 설치 관리자 서비스를 활성화하려면

1. Windows 검색 상자에 **services.msc**를 입력하여 Windows Services Manager를 엽니다.
2. [Name] 열에서 [Windows Modules Installer]를 찾습니다.
3. [Windows Modules Installer]를 선택한 다음 [Action], [Properties]를 선택합니다.
4. [General] 탭에서, [Startup type]에 대해 [Manual] 또는 [Automatic]을 선택합니다.
5. 확인을 선택합니다.

Amazon SSM Agent가 비활성화되어 있어야 합니다.

이미지 생성 프로세스를 수행하려면 Amazon SSM Agent 서비스를 비활성화해야 합니다.

Amazon SSM Agent 서비스를 비활성화하려면

1. Windows 검색 상자에 **services.msc**를 입력하여 Windows Services Manager를 엽니다.
2. [Name] 열에서 [Amazon SSM Agent]를 찾습니다.
3. [Amazon SSM Agent]를 선택한 다음 [Action], [Properties]를 선택합니다.
4. [General] 탭에서 [Startup type]에 대해 [Disabled]를 선택합니다.
5. 확인을 선택합니다.

SSL3 및 TLS 버전 1.2가 활성화되어 있어야 합니다.

Windows용 SSL/TLS를 구성하려면 Microsoft Windows 설명서에서 TLS 1.2를 활성화하는 방법을 참조하십시오.

에는 사용자 프로필이 하나만 존재할 수 있습니다. WorkSpace

이미지를 만드는 데 사용하는 WorkSpaces 사용자 프로필 (`D:\Users\username`) 은 하나만 WorkSpace 있을 수 있습니다. 의 대상 사용자에게 속하지 않는 사용자 프로필을 모두 삭제하십시오 WorkSpace.

이미지 생성이 제대로 되려면 다음과 같은 사용자 프로필을 세 개만 WorkSpace 사용할 수 있습니다.

- WorkSpace(`D:\Users\username`) 의 대상 사용자의 사용자 프로필

- 기본 사용자 프로필(기본 프로필이라고도 함)
- 관리자 사용자 프로필

추가 사용자 프로필이 있는 경우 Windows Control Panel에서 고급 시스템 속성을 통해 삭제할 수 있습니다.

사용자 프로필을 삭제하려면

1. 고급 시스템 속성에 액세스하려면 다음 중 하나를 수행합니다.
   - Windows 키+Pause Break를 누른 다음 Control Panel 왼쪽 창의 Advanced system settings > System and Security > System 대화 상자를 선택합니다.
   - Windows 검색 상자에 **`control panel`**을 입력합니다. Control Panel에서 System and Security를 선택한 다음 System을 선택하고 Control Panel 왼쪽 창의 Advanced system settings > System and Security > System 대화 상자를 선택합니다.
2. System Properties 대화 상자의 Advanced 탭에 있는 User Profiles에서 Settings를 선택합니다.
3. 관리자 프로필, 기본 프로필 및 의도한 WorkSpaces 사용자의 프로필 이외의 프로필이 나열되어 있는 경우 해당 추가 프로필을 선택하고 삭제를 선택합니다.
4. 프로필을 삭제할 것인지 묻는 메시지가 나타나면 예를 선택합니다.
5. 필요한 경우 3단계와 4단계를 반복하여 에 속하지 않는 다른 프로필을 모두 제거합니다 WorkSpace.
6. 확인을 두 번 선택하고 제어판을 닫습니다.
7. 를 다시 시작합니다 WorkSpace.

AppX 패키지는 스테이징된 상태일 수 없습니다.

하나 이상의 AppX 패키지가 스테이징된 상태에 있습니다. 이로 인해 이미지를 생성하는 중에 Sysprep 오류가 발생할 수 있습니다.

스테이징된 AppX 패키지를 모두 제거하려면

1. Windows 검색 상자에 **`powershell`**을 입력합니다. [Run as Administrator]를 선택합니다.
2. “이 앱이 디바이스를 변경할 수 있도록 허용하시겠습니까?“라고 묻는 메시지가 나타나면 예를 선택합니다.
3. Windows PowerShell 창에서 다음 명령을 입력하여 스테이징된 AppX 패키지를 모두 나열하고 각 패키지 다음에 Enter 키를 누릅니다.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                ($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                $_.PackageUserInformation -like "*Staged*")
                                }
```

4. 다음 명령을 입력하여 스테이징된 AppX 패키지를 모두 제거하고 Enter 키를 누릅니다.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. 이미지 검사기를 다시 실행합니다. 이 테스트가 여전히 실패하면 다음 명령을 입력하여 AppX 패키지를 모두 제거하고, 각 명령 다음에는 Enter 키를 누릅니다.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows가 이전 버전에서 업그레이드되지 않았어야 합니다.

한 버전의 Windows 10에서 더 최신 버전의 Windows 10으로 업그레이드(Windows 기능/버전 업그레이드)를 수행한 Windows 시스템에서는 이미지 생성이 지원되지 않습니다.

이미지를 만들려면 Windows 기능/버전 업그레이드를 거치지 WorkSpace 않은 버전을 사용하십시오.

Windows 초기화 횟수는 0이 아니어야 합니다.

초기화 기능을 사용하면 Windows 평가판의 정품 인증 기간을 연장할 수 있습니다. 이미지 생성 프로세스에서는 초기화 횟수가 0이외의 값이어야 합니다.

Windows 초기화 횟수를 확인하려면

1. Windows 시작 메뉴에서 Windows 시스템을 선택한 다음 명령 프롬프트를 선택합니다.
2. 명령 프롬프트 창에 다음 명령을 입력한 다음 Enter 키를 누릅니다.

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

초기화 횟수를 0 이외의 값으로 재설정하려면 Microsoft Windows 설명서의 Windows 설치 Sysprep(일반화)을 참조하십시오.

기타 문제 해결 팁

이미지 검사기에서 실행한 모든 테스트를 WorkSpace 통과했지만 여전히 에서 이미지를 생성할 수 없는 경우 다음 문제를 확인하십시오. WorkSpace

- 도메인 게스트 그룹 내의 사용자에게 이 WorkSpace 할당되지 않았는지 확인하세요. 도메인 계정이 있는지 확인하려면 다음 PowerShell 명령을 실행합니다.

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- Windows WorkSpaces 7만 해당: 이미지를 만드는 동안 사용자 프로필을 복사하는 동안 문제가 발생하는 경우 다음 문제가 있는지 확인하세요.
  - 프로필 경로가 길면 이미지 생성 오류가 발생할 수 있습니다. 사용자 프로필 내 모든 폴더의 경로가 261자 미만인지 확인합니다.
  - 프로필 폴더에 전체 권한을 시스템 및 모든 애플리케이션 패키지에 부여해야 합니다.
  - 사용자 프로필의 파일이 프로세스에 의해 잠겨 있거나 이미지 생성 시 사용 중인 경우 프로필 복사가 실패할 수 있습니다.
- 일부 그룹 정책 객체(GPO)는 Windows 인스턴스 구성 중에 EC2Config 서비스 또는 EC2Launch 스크립트에서 요청할 때 RDP 인증서 지문에 대한 액세스를 제한합니다. 이미지를 만들기 전에 상속이 WorkSpace 차단되고 GPO가 적용되지 않은 새 OU (조직 구성 단위) 로 이미지를 이동하십시오.
- Windows 원격 관리(WinRM) 서비스가 자동으로 시작되도록 구성되어 있는지 확인합니다. 다음을 따릅니다.
  1. Windows 검색 상자에 **`services.msc`**를 입력하여 Windows Services Manager를 엽니다.
  2. [Name] 열에서 [Windows Remote Management (WS-Management)]를 찾습니다.
  3. [Windows Remote Management (WS-Management)]를 선택한 다음 [Action], [Properties]를 선택합니다.

4. [General] 탭에서 [Startup type]에 대해 [Automatic]을 선택합니다.
5. 확인을 선택합니다.

3단계: 사용자 지정 이미지 및 사용자 지정 번들 생성

이미지를 검증한 후 커스텀 WorkSpace 이미지와 커스텀 번들 생성을 진행할 수 있습니다.

사용자 지정 이미지 및 사용자 지정 번들을 생성하려면

1. 에 여전히 연결되어 있는 경우 WorkSpaces 클라이언트 애플리케이션에서 Amazon을 WorkSpaces 선택하고 Disconnect를 선택하여 연결을 끊으십시오. WorkSpace
2. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
3. 탐색 창에서 WorkSpaces를 선택합니다.
4. 를 WorkSpace 선택하여 세부 정보 페이지를 열고 이미지 생성을 선택합니다. 상태가 WorkSpace 중지됨인 경우 먼저 시작 (작업, 시작 선택 WorkSpaces) 해야 작업, 이미지 생성을 선택할 수 있습니다.

   > **Note**
   >
   > 프로그래밍 방식으로 이미지를 만들려면 CreateWorkspaceImage API 작업을 사용하십시오. 자세한 내용은 Amazon WorkSpaces API 레퍼런스를 참조하십시오 CreateWorkspaceImage.

5. 계속하기 WorkSpace 전에 재부팅 (재시작) 하라는 메시지가 표시됩니다. 재부팅하면 Amazon WorkSpaces 소프트웨어가 최신 버전으로 WorkSpace 업데이트됩니다.

   메시지를 닫고 위의 단계를 WorkSpace 따라 재부팅하십시오. 재부팅 a WorkSpace 완료되면 이 절차의 Step 4를 반복하되 이번에는 재부팅 메시지가 나타나면 다음을 선택합니다. 이미지를 만들려면 의 상태가 [사용 가능] 이고 수정 상태는 [없음] 이어야 합니다. WorkSpace
6. 이미지를 식별하는 데 도움이 되는 이미지 이름과 설명을 입력하고 Create Image(이미지 생성)를 선택합니다. 이미지를 만드는 동안에는 의 상태가 일시 WorkSpace WorkSpace 중단되고 를 사용할 수 없습니다.

> **Note**
>
> 이미지 설명을 입력할 때 특수 문자 “-”를 사용하지 마십시오. 그렇지 않으면 오류가 발생합니다.

7. 탐색 창에서 [Images]를 선택합니다. 상태가 사용 가능으로 WorkSpace 변경되면 이미지가 완성됩니다 (최대 45분이 소요될 수 있음).
8. 이미지를 선택하고 작업, 번들 생성을 선택합니다.

> **Note**
>
> 프로그래밍 방식으로 번들을 생성하려면 CreateWorkspaceBundle API 작업을 사용하세요. 자세한 내용은 Amazon WorkSpaces API 레퍼런스를 참조하십시오 CreateWorkspaceBundle.

9. 번들 이름과 설명을 입력하고 다음 작업을 수행합니다.

   - 번들 하드웨어 유형의 경우 이 사용자 지정 WorkSpaces 번들에서 시작할 때 사용할 하드웨어를 선택합니다.
   - 스토리지 설정에서 루트 볼륨과 사용자 볼륨 크기의 기본 조합 중 하나를 선택하거나 사용자 지정을 선택한 다음 루트 볼륨 크기 및 사용자 볼륨 크기에 값(최대 2,000GB)을 입력합니다.

     루트 볼륨(Microsoft Windows의 경우 C 드라이브, Linux의 경우 /) 및 사용자 볼륨(Windows의 경우 D 드라이브, Linux의 경우 /home)의 사용 가능 크기 조합(기본값)은 다음과 같습니다.

     - 루트: 80GB, 사용자: 10GB, 50GB 또는 100GB
     - 루트: 175GB, 사용자: 100GB
     - 그래픽.G4dn, GraphicsPro .g4dn, 그래픽 및 GraphicsPro WorkSpaces 전용: 루트: 100GB, 사용자: 100GB

     또는 루트 볼륨 및 사용자 볼륨의 크기를 각각 최대 2000GB까지 확장할 수 있습니다.

> **Note**
>
> 데이터를 보존하기 위해 a를 실행한 후에는 루트 볼륨이나 사용자 볼륨의 크기를 줄일 수 없습니다. WorkSpace 대신 를 실행할 때 이러한 볼륨의 최소 크기를 지정해야 WorkSpace 합니다. Value, Standard, Performance, Power 또는 PowerPro WorkSpace 루트 볼륨은 최소 80GB, 사용자 볼륨은 10GB 이상으로 실행할 수 있습니다. 그래

픽.G4DN, GraphicsPro .g4dn, Graphics를 실행하거나 GraphicsPro WorkSpace 루트 볼륨의 경우 최소 100GB, 사용자 볼륨의 경우 100GB 이상으로 실행할 수 있습니다.

10. 번들 생성을 선택합니다.
11. 번들이 생성되었는지 확인하려면 번들을 생성하고 번들이 목록에 있는지 확인합니다.

Windows 사용자 지정 이미지에는 무엇이 포함되어 있습니까? WorkSpaces

Windows 7, Windows 10 또는 Windows WorkSpace 11에서 이미지를 만드는 경우 C 드라이브의 전체 콘텐츠가 포함됩니다.

Windows 10 또는 11의 WorkSpaces 경우 의 사용자 `D:\Users\username` 프로필은 사용자 지정 이미지에 포함되지 않습니다.

Windows WorkSpaces 7의 경우 다음을 제외한 사용자 프로필의 전체 `D:\Users\username` 내용이 포함됩니다.

- 연락처
- 다운로드
- 음악
- 사진
- 저장된 게임
- 비디오
- 팟캐스트
- 가상 머신
- .virtualbox
- 추적
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\

- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Linux WorkSpace 사용자 지정 이미지에 포함된 내용

Amazon WorkSpace Linux에서 이미지를 생성하면 사용자 볼륨 (/home) 의 전체 콘텐츠가 제거됩니다. 제거되는 다음 폴더 및 키를 제외한 루트 볼륨(/)의 내용이 포함됩니다.

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules

- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/ domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/ .yaml zz-workspaces-domain
- yy-workspaces-base/etc/netplan/ .yaml
- /var/lib/ /사용자 AccountsService

다음 키는 사용자 지정 이미지 생성 중에 폐기됩니다.

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

사용자 지정 WorkSpaces 번들 업데이트

번들을 기반으로 하는 WorkSpaces를 수정하고, WorkSpaces에서 이미지를 생성하고, 새 이미지를 사용하여 번들을 업데이트하면 기존 사용자 지정 WorkSpaces 번들을 업데이트할 수 있습니다. 그러면 업데이트된 번들을 사용하여 새 WorkSpaces를 시작할 수 있습니다.

> **Important**
>
> 기존 WorkSpaces는 기반이 되는 번들을 업데이트할 때 자동으로 업데이트되지 않습니다. 업데이트한 번들을 기반으로 하는 기존 WorkSpaces를 업데이트하려면 WorkSpaces를 다시 빌드하거나 삭제 후 다시 생성해야 합니다.

콘솔을 사용하여 번들을 업데이트하는 방법

1. 번들을 기반으로 하는 WorkSpace에 연결하여 필요한 사항을 변경합니다. 예를 들어 최신 운영 체제 및 애플리케이션 패치를 적용하고 추가 애플리케이션을 설치할 수 있습니다.

   또는 번들을 생성할 때 사용한 이미지와 동일한 기본 소프트웨어 패키지(Plus 또는 Standard)로 새 WorkSpaces를 생성한 후 필요한 사항을 변경할 수도 있습니다.
2. 여전히 WorkSpaces에 연결되어 있는 경우 WorkSpaces 클라이언트 애플리케이션에서 Amazon WorkSpaces, 연결 해제를 선택하여 연결을 끊습니다.
3. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
4. 탐색 창에서 [WorkSpaces]를 선택합니다.
5. WorkSpaces를 선택하고 [Actions], [Create Image]를 선택합니다. WorkSpaces의 상태가 STOPPED인 경우 작업, WorkSpaces 시작을 선택하여 먼저 시작한 후 작업, 이미지 생성을 선택합니다.
6. 이미지 이름과 설명을 입력하고 Create Image(이미지 생성)를 선택합니다. 이미지가 생성되는 동안에는 WorkSpaces를 사용할 수 없습니다. 이미지 생성 프로세스에 대한 자세한 내용은 사용자 지정 WorkSpaces 이미지 및 번들 생성 섹션을 참조하세요.
7. 탐색 창에서 [Bundles]를 선택합니다.
8. 번들을 선택하여 세부 정보 페이지를 연 다음 소스 이미지에서 편집을 선택합니다.
9. 소스 이미지 업데이트 페이지에서 생성한 이미지를 선택하고 번들 업데이트를 선택합니다.
10. 필요에 따라 WorkSpaces를 다시 빌드하거나 삭제 후 다시 생성하여 번들을 기반으로 하는 기존 WorkSpaces를 업데이트합니다. 자세한 내용은 재구축 a WorkSpace 섹션을 참조하세요.

프로그래밍 방식으로 번들을 업데이트하는 방법

프로그래밍 방식으로 번들을 업데이트하려면 UpdateWorkspaceBundle API 작업을 사용하세요. 자세한 내용은 Amazon WorkSpaces API Reference의 UpdateWorkspaceBundle을 참조하세요.

사용자 지정 WorkSpaces 이미지 복사

AWS 리전 내에서 또는 리전 간에 사용자 지정 WorkSpaces 이미지를 복사할 수 있습니다. 이미지를 복사하면 고유한 식별자로 구분되는 동일한 이미지가 생성됩니다.

대상 리전이 Bring Your Own License(BYOL)에 대해 활성화되어 있으면 BYOL 이미지를 다른 리전으로 복사할 수 있습니다. 관련된 모든 계정 및 리전에 BYOL이 활성화되어 있는지 확인하세요.

> **Note**
>
> 중국(닝샤) 리전에서는 동일한 리전 내에서만 이미지를 복사할 수 있습니다.
> AWS GovCloud (US) Region에서 다른 AWS 리전과 이미지를 복사하려면 AWS Support에 문의하세요.
> 옵트인 리전에서 다른 리전으로 이미지를 복사하려면 AWS Support에 문의하세요. 옵트인 리전에 대한 자세한 내용은 사용 가능한 리전를 참조하세요.

다른 AWS 계정에서 나와 공유된 이미지를 복사할 수도 있습니다. 공유 이미지에 대한 자세한 내용은 사용자 지정 WorkSpaces 이미지 공유 또는 공유 해제 섹션을 참조하세요.

리전 내에서 또는 리전 간에 이미지 복사 시 추가 요금이 부과되지 않습니다. 대상 리전의 이미지 개수 할당량이 적용됩니다. Amazon WorkSpaces 할당량에 대한 자세한 내용은 아마존 WorkSpaces 쿼터 섹션을 참조하세요.

이미지 복사 IAM 권한

IAM 사용자를 사용하여 이미지를 복사하려면 사용자에게 `workspaces:DescribeWorkspaceImages` 및 `workspaces:CopyWorkspaceImage`에 대한 권한이 있어야 합니다.

다음 예시 정책을 통해 사용자는 지정된 이미지를 지정된 리전의 지정된 계정에 복사할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

이미지를 소유하지 않은 계정의 공유 이미지를 복사하기 위해 IAM 정책을 생성하는 경우 ARN에서 계정 ID를 지정할 수 없습니다. 대신 다음 예시 정책에 표시된 대로 계정 ID에 * 기호를 사용해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

해당 계정이 복사할 이미지를 소유한 경우에만 ARN에서 계정 ID를 지정할 수 있습니다.

IAM 작업에 관한 자세한 내용은 WorkSpaces의 Identity and Access Management 단원을 참조하세요.

이미지 대량 복사

콘솔을 사용하여 이미지를 하나씩 복사할 수 있습니다. 이미지를 대량 복사하려면 CopyWorkspaceImage API 작업 또는 AWS Command Line Interface(AWS CLI)에서 copy-workspace-image 명령을 사용합니다. 자세한 내용은 Amazon WorkSpaces API Reference의 CopyWorkspaceImage 또는 AWS CLI 명령 참조의 copy-workspace-image를 참조하세요.

Important

공유 이미지를 복사하기 전에 해당 이미지가 올바른 AWS 계정에서 공유되었는지 확인하세요. 이미지가 공유되었는지 확인하고 이미지를 소유한 AWS 계정 ID를 보려면 DescribeWorkSpaceImages 및 DescribeWorkspaceImagePermissions API 작업 또는 AWS

CLI에서 describe-workspace-images 및 describe-workspace-image-permissions 명령을 사용하세요.

콘솔을 사용하여 이미지를 복사하는 방법

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Images]를 선택합니다.
3. 이미지를 선택하고 작업, 이미지 삭제를 선택합니다.
4. 대상 선택에서 이미지를 복사할 대상 AWS 리전을 선택합니다.
5. 복사본 사본의 이름에 복사한 이미지의 새 이름을 입력하고 설명에는 복사한 이미지에 대한 설명을 입력합니다.
6. (선택 사항) 태그에서 복사한 이미지의 태그를 입력합니다. 자세한 내용은 WorkSpaces 리소스 태그 지정 섹션을 참조하세요.
7. 이미지 복사를 선택합니다.

사용자 지정 WorkSpaces 이미지 공유 또는 공유 해제

동일한 AWS 리전 내의 AWS 계정 간에 사용자 지정 WorkSpaces 이미지를 공유할 수 있습니다. 이미지를 공유한 후 수신자 계정은 필요에 따라 이미지를 다른 AWS 리전에 복사할 수 있습니다. 객체 복사에 대한 자세한 내용은 사용자 지정 WorkSpaces 이미지 복사 섹션을 참조하세요.

> **Note**
>
> 중국(닝샤) 리전에서는 동일한 리전 내에서만 이미지를 복사할 수 있습니다.
> AWS GovCloud (US) Region에서 다른 AWS 리전과 이미지를 복사하려면 AWS Support에 문의하세요.

이미지 공유에 대한 추가 비용은 없습니다. 그러나 AWS 리전의 이미지 개수 할당량이 적용됩니다. 공유된 이미지는 수신자가 이미지를 복사하기 전까지는 수신자 계정의 할당량에 포함되지 않습니다. Amazon WorkSpaces 할당량에 대한 자세한 내용은 아마존 WorkSpaces 쿼터 섹션을 참조하세요.

공유된 이미지를 삭제하려면 먼저 공유를 해제해야 합니다.

기존 보유 라이선스(Bring Your Own License) 이미지 공유

기존 보유 라이선스 사용(BYOL) 이미지는 BYOL이 활성화된 AWS 계정과만 공유할 수 있습니다. BYOL 이미지를 공유할 AWS 계정도 조직의 일부여야 합니다(동일한 지급인 계정).

> **Note**
>
> 현재 AWS GovCloud(미국 서부) 리전과 AWS GovCloud(미국 동부) 리전에서는 AWS 계정 간에 BYOL 이미지를 공유하는 것이 지원되지 않습니다. AWS GovCloud(미국 서부) 리전과 AWS GovCloud(미국 동부) 리전에서 계정 간에 BYOL 이미지를 공유하려면 AWS Support에 문의하세요.

나와 공유된 이미지

나와 공유된 이미지를 복사할 수 있습니다. 그런 다음 공유된 이미지의 복사본을 사용하여 새 WorkSpaces를 시작할 번들을 만들 수 있습니다.

> **Important**
>
> 공유 이미지를 복사하기 전에 해당 이미지가 올바른 AWS 계정에서 공유되었는지 확인하세요. 이미지 공유 여부를 프로그래밍 방식으로 확인하려면 AWS 명령줄 인터페이스(CLI)에서 DescribeWorkSpaceImages 및 DescribeWorkspaceImagePermissions API 작업 또는 escribe-workspace-images 및 describe-workspace-image-permissions 명령을 사용하세요.

공유된 이미지에 표시되는 생성 날짜는 이미지를 공유한 날짜가 아니라 이미지를 처음 만든 날짜입니다.

나와 공유된 이미지를 다른 계정과 더 이상 공유할 수 없습니다.

이미지를 공유하는 방법

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Images]를 선택합니다.
3. 이미지를 선택하여 세부 정보 페이지를 엽니다.
4. 이미지 세부 정보 페이지의 공유 계정 섹션에서 계정 추가를 선택합니다.
5. 계정 추가 페이지의 공유할 계정 추가에서 이미지를 공유하려는 계정의 계정 ID를 입력합니다.

> **Important**
>
> 이미지를 공유하기 전에 올바른 AWS 계정 ID와 공유하고 있는지 확인하세요.

6. 이미지 공유를 선택합니다.

> **Note**
>
> 공유 이미지를 사용하려면 수신자 계정이 먼저 이미지를 복사해야 합니다. 그러면 수신자 계정이 공유된 이미지의 복사본을 사용하여 새 WorkSpaces를 시작할 번들을 만들 수 있습니다.

이미지 공유를 중지하는 방법

1. https://console.aws.amazon.com/workspaces/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Images]를 선택합니다.
3. 이미지를 선택하여 세부 정보 페이지를 엽니다.
4. 이미지 세부 정보 페이지의 공유 계정 섹션에서 공유를 중단하려는 AWS 계정을 선택한 다음 공유 해제를 선택합니다.
5. 이미지 공유 해제를 확인하라는 메시지가 표시되면 공유 해제를 선택합니다.

> **Note**
>
> 이미지 공유를 해제한 후 삭제하려면 먼저 이미지를 공유한 모든 계정에서 공유를 해제해야 합니다.

이미지 공유를 해제한 후에는 수신자 계정에서 더 이상 이미지를 복사할 수 없습니다. 그러나 이미 수신자 계정에 있는 공유 이미지의 복사본은 모두 해당 계정에 남아 있으며 이러한 복사본에서 새 WorkSpaces를 시작할 수 있습니다.

프로그래밍 방식으로 이미지를 공유하거나 공유 해제하는 방법

프로그래밍 방식으로 이미지를 공유하거나 공유 해제하려면 UpdateWorkspaceImagePermission API 작업 또는 update-workspace-image-permission AWS Command Line Interface(AWS CLI) 명령을 사

용합니다. 이미지가 공유되었는지 확인하려면 DescribeWorkspaceImagePermissions API 작업 또는 describe-workspace-image-permissions CLI 명령을 사용합니다.

사용자 지정 WorkSpaces 번들 또는 이미지 삭제

필요에 따라 사용하지 않는 사용자 지정 번들 또는 사용자 지정 이미지를 삭제할 수 있습니다.

번들 삭제

번들을 삭제하려면 먼저 번들을 기반으로 WorkSpaces 하는 모든 번들을 삭제해야 합니다.

콘솔을 사용하여 번들을 삭제하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Bundles]를 선택합니다.
3. 삭제할 번들을 선택하고 삭제를 선택합니다.
4. 확인 메시지가 나타나면 삭제를 선택합니다.

프로그래밍 방식으로 번들을 삭제하는 방법

프로그래밍 방식으로 번들을 삭제하려면 DeleteWorkspaceBundle API 작업을 사용하세요. 자세한 내용은 Amazon WorkSpaces API 레퍼런스를 참조하십시오 DeleteWorkspaceBundle.

> **Note**
>
> 번들을 삭제한 후 이름이 같은 새 번들을 생성하려면 최소 2시간이 지나야 합니다.

이미지 삭제하기

사용자 지정 번들을 삭제한 후 해당 번들을 생성 또는 업데이트하는 데 사용한 이미지를 삭제할 수 있습니다.

이미지를 삭제하려면 먼저 해당 이미지와 관련된 번들을 삭제하거나 다른 소스 이미지를 사용하도록 번들을 업데이트해야 합니다. 또한 이미지를 다른 계정과 공유하는 경우 이미지 공유를 해제해야 합니다. 또한 이미지가 보류 중 또는 검증 상태여서는 안 됩니다.

콘솔을 사용하여 이미지를 삭제하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Images]를 선택합니다.
3. 이미지를 선택하고 삭제를 선택합니다.
4. 확인 메시지가 나타나면 삭제를 선택합니다.

이미지를 프로그래밍 방식으로 삭제하는 방법

프로그래밍 방식으로 이미지를 삭제하려면 DeleteWorkspaceImage API 작업을 사용하세요. 자세한 내용은 Amazon WorkSpaces API 레퍼런스를 참조하십시오 DeleteWorkspaceImage.

기존 보유 Windows 데스크톱 라이선스 사용

Microsoft와의 라이선스 계약에서 허용하는 경우 Windows 10 또는 11 데스크톱을 가져와 배포할 수 있습니다 WorkSpaces. 이렇게 하려면 기존 보유 라이선스 사용(BYOL)을 활성화하고 다음 요구 사항을 충족하는 Windows 10 또는 11 라이선스를 제공해야 합니다. 에서 AWS Microsoft 소프트웨어를 사용하는 방법에 대한 자세한 내용은 Amazon Web Services 및 Microsoft를 참조하십시오.

Microsoft 라이선스 조건을 계속 준수하려면 클라우드의 전용 WorkSpaces 하드웨어에서 BYOL을 AWS 실행하세요. AWS 기존 보유 라이선스를 사용하면 사용자에게 일관된 환경을 제공할 수 있습니다. 자세한 내용은 요금을 참조하십시오. WorkSpaces

> **Important**
>
> Windows 10 또는 11의 한 버전에서 최신 버전의 Windows 10 또는 11로 업그레이드된 Windows 10 또는 11 시스템에서는 이미지 생성이 지원되지 않습니다 (Windows 기능/버전 업그레이드). 하지만 Windows 누적 업데이트 또는 보안 업데이트는 이미지 생성 프로세스에서 지원됩니다. WorkSpaces

내용

- 2단계: Amazon 콘솔을 사용하여 BYOL 계정의 BYOL을 활성화합니다. WorkSpaces
- 3단계: Windows VM에서 BYOL 검사기 스크립트 PowerShell 실행
- 4단계: 가상화 환경에서 VM 내보내기
- 5단계: VM을 이미지로 Amazon EC2에 가져오기
- 6단계: 콘솔을 사용하여 BYOL 이미지 생성 WorkSpaces
- 7단계: BYOL 이미지에서 사용자 지정 번들 생성
- 8단계: 전용 디렉터리 등록 WorkSpaces
- 9단계: BYOL 시작 WorkSpaces
- BYOL 계정 연결

요구 사항

시작하기 전에 다음을 확인하십시오.

- Microsoft 라이선스 계약에서 Windows를 가상 호스팅 환경에서 실행하도록 허용합니다.
- GPU를 지원하지 않는 번들 (그래픽.G4dn, GraphicsPro .g4dn, Graphics 등이 아닌 번들) 을 사용할 경우 지역당 최소 100개를 사용해야 합니다. GraphicsPro WorkSpaces WorkSpaces 이 AutoStop WorkSpaces 100개에는 과 를 섞어서 사용할 수 있습니다. AlwaysOn 전용 하드웨어를 실행하려면 WorkSpaces 지역당 최소 100개를 WorkSpaces 사용해야 합니다. Microsoft 라이선스 요구 사항을 준수하려면 전용 하드웨어를 실행해야 합니다. WorkSpaces 전용 하드웨어가 별도로 프로비저닝되므로 VPC가 AWS 기본 테넌시를 유지할 수 있습니다.

  GPU 지원 (Graphics.G4dn, GraphicsPro .g4dn, Graphics 및 GraphicsPro) 번들을 사용할 계획이라면 전용 하드웨어에서 매월 한 지역에서 최소 4개 또는 20개의 GPU 지원 버전을 실행해야 합니다. AlwaysOn AutoStop WorkSpaces

  > **Note**
  >
  > - 현재 PCoIP 프로토콜에 대해서만 그래픽.g4dn, .g4dn, 그래픽 및 번들을 생성할 수 있습니다. GraphicsPro GraphicsPro
  > - 2023년 11월 30일 이후에는 Graphics 번들이 더 이상 지원되지 않습니다. Graphics.g4dn 번들로 마이그레이션하는 것이 좋습니다. WorkSpaces 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.
  > - 그래픽 및 GraphicsPro 번들은 현재 아시아 태평양 (뭄바이) 지역에서 사용할 수 없습니다.

- Graphics.g4dn, GraphicsPro .g4dn, 그래픽 및 GraphicsPro 번들은 현재 아프리카 (케이프타운) 지역에서 사용할 수 없습니다.
- 아프리카 (케이프타운) WorkSpaces 지역에서 를 실행하려면 아프리카 (케이프타운) 지역에서 최소 WorkSpaces 400개를 실행해야 합니다.
- Windows 11 번들은 WSP 프로토콜용으로만 생성할 수 있습니다.
- 그래픽.g4dn 및 GraphicsPro .g4dn 번들은 현재 Windows 11에서 사용할 수 없습니다.
- Windows 11에서는 그래픽 및 번들이 지원되지 않습니다. GraphicsPro
- Value 번들은 Windows 11에서 사용할 수 없습니다. 기존 밸류 번들 WorkSpaces 마이그레이션에 대한 자세한 내용은 을 참조하십시오. 마이그레이션 a WorkSpace
- 최상의 화상 회의 경험을 위해 Power 또는 Bundles를 사용하는 것이 좋습니다. PowerPro
- Windows 11이 작동하려면 UEFI (통합 확장 가능 펌웨어 인터페이스) 부팅 모드가 필요합니다. VM을 성공적으로 가져오려면 선택적 `--boot-mode` 매개 변수를 UEFI로 지정해야 합니다.

- WorkSpaces /16 IP 주소 범위의 관리 인터페이스를 사용할 수 있습니다. 관리 인터페이스는 대화형 스트리밍에 사용되는 보안 WorkSpaces 관리 네트워크에 연결됩니다. WorkSpaces 이를 통해 관리할 수 있습니다 WorkSpaces. 자세한 정보는 네트워크 인터페이스을 참조하세요. 이 목적을 위해 다음 IP 주소 범위 중 하나 이상에서 /16 넷마스크를 예약해야 합니다.
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

  Note
  - WorkSpaces 서비스를 채택함에 따라 사용 가능한 관리 인터페이스 IP 주소 범위가 자주 변경됩니다. 현재 사용 가능한 범위를 확인하려면 list-available-management-cidr-range AWS Command Line Interface (AWS CLI) 명령을 실행합니다.
  - 선택한 /16 CIDR 블록 외에도 54.239.224.0/20 IP 주소 범위가 모든 지역의 관리 인터페이스 트래픽에 사용됩니다. AWS
- Microsoft Windows에 필요한 관리 인터페이스 포트와 WorkSpaces BYOL용 Microsoft Office KMS 정품 인증을 열었는지 확인하십시오. 자세한 정보는 관리 인터페이스 포트을 참조하세요.

- 지원되는 64비트 버전의 Windows를 실행하는 가상 머신(VM)이 있습니다. 지원되는 버전 목록은 이 주제의 다음 단원인 BYOL을 지원하는 Windows 버전 단원을 참조하십시오. VM은 다음 요구 사항도 충족해야 합니다.
  - Windows 운영 체제를 키 관리 서버에 대해 활성화해야 합니다.
  - Windows 운영 체제의 기본 언어가 English (United States)(영어(미국))여야 합니다.
  - Windows에 포함된 것 이외의 소프트웨어를 VM에 설치할 수 없습니다. 나중에 사용자 지정 이미지를 생성하면 바이러스 백신 솔루션과 같은 소프트웨어를 추가할 수 있습니다.
  - 이미지를 생성하기 전에는 기본 사용자 프로필(`C:\Users\Default`)을 사용자 지정하거나 기타 방법으로도 사용자 지정하지 마십시오. 모든 사용자 지정은 이미지 생성 후에 이루어져야 합니다. 이미지 생성 후에 그룹 정책 객체(GPO)를 통해 사용자 프로필을 사용자 지정하고 적용하는 것이 좋습니다. 이는 GPO를 통해 수행된 사용자 지정은 쉽게 수정하거나 롤백할 수 있으며 기본 사용자 프로필에 수행된 사용자 지정보다 오류가 발생할 가능성이 낮기 때문입니다.
  - 이미지를 공유하기 전에 로컬 관리자 액세스 권한이 있는 WorkSpaces_BYOL 계정을 만들어야 합니다. 이 계정에 대한 암호는 나중에 필요할 수 있으므로 기록해 두십시오.
  - VM은 최대 크기가 70GB이고 최소 10GB의 사용 가능한 공간을 갖춘 단일 볼륨에 있어야 합니다. BYOL 이미지를 위해 Microsoft Office를 구독할 계획이라면 VM이 단일 볼륨에 있어야 하며 최대 크기가 70GB이고 사용 가능한 공간이 20GB 이상이어야 합니다. 루트 볼륨이 있는 디스크는 70GB를 초과할 수 없습니다.
  - VM에서 Windows PowerShell 버전 4 이상을 실행해야 합니다.
- 3단계: Windows VM에서 BYOL 검사기 스크립트 PowerShell 실행에서 BYOL 검사기 스크립트를 실행하기 전에 최신 Microsoft Windows 패치를 설치했는지 확인하세요.

> **Note**
>
> - AutoStop WorkSpacesBYOL의 경우 동시 로그인 수가 많으면 사용 WorkSpaces 가능한 시간이 크게 늘어날 수 있습니다. 동시에 많은 사용자가 BYOL에 로그인할 것으로 예상되는 경우 AutoStop WorkSpaces 계정 관리자에게 조언을 구하십시오.
> - 암호화된 AMI는 가져오기 프로세스에서 지원되지 않습니다. EBS 암호화를 사용하는 EC2 AMI를 생성하는 데 사용된 인스턴스를 비활성화해야 합니다. 최종 WorkSpaces 버전이 프로비저닝된 후에 암호화를 활성화할 수 있습니다.

BYOL을 지원하는 Windows 버전

VM은 다음 Windows 버전 중 하나를 실행해야 합니다.

- Windows 10 버전 21H2(2021년 12월 업데이트)
- Windows 10 버전 22H2(2022년 11월 업데이트)
- 윈도우 10 엔터프라이즈 LTSC 2019 (1809)
- 윈도우 10 엔터프라이즈 LTSC 2021 (21/2)
- 윈도우 11 버전 23H2 (2023년 10월 릴리스)
- Windows 11 버전 22H2(2022년 10월 릴리스)

지원되는 모든 OS 버전은 사용 중인 AWS 지역에서 사용할 수 있는 모든 컴퓨팅 유형을 지원합니다. WorkSpaces Microsoft에서 더 이상 지원하지 않는 Windows 버전은 작동이 보장되지 않으며 AWS 지원 부서에서 지원하지 않습니다.

> **Note**
>
> Windows 10 N 및 Windows 11 N 버전은 현재 BYOL에서 지원되지 않습니다.

BYOL 이미지에 Microsoft Office 추가

Office를 구독하기로 선택한 AWS경우 추가 요금이 적용됩니다. 자세한 내용은 WorkSpaces 요금을 참조하십시오.

> **Important**
>
> - BYOL 이미지를 만드는 데 사용하는 VM에 Microsoft Office가 이미 설치되어 있는 경우 Office를 통해 구독하려면 VM에서 해당 Office를 제거해야 합니다. AWS
> - Office를 AWS구독하려는 경우 VM에 20GB 이상의 사용 가능한 디스크 공간이 있는지 확인하세요.
> - 이미지를 가져오는 동안 Office 2016 또는 2019는 구독할 수 있지만 Office 2021은 구독할 수 없습니다. Office 2021과 Microsoft Visio 2021 및 Microsoft Project 2021 등 기타 애플리케이션의 경우 Manage applications를 참조하세요.

- WorkSpacesAmazon의 브라우저 기반 애플리케이션과 데스크톱 애플리케이션 모두에 대해 자체 Microsoft 365 라이선스를 사용하려면 BYOL 이미지 통합 프로세스가 완료된 후 BYOL 이미지에 Microsoft 365 애플리케이션을 설치해야 합니다.

> **Note**
>
> 그래픽.G4dn GraphicsPro 및.g4dn BYOL 이미지는 오피스 2019만 지원하며 오피스 2016은 지원하지 않습니다.

Office를 구독하는 경우 BYOL 이미지 수집 프로세스에는 최소 3시간이 소요됩니다.

BYOL 수집 프로세스 중 Office를 구독하는 방법에 대한 자세한 내용은 6단계: 콘솔을 사용하여 BYOL 이미지 생성 WorkSpaces 섹션을 참조하세요.

Office 언어 설정

BYOL 이미지 통합을 수행하는 지역에 따라 Office 구독에 사용되는 언어를 선택합니다. AWS 예를 들어 아시아 태평양(도쿄) 리전에서 BYOL 이미지 통합을 수행하는 경우 Office 구독의 언어는 일본어입니다.

기본적으로 자주 사용되는 여러 Office 언어 팩이 사용자 컴퓨터에 설치됩니다. WorkSpaces 원하는 언어 팩이 설치되지 않은 경우 Microsoft에서 언어 팩을 추가로 다운로드할 수 있습니다. 자세한 내용은 Microsoft 설명서에서 Language Accessory Pack for Office를 참조하세요.

Office의 언어를 변경하려면 다음과 같은 몇 가지 옵션을 사용할 수 있습니다.

옵션 1: 개별 사용자가 Office 언어 설정을 사용자 지정하도록 허용

개별 사용자는 자신의 Office 언어 설정을 조정할 수 WorkSpaces 있습니다. 자세한 내용은 Microsoft 설명서의 Office에서 편집 또는 작성 언어 추가 또는 언어 기본 설정 지정을 참조하세요.

옵션 2: GPO 관리 템플릿 (.admx/.adml) 을 사용하여 모든 사용자에게 기본 Office 언어 설정을 적용합니다. WorkSpaces

GPO (그룹 정책 개체) 설정을 사용하여 사용자에게 기본 Office 언어 설정을 적용할 수 있습니다. WorkSpaces

> **Note**
>
> WorkSpaces 사용자는 GPO를 통해 적용되는 언어 설정을 재정의할 수 없습니다.

GPO를 사용하여 Office에 언어를 설정하는 방법에 대한 자세한 내용은 Microsoft 설명서의 Office 언어 설정 사용자 지정을 참조하세요. Office 2016과 Office 2019는 동일한 GPO 설정(Office 2016으로 레이블이 지정됨)을 사용합니다.

GPO를 사용하려면 Active Directory 관리 도구를 설치해야 합니다. Active Directory 관리 도구를 사용하여 GPO를 작업하는 방법에 대한 자세한 내용은 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

Office 2016 또는 Office 2019 정책 설정을 구성하려면 먼저 Microsoft Download Center에서 Office용 관리 템플릿 파일(.admx/.adml)을 다운로드해야 합니다. 관리 템플릿 파일을 다운로드한 후에는 디렉터리의 도메인 컨트롤러의 중앙 저장소에 `office16.admx` 및 `office16.adml` 파일을 추가해야 합니다. WorkSpaces (`office16.admx` 및 `office16.adml` 파일은 Office 2016과 Office 2019에 모두 적용됩니다.) `.admx` 및 `.adml` 파일 작업에 대한 자세한 내용은 Microsoft 설명서에서 How to create and manage the Central Store for Group Policy Administrative Templates in Windows를 참조하세요.

다음 절차에서는 중앙 저장소를 생성하고 관리 템플릿 파일을 추가하는 방법을 설명합니다. 디렉터리에 연결된 디렉터리 관리 WorkSpace 또는 Amazon EC2 인스턴스에서 다음 절차를 수행합니다. WorkSpaces

Office에 그룹 정책 관리 템플릿 파일을 설치하는 방법

1. Microsoft Download Center에서 Office용 관리 템플릿 파일(.admx/.adml)을 다운로드합니다.
2. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 Windows 파일 탐색기를 열고 주소 표시줄에 조직의 FQDN (정규화된 도메인 이름) (예:) 을 입력합니다. WorkSpaces `\\example.com`
3. `SYSVOL` 폴더를 엽니다.
4. 이름이 *`FQDN`*인 폴더를 엽니다.
5. `Policies` 폴더를 엽니다. 이제 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies`에 들어왔을 것입니다.
6. 아직 폴더가 없다면 이름을 `PolicyDefinitions`로 지정하여 폴더를 만듭니다.
7. `PolicyDefinitions` 폴더를 엽니다.
8. `office16.admx` 파일을 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions` 폴더로 복사합니다.

9. `PolicyDefinitions` 폴더에 이름이 `en-US`인 폴더를 만듭니다.
10. `en-US` 폴더를 엽니다.
11. `office16.adml` 파일을 `\\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-US` 폴더로 복사합니다.

Office에 GPO 언어 설정을 구성하는 방법

1. 디렉터리 관리 WorkSpace 또는 디렉터리에 연결된 Amazon EC2 인스턴스에서 그룹 정책 관리 도구 () gpmc.msc 를 엽니다. WorkSpaces
2. 포리스트(Forest:***FQDN***)를 확장합니다.
3. 도메인을 확장합니다.
4. FQDN(예: `example.com`)을 확장합니다.
5. FQDN을 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 작업 메뉴를 연 후 이 도메인에 GPO를 생성하고 여기에 연결을 선택합니다.
6. GPO의 이름을 지정합니다(예: **`Office`**).
7. GPO를 선택하고 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 작업 메뉴를 연 후 편집을 선택합니다.
8. 그룹 정책 관리 편집기에서 사용자 구성, 정책, 로컬 컴퓨터에서 검색한 관리 템플릿 정책 정의(ADMX 파일), Microsoft Office 2016, 언어 기본 설정을 선택합니다.

   > **Note**
   >
   > Office 2016과 Office 2019는 동일한 GPO 설정(Office 2016으로 레이블이 지정됨)을 사용합니다. 사용자 구성, 정책에 로컬 컴퓨터에서 검색된 관리 템플릿 정책 정의(ADMX 파일)가 표시되지 않으면 `office16.admx` 및 `office16.adml` 파일이 도메인 컨트롤러에 제대로 설치되지 않은 것입니다.

9. 언어 기본 설정에서 다음 설정에 사용할 언어를 지정합니다. 각 설정을 활성화됨으로 설정한 다음 옵션에서 원하는 언어를 선택합니다. 확인을 선택하여 각 설정을 저장합니다.
   - 표시 언어 > 도움말을 표시할 언어
   - 표시 언어 > 메뉴 및 대화 상자를 표시할 언어
   - 편집 언어 > 기본 편집 언어
10. 작업을 마치면 그룹 정책 관리 도구를 닫습니다.

11. 그룹 정책 설정 변경 사항은 해당 세션의 다음 그룹 정책 업데이트 WorkSpace 이후와 WorkSpace 세션이 다시 시작된 후에 적용됩니다. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.

    - 를 재부팅합니다 WorkSpace (Amazon WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
    - 관리 명령 프롬프트에서 gpupdate /force를 입력합니다.

옵션 3: 사용자의 Office 언어 레지스트리 설정을 업데이트하십시오. WorkSpaces

레지스트리를 통해 Office 언어 설정을 지정하려면 다음 레지스트리 설정을 업데이트하세요.

- HKEY_CURRENT_USER\ 소프트웨어\ 마이크로소프트\ 오피스\ 16.0\ Common\ UI언어 LanguageResources
- HKEY_CURRENT_USER\ 소프트웨어\ 마이크로소프트\ 오피스\ 16.0\ 커먼\ LanguageResources HelpLanguage

이러한 설정의 경우 적절한 오피스 로캘 ID(LCID)와 함께 DWORD 키 값을 추가하세요. 예를 들어 영어(미국)의 LCID는 1033입니다. LCID는 10진수 값이므로 DWORD 값의 Base 옵션을 십진수로 설정해야 합니다. Office LCID 목록은 Microsoft 설명서에서 Office 2016의 언어 식별자 및 OptionState ID 값을 참조하십시오.

GPO 설정 또는 로그온 스크립트를 WorkSpaces 통해 이러한 레지스트리 설정을 사용자에게 적용할 수 있습니다.

Office의 언어 설정을 사용하는 방법에 대한 자세한 내용은 Microsoft 설명서의 Customize language setup and settings for Office를 참조하세요.

기존 BYOL에 Office를 추가합니다. WorkSpaces

다음을 수행하여 기존 WorkSpaces BYOL에 Office 구독을 추가할 수도 있습니다.

- 애플리케이션 관리 (권장) - 기존 WorkSpaces 애플리케이션에 Microsoft Office, Microsoft Visio 또는 Microsoft Project 2021을 설치하고 구성할 수 있습니다. 자세한 내용은 Manage applications를 참조하세요.
- 마이그레이션 WorkSpace - Office와 함께 BYOL 번들을 설치한 후 WorkSpaces 마이그레이션 기능을 사용하여 기존 BYOL을 Office에 구독된 BYOL 번들로 WorkSpaces 마이그레이션할 수 있습니다. 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.

> **Note**
>
> 응용 프로그램 관리 옵션을 사용하면 Microsoft Office 2021과 Microsoft Visio 2021 및 Microsoft Project 2021과 같은 기타 응용 프로그램을 설치할 수 WorkSpaces 있습니다. 마이크로소프트 오피스 2016 또는 2019를 컴퓨터에 설치하려면 WorkSpaces 를 사용하십시오마이그레이션 a WorkSpace.

Microsoft Office 버전 간 마이그레이션

Microsoft Office 버전 간에 마이그레이션할 수 있는 옵션은 다음과 같습니다.

- 응용 프로그램 관리 (권장) - 원래 Office 버전을 제거하고 Office 2021과 Microsoft Visio 2021 및 Microsoft Project 2021과 같은 기타 응용 프로그램을 기존 버전에 설치할 수 있습니다. WorkSpaces 예를 들어 Microsoft Office 2019에서 Microsoft Office 2021로 마이그레이션하려면 애플리케이션 관리 워크플로를 사용하여 Microsoft Office 2019를 제거하고 Microsoft Office 2021을 설치합니다. 자세한 내용은 Manage applications를 참조하세요.
- 마이그레이션 WorkSpace - Microsoft Office 2016에서 Microsoft Office 2019로 또는 Microsoft Office 2019에서 Microsoft Office 2016으로 마이그레이션하려면 마이그레이션하려는 Office 버전을 구독하는 BYOL 번들을 만들어야 합니다. 그런 다음 WorkSpaces 마이그레이션 기능을 사용하여 Office를 WorkSpaces 구독하는 기존 BYOL을 마이그레이션하려는 Office 버전을 구독하는 BYOL 번들로 마이그레이션하세요. 예를 들어, 마이크로소프트 오피스 2016에서 마이크로소프트 오피스 2019로 마이그레이션하려면 마이크로소프트 오피스 2019를 구독하는 BYOL 번들을 만드세요. 그런 다음 WorkSpaces 마이그레이션 기능을 사용하여 Office 2016을 구독하는 기존 WorkSpaces BYOL을 Office 2019에 구독된 BYOL 번들로 마이그레이션할 수 있습니다. 자세한 내용은 마이그레이션을 참조하십시오. WorkSpace

이러한 옵션을 사용하여 Microsoft Office에 WorkSpaces 가입한 제품을 Microsoft 365 애플리케이션으로 AWS 마이그레이션할 수 있습니다. 그러나 응용 프로그램 관리는 사용자 컴퓨터에서 Microsoft Office를 제거하는 것으로 제한됩니다. WorkSpace Microsoft 365 응용 프로그램을 사용자 컴퓨터에 설치하려면 자체 도구 및 설치 프로그램을 가져와야 합니다 WorkSpaces.

> **Note**
>
> 응용 프로그램 관리를 사용하여 Microsoft Office, Microsoft Visio 또는 MicrosoftProject 2021을 사용자 컴퓨터에 설치하거나 제거할 수 있습니다. WorkSpaces Microsoft Office 2016 또는

2019 버전의 경우 사용자 버전에서만 제거할 수 있습니다 WorkSpaces. Microsoft Office 2016 또는 2019를 컴퓨터에 설치하려면 a를 마이그레이션하십시오 WorkSpaces WorkSpace.

마이그레이션 프로세스에 대한 자세한 내용은 마이그레이션 a WorkSpace 섹션을 참조하세요.

Office 구독 취소

Office 구독 취소 옵션은 다음과 같습니다.

- 응용 프로그램 관리 (권장) - Microsoft Office와 Microsoft Visio 및 Microsoft Project와 같은 다른 응용 프로그램을 사용자 컴퓨터에서 제거할 수 있습니다. WorkSpaces 자세한 내용은 Manage applications를 참조하세요.
- 마이그레이션 WorkSpace - Office에 구독되지 않은 BYOL 번들을 만들 수 있습니다. 그런 다음 WorkSpaces 마이그레이션 기능을 사용하여 기존 BYOL을 WorkSpaces Office에 구독되지 않은 BYOL 번들로 마이그레이션하세요. 자세한 정보는 마이그레이션 a WorkSpace을 참조하세요.

Office 업데이트

Office를 통해 AWS구독한 경우 Office 업데이트가 정기 Windows 업데이트의 일부로 포함됩니다. 모든 보안 패치와 업데이트를 최신 상태로 유지하려면 BYOL 기본 이미지를 정기적으로 업데이트하는 것이 좋습니다.

1단계: Amazon 콘솔을 사용하여 BYOL 계정의 자격 확인 WorkSpaces

계정을 BYOL에 사용할 수 있도록 하려면 먼저 확인 프로세스를 거쳐 BYOL 자격을 확인해야 합니다. 이 프로세스를 진행하기 전까지는 Amazon WorkSpaces 콘솔에서 BYOL 활성화 옵션을 사용할 수 없습니다.

Note

확인 프로세스에는 영업일 기준 최소 1일이 소요됩니다. 기존 AWS 계정의 CIDR 범위 및 BYOL 구성을 다른 계정에 적용하려는 경우 두 계정을 함께 연결하여 동일한 기본 하드웨어를 사용할 수 있습니다. AWS 계정을 연결하기 위해 지원 티켓을 제출할 필요는 없습니다. CreateAccountLinkInvitations및 와 같은 API를 사용하여 AWS 계정을 AcceptAccountLinkInvitation연결할 수 있습니다. 자세한 정보는 BYOL 계정 연결을 참조하세요.

Amazon 콘솔을 사용하여 BYOL 계정의 자격을 확인하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 선택한 다음 기존 보유 라이선스 사용 (BYOL) 에서 BYOL 설정 보기를 WorkSpaces 선택합니다. 계정에서 현재 BYOL을 사용할 수 없는 경우 다음 단계에 대한 지침을 제공하는 메시지가 나타납니다. 시작하려면 AWS 계정 관리자 또는 영업 담당자에게 문의하거나 센터에 문의하세요.AWS Support 담당자를 통해 BYOL 자격 여부를 확인할 수 있습니다.

   BYOL 자격 여부를 결정하려면 담당자에게 특정 정보가 필요합니다. 예를 들어, 다음 질문에 답하라는 요청을 받을 수 있습니다.

   - 앞서 나열한 BYOL 요구 사항을 검토하고 수락했나요?
   - BYOL에 계정을 활성화해야 하는 AWS 지역은 어디입니까?
   - 지역당 몇 개의 BYOL을 WorkSpaces 배포할 계획입니까? AWS
   - 램프업 계획은 어떻게 되나요?
   - 리셀러를 통해 구매하고 WorkSpaces 계신가요?
   - BYOL에 필요한 번들 유형은 무엇인가요?
   - 조직에 같은 지역에서 BYOL에 사용할 수 있는 다른 AWS 계정이 있습니까? 그렇다면 해당 계정을 연결하여 동일한 기본 하드웨어를 사용하도록 하고 싶으신가요?

     계정이 연결된 경우 BYOL 자격 여부를 판단하기 위해 해당 계정에 WorkSpaces 배포된 총 계정 수를 집계합니다. 위 두 질문에 모두 '예'로 답한 경우 계정을 함께 연결할 수 있습니다. CreateAccountLinkInvitations및 와 같은 API를 사용하여 AWS 계정을 AcceptAccountLinkInvitation연결할 수 있습니다. 다른 BYOL 지원 계정을 연결하되 다른 BYOL 설정 (CIDR 범위 및 이미지) 을 사용하려면 AWS Support에 문의하여 BYOL에 새 계정을 활성화하십시오.
3. BYOL 자격이 확인되면 다음 단계로 진행하여 Amazon 콘솔에서 계정에 BYOL을 활성화할 수 있습니다. WorkSpaces

2단계: Amazon 콘솔을 사용하여 BYOL 계정의 BYOL을 활성화합니다. WorkSpaces

계정에 대해 BYOL을 활성화하려면 관리 네트워크 인터페이스를 지정해야 합니다. 이 인터페이스는 안전한 Amazon WorkSpaces 관리 네트워크에 연결되어 있습니다. WorkSpace 데스크톱을 Amazon WorkSpaces 클라이언트에 대화식으로 스트리밍하고 Amazon에서 관리할 수 있도록 WorkSpaces 하는 데 사용됩니다 WorkSpace.

> **Note**
>
> 계정에 BYOL을 활성화하기 위해 이 절차의 단계는 리전별로 한 번만 수행하면 됩니다.

Amazon 콘솔을 사용하여 계정에 BYOL을 활성화하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 선택한 다음 기존 보유 라이선스 사용 (BYOL) 에서 BYOL 설정 보기를 WorkSpaces 선택합니다.
3. 계정 설정 페이지의 기존 보유 라이선스 사용(BYOL)에서 BYOL 활성화를 선택합니다.

   BYOL 활성화 옵션이 보이지 않는다면 해당 계정은 현재 BYOL을 사용할 수 없다는 의미입니다. 자세한 정보는 1단계: Amazon 콘솔을 사용하여 BYOL 계정의 자격 확인 WorkSpaces 을 참조하세요.
4. Bring Your Own License (BYOL)(기존 보유 라이선스 사용(BYOL)) 아래에 있는 Management network interface IP address range(관리 네트워크 인터페이스 IP 주소 범위) 영역에서 IP 주소 범위를 선택한 다음 Display available CIDR blocks(사용 가능한 CIDR 블록 표시)를 선택합니다.

   WorkSpaces Amazon은 사용자가 지정한 범위 내에서 사용 가능한 IP 주소 범위를 검색하여 IPv4 클래스 없는 도메인 간 라우팅 (CIDR) 블록으로 표시합니다. 특정 IP 주소 범위가 필요한 경우 검색 범위를 편집할 수 있습니다.

   > **Important**
   >
   > IP 주소 범위를 지정한 후에는 수정할 수 없습니다. 내부 네트워크에서 사용하는 범위와 충돌하지 않는 IP 주소 범위를 지정해야 합니다. 지정할 범위에 대해 궁금한 점이 있으면 계속 진행하기 전에 AWS 계정 관리자 또는 영업 담당자에게 문의하거나 센터에 문의하십시오.AWS Support
5. 결과 목록에서 원하는 CIDR 블록을 선택한 다음 Enable BYOL(BYOL 활성화)을 선택합니다.

   이 프로세스는 여러 시간이 걸릴 수 있습니다. BYOL 계정을 WorkSpaces 활성화하는 동안 다음 단계로 진행하십시오.

3단계: Windows VM에서 BYOL 검사기 스크립트 PowerShell 실행

계정에 대해 BYOL을 활성화한 후에는 VM이 BYOL에 대한 요구 사항을 충족하는지 확인해야 합니다. 이렇게 하려면 다음 단계를 수행하여 WorkSpaces BYOL 검사기 스크립트를 다운로드하고 실행합니다. PowerShell 이 스크립트는 이미지를 생성하는 데 사용할 계획인 VM에서 일련의 테스트를 수행합니다.

> **Important**
>
> BYOL에 VM을 사용하려면 먼저 VM이 모든 테스트를 통과해야 합니다.

BYOL 확인 스크립트를 다운로드하려면

BYOL 확인 스크립트를 다운로드하여 실행하기 전에 최신 Windows 보안 업데이트가 VM에 설치되어 있는지 확인합니다. 이 스크립트를 실행하는 동안에는 Windows 업데이트 서비스가 비활성화됩니다.

1. https://tools.amazonworkspaces.com/BYOLChecker.zip 에서 BYOL 확인 스크립트 .zip 파일을 `Downloads` 폴더에 다운로드합니다.
2. `Downloads` 폴더에 `BYOL` 폴더를 만듭니다.
3. `BYOLChecker.zip` 파일의 압축을 풀고 이를 `Downloads\BYOL` 폴더에 복사합니다.
4. 압축을 푼 파일만 남아 있도록 `Downloads\BYOLChecker.zip` 폴더를 삭제합니다.

다음 단계를 수행하여 BYOL 확인 스크립트를 실행합니다.

BYOL 확인 스크립트를 실행하려면

1. Windows 데스크톱에서 Windows를 엽니다. PowerShell Windows 시작 버튼을 선택하고 PowerShellWindows를 마우스 오른쪽 단추로 클릭한 다음 관리자 권한으로 실행을 선택합니다. 사용자 계정 컨트롤에서 장치를 변경할지 여부를 선택하라는 메시지가 표시되면 [예] 를 선택합니다. PowerShell
2. PowerShell 명령 프롬프트에서 BYOL Checker 스크립트가 있는 디렉토리로 변경합니다. 예를 들어 스크립트가 `Downloads\BYOL` 디렉터리에 있는 경우 다음 명령을 입력하고 Enter 키를 누릅니다.

   ```
   cd C:\Users\username\Downloads\BYOL
   ```
3. 다음 명령을 입력하여 컴퓨터의 PowerShell 실행 정책을 업데이트합니다. 그러면 BYOL 확인 스크립트를 실행할 수 있습니다.

```
Set-ExecutionPolicy AllSigned
```

4. PowerShell 실행 정책 변경 여부를 확인하라는 메시지가 표시되면 를 입력하여 Yes A to All로 지정합니다.
5. 다음 명령을 입력하여 BYOL 확인 스크립트를 실행합니다.

   ```
   .\BYOLChecker.ps1
   ```
6. 보안 알림이 나타나면 R 키를 눌러 Run Once(한 번 실행)를 수행합니다.
7. [WorkSpaces 이미지 검증] 대화 상자에서 [테스트 시작] 을 선택합니다.
8. 각 테스트가 완료된 후 테스트의 상태를 볼 수 있습니다. 테스트의 상태가 FAILED(실패)인 경우 Info(정보)를 선택하여 실패의 원인이 된 문제를 해결하는 방법에 대한 정보를 표시합니다. 테스트가 WARNING(경고) 상태를 표시하는 경우 Fix All Warnings(모든 경고 수정) 버튼을 선택합니다.
9. 해당하는 경우 테스트 실패 및 경고의 원인이 되는 문제를 해결하고 VM이 모든 테스트를 통과할 때까지 Step 7 및 Step 8를 반복합니다. VM을 내보내기 전에 모든 실패와 경고를 해결해야 합니다.
10. BYOL 스크립트 확인에서는 `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` 및 `ImageInfo.text`의 로그 파일 두 개가 생성됩니다. 이러한 파일은 BYOL 확인 스크립트 파일이 포함된 디렉터리에 있습니다.

    > **Tip**
    >
    > 이러한 파일을 삭제하지 마십시오. 문제가 발생하는 경우 이러한 파일이 문제 해결에 도움이 될 수 있습니다.

11. VM에서 모든 테스트를 통과하면 Validation Successful(검증 성공) 메시지가 표시됩니다. 도구에 표시된 VM 로캘 설정을 검토합니다. 로캘 설정을 업데이트하려면 Microsoft 설명서의 이 지침을 따르고 BYOL 확인 스크립트를 다시 실행합니다.
12. VM을 종료하고 스냅샷을 만듭니다.
13. VM을 다시 시작합니다. Run Sysprep(Sysprep 실행)을 선택합니다. Sysprep이 성공하면 Step 12 이후에 내보낸 VM을 Amazon Elastic Compute Cloud(Amazon EC2)로 가져올 수 있습니다. 그렇지 않으면 Sysprep 로그를 검토하고, Step 12에서 만든 스냅샷으로 롤백하고, 보고된 문제를 해결하고, 새 스냅샷을 만든 다음, BYOL 확인 스크립트를 다시 실행합니다.

    Sysprep이 실패하는 가장 일반적인 이유는 최신 AppX 패키지가 모든 사용자에 대해 설치되지 않았기 때문입니다. Remove-AppxPackage PowerShell cmdlet을 사용하여 AppX 패키지를 제거합니다.

14. 이미지를 성공적으로 생성한 후에는 _BYOL 계정을 제거할 수 있습니다. WorkSpaces

오류 메시지 및 오류 수정 목록

BYOL을 가져오려면 PowerShell 4.0 이상이 필요합니다. 설치된 버전은 지원되지 PowerShell 않습니다.

PowerShell 버전 4.0 이상을 설치해야 합니다. 자세한 내용은 Microsoft Windows를 참조하십시오 PowerShell.

BYOL 가져오기는 활성 Microsoft Office가 설치된 시스템을 지원하지 않습니다.

가져오기 전에 Microsoft Office를 제거해야 합니다. 자세한 내용은 PC에서 PC에서 Office 제거를 참조하세요.

BYOL을 가져오려면 PCoIP 에이전트가 없는 시스템이 필요합니다.

PCoIP 에이전트를 제거합니다. PCoIP 에이전트 제거에 대한 자세한 내용은 Uninstalling the Teradici PCoIP Software Client for Mac을 참조하세요.

BYOL을 가져오려면 Windows 업데이트를 비활성해야 합니다.

다음 단계에 따라 Windows 업데이트를 비활성화하세요.

1. Windows 키 + R을 누르고 `services.msc`를 입력한 후 Enter 키를 누릅니다.
2. Windows 업데이트를 마우스 오른쪽 버튼으로 클릭한 다음 속성을 선택합니다.
3. 일반 탭에서 시작 유형을 비활성화됨으로 설정합니다.
4. 중지를 선택합니다.
5. 적용을 선택하고 확인을 선택합니다.
6. 컴퓨터를 다시 시작합니다.

BYOL을 가져오려면 자동 마운트를 활성화해야 합니다.

자동 마운트를 활성화해야 합니다. 관리자 권한으로 PowerShell에서 다음 명령을 실행합니다.

```
C:\> diskpart
DISKPART> automount enable
```

새 볼륨 자동 마운트가 활성화되었습니다.

BYOL을 가져오려면 WorkSpaces _BYOL 계정을 활성화해야 합니다.

WorkSpaces_BYOL 계정을 활성화해야 합니다. 자세한 내용은 Amazon 콘솔을 사용하여 BYOL에 대한 계정의 BYOL 활성화를 참조하십시오. WorkSpaces

BYOL을 가져오려면 네트워크 인터페이스가 DHCP를 사용하여 IP 주소를 자동으로 할당해야 합니다. 네트워크 인터페이스가 현재 고정 IP 주소를 사용하고 있습니다.

네트워크 인터페이스가 DHCP를 사용하도록 변경해야 합니다. 자세한 내용은 TCP/IP 설정 변경을 참조하세요.

BYOL을 가져오려면 로컬 디스크에 20GB 이상의 공간이 필요합니다.

로컬 디스크에는 충분한 공간이 있어야 하며 20GB 이상의 여유 공간이 필요합니다.

BYOL을 가져오려면 로컬 드라이브 1개가 있는 시스템이 필요합니다. 추가 로컬, 이동식 또는 네트워크 드라이브가 있습니다.

이미지를 가져오는 데 사용되는 드라이브에는 WorkSpace C 및 D 드라이브만 있을 수 있습니다. 가상 드라이브를 포함한 기타 모든 드라이브를 제거합니다.

BYOL을 가져오려면 Windows 10 또는 Windows 11이 필요합니다.

Windows 10 또는 Windows 11 운영 체제를 사용하세요.

BYOL을 가져오려면 AD 도메인에 조인되지 않은 시스템이 필요합니다.

시스템이 AD 도메인에 조인되지 않아야 합니다. 자세한 내용은 Azure Active Directory device management FAQ를 참조하세요.

BYOL을 가져오려면 Azure 도메인에 조인되지 않은 시스템이 필요합니다.

시스템이 Azure 도메인에 조인되지 않아야 합니다. 자세한 내용은 Azure Active Directory device management FAQ를 참조하세요.

BYOL을 가져오려면 Windows Public Firewall을 비활성화해야 합니다.

공용 방화벽 프로필을 비활성화해야 합니다. 자세한 내용은 Microsoft Defender 방화벽 설정 또는 해제를 참조하세요.

BYOL을 가져오려면 VMware 도구가 없는 시스템이 필요합니다.

VMware 도구를 제거해야 합니다. 자세한 내용은 Uninstalling and manually installing VMware Tools in VMware Fusion (1014522)을 참조하세요.

BYOL을 가져오려면 로컬 디스크가 80GB 미만이어야 합니다.

디스크가 80GB보다 작아야 합니다. 디스크 크기를 줄이세요.

BYOL을 가져오려면 로컬 드라이브에 파티션이 2개 미만이어야 합니다. 또한 모든 Windows 10 파티션은 MBR로 파티셔닝되어야 하고 모든 Windows 11 파티션은 GPT로 파티셔닝되어야 합니다.

볼륨은 Windows 10의 경우 MBR로 파티셔닝되고 Windows 11의 경우 GPT로 파티셔닝되어야 합니다. 자세한 내용은 Manage disks를 참조하세요.

BYOL을 가져오려면 재부팅이 필요한 보류 중인 모든 업데이트를 완료해야 합니다.

모든 업데이트를 설치하고 운영 체제를 재부팅하세요.

BYOL을 가져오려면 이 옵션을 비활성화해야 AutoLogon 합니다.

레지스트리를 AutoLogon 비활성화하려면:

1. Windows 키 + R을 누르고 명령 프롬프트에 `Regedit.exe`를 입력합니다.
2. `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`까지 아래로 스크롤합니다.
3. `DontDisplayLastUserName`에 값을 추가합니다.
4. 유형에 `REG_SZ`를 입력합니다.
5. 값에 `0`를 입력합니다.

> **Note**
>
> - `DontDisplayLastUserName` 값은 로그온 대화 상자에 PC에 마지막으로 로그온한 사용자의 사용자 이름을 표시할지 여부를 결정합니다.
> - 값은 기본적으로 존재하지 않습니다. 존재하는 경우 로 `0` 설정해야 합니다. 그렇지 `DefaultUser` 않으면 의 값이 지워지고 AutoLogon 실패합니다.

BYOL을 가져오려면 **`RealTimeIsUniversal`**을 활성화해야 합니다.

RealTimeUniversal 레지스트리 키를 활성화해야 합니다. 자세한 내용은 Windows Server 2008 이상에 대한 시간 설정 구성을 참조하세요.

BYOL을 가져오려면 부팅 가능한 파티션 하나가 있는 시스템이 필요합니다.

부팅 가능한 파티션 수는 1개를 초과할 수 없습니다.

추가 파티션을 제거하는 방법

1. Windows 로고 + R 키를 눌러 실행 상자를 엽니다. `msconfig`를 입력하고 키보드에서 Enter 키를 눌러 시스템 구성 창을 엽니다.
2. 창에서 부팅 탭을 선택하고 사용하려는 OS가 현재 OS, 기본 OS로 설정되어 있는지 확인합니다. 설정되어 있지 않으면 창에서 원하는 OS를 선택하고 같은 창에서 기본값으로 설정을 선택합니다.
3. 다른 파티션을 삭제하려면 해당 파티션을 선택한 다음 삭제, 적용, 확인을 선택합니다.

오류가 계속 표시되면 설치 또는 복구 디스크에서 컴퓨터를 부팅하고 다음 단계를 따르세요.

1. 초기 언어 화면을 건너뛰고 기본 설치 화면에서 컴퓨터 복구를 선택합니다.
2. 옵션 선택 화면에서 문제 해결을 선택합니다.
3. 고급 옵션 화면에서 명령 프롬프트를 선택합니다.
4. 명령 프롬프트에서 `bootrec.exe /fixmbr`를 입력한 다음 Enter 키를 누릅니다.

BYOL을 가져오려면 64비트 시스템이 필요합니다.

64비트 OS 이미지를 사용해야 합니다. 자세한 내용은 BYOL을 지원하는 Windows 버전을 참조하세요.

BYOL을 가져오려면 초기화되지 않은 시스템이 필요합니다.

이미지 초기화 횟수가 0이 아니어야 합니다. 초기화 기능을 사용하면 Windows 평가판의 정품 인증 기간을 연장할 수 있습니다. 이미지 생성 프로세스에서는 초기화 횟수가 0이외의 값이어야 합니다.

Windows 초기화 횟수를 확인하려면

1. Windows 시작 메뉴에서 Windows 시스템을 선택한 다음 명령 프롬프트를 선택합니다.
2. 명령 프롬프트에서 `cscript C:\Windows\System32\slmgr.vbs /dlv`를 입력한 다음 Enter 키를 누릅니다.
3. 초기화 횟수를 0 이외의 값으로 재설정합니다. 자세한 내용은 Sysprep (Generalize) a Windows installation을 참조하세요.

BYOL을 가져오려면 인플레이스로 업그레이드되지 않은 시스템이 필요합니다. 이 시스템은 인플레이스로 업그레이드되었습니다.

Windows가 이전 버전에서 업그레이드되지 않았어야 합니다.

BYOL을 가져오려면 시스템에 바이러스 백신이 설치되어 있지 않아야 합니다.

바이러스 백신 소프트웨어를 제거해야 합니다. BYOL 검사기를 실행하여 제거할 바이러스 백신 소프트웨어에 대한 세부 정보를 확인합니다.

BYOL을 가져오려면 Windows 10 시스템에 레거시 부팅 모드가 있어야 합니다.

Windows 10에는 레거시 BIOS를 BootMode 사용해야 합니다. 자세한 내용은 부팅 모드를 참조하십시오.

4단계: 가상화 환경에서 VM 내보내기

BYOL에 대한 이미지를 생성하려면 먼저 가상화 환경에서 VM을 내보내야 합니다. VM은 최대 크기가 70GB이고 최소 10GB의 사용 가능한 공간을 갖춘 단일 볼륨에 있어야 합니다. 자세한 내용은 가상화 환경의 설명서와 VM Import/Export 사용 설명서의 가상화 환경 설명서 및 해당 가상화 환경에서 Export Your VM from its Virtualization Environment를 참조하세요.

5단계: VM을 이미지로 Amazon EC2에 가져오기

VM을 내보낸 후 VM에서 Windows 운영 체제를 가져오기 위한 요구 사항을 검토합니다. 필요에 따라 작업을 수행합니다. 자세한 내용은 VM Import/Export 요구 사항을 참조하십시오.

> **Note**
>
> 암호화된 디스크를 사용하는 VM은 가져오기가 지원되지 않습니다. Amazon Elastic Block Store(Amazon EBS) 볼륨에 대한 기본 암호화를 선택한 경우 VM을 가져오기 전에 해당 옵션을 선택 취소해야 합니다.

VM을 Amazon Machine Image(AMI)로 Amazon EC2에 가져옵니다. 다음 방법 중 한 가지를 선택하세요.

- import-image 명령과 AWS CLI를 함께 사용합니다. 자세한 내용은 AWS CLI Command Reference의 import-image를 참조하세요.
- ImportImage API 작업을 사용합니다. 자세한 내용은 Amazon EC2 API 참조를 참조하십시오 ImportImage.

자세한 내용은 VM Import/Export 사용 설명서에서 Importing a VM as an Image를 참조하세요.

6단계: 콘솔을 사용하여 BYOL 이미지 생성 WorkSpaces

다음 단계를 수행하여 WorkSpaces BYOL 이미지를 생성합니다.

> **Note**
>
> 이 절차를 수행하려면 다음을 수행할 수 있는 AWS Identity and Access Management (IAM) 권한이 있는지 확인하십시오.
>
> - 전화 WorkSpaces **`ImportWorkspaceImage`**.
> - BYOL 이미지를 생성하는 데 사용할 Amazon EC2 이미지에서 Amazon EC2 **`DescribeImages`**를 호출합니다.
> - BYOL 이미지를 생성하는 데 사용할 Amazon EC2 이미지에서 Amazon EC2 **`ModifyImageAttribute`**를 호출합니다. Amazon EC2 이미지에 대한 시작 권한이 제한되지 않는지 확인하세요. 이미지는 BYOL 이미지 생성 프로세스 전체에서 공유할 수 있어야 합니다.
>
> WorkSpacesBYOL과 관련된 IAM 정책의 예는 을 참조하십시오. WorkSpaces의 Identity and Access Management IAM에서의 권한 작업에 대한 자세한 내용은 IAM 사용 설명서에서 IAM 사용자의 권한 변경을 참조하세요.
> 이미지에서 그래픽.G4dn, GraphicsPro .g4dn, 그래픽 또는 GraphicsPro 번들을 생성하려면 센터에 문의하여 계정을 허용 목록에 추가하세요.AWS Support 계정이 허용 목록에 등록되면 AWS CLI import-workspace-image 명령을 사용하여 그래픽.G4DN, .g4dn, 그래픽 또는 이미지를 인제스트할 수 있습니다. GraphicsPro GraphicsPro 자세한 내용은 명령 참조서를 참조하십시오. import-workspace-imageAWS CLI

Windows VM에서 이미지를 생성하려면

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 [Images]를 선택합니다.
3. BYOL 이미지 생성을 선택합니다.
4. BYOL 이미지 생성 페이지에서 다음을 수행합니다.

- AMI ID에서 EC2 콘솔 링크를 선택하고 이전 섹션(5단계: VM을 이미지로 Amazon EC2에 가져오기)에서 설명한 대로 가져온 Amazon EC2 이미지를 선택합니다. 이미지 이름은 `ami-`로 시작하고 뒤에 AMI의 식별자가 있어야 합니다(예: `ami-1234567e`).
- 이미지 이름에 이미지의 고유 이름을 입력합니다.
- 설명에 이미지를 신속하게 식별하는 데 도움이 되는 설명을 입력합니다.
- 인스턴스 유형에서 이미지에 사용할 프로토콜 (PCoIP 또는 WSP GraphicsPro) 중 적절한 번들 유형 (일반, Graphics.G4dn, 그래픽 또는) 을 선택합니다. WorkSpaces .g4dn 번들을 생성하려면 Graphics.g4dn을 선택하십시오. GraphicsPro GPU를 지원하지 않는 번들 (그래픽.G4dn, .g4dn, 그래픽 또는 이외의 번들) 의 경우 일반을 선택하십시오. GraphicsPro GraphicsPro

  > **Note**
  >
  > 그래픽.G4dn, GraphicsPro .g4dn, 그래픽 및 GraphicsPro 이미지는 현재 PCoIP 프로토콜용으로만 만들 수 있습니다.

- (선택 사항) 애플리케이션 선택에서 구독하려는 Microsoft Office 버전을 선택합니다. 자세한 정보는 BYOL 이미지에 Microsoft Office 추가을 참조하세요.
- (선택 사항) 태그에서 새 태그 추가를 선택하여 태그를 이 이미지에 연결합니다. 자세한 정보는 WorkSpaces 리소스 태그 지정을 참조하세요.

5. BYOL 이미지 생성을 선택합니다.

   이미지가 생성되는 동안 콘솔 이미지 페이지의 이미지 상태는 보류 중으로 표시됩니다. BYOL 수집 프로세스에는 최소 90분이 소요됩니다. Office도 구독하는 경우 프로세스에 최소 3시간이 걸릴 것으로 예상하세요.

   이미지 확인이 성공하지 않으면 콘솔에 오류 코드가 표시됩니다. 이미지 생성이 완료되면 상태가 사용 가능으로 변경됩니다.

7단계: BYOL 이미지에서 사용자 지정 번들 생성

BYOL 이미지가 생성된 후에는 이미지를 사용하여 사용자 지정 번들을 생성할 수 있습니다. 자세한 내용은 사용자 지정 WorkSpaces 이미지 및 번들 생성을 참조하세요.

8단계: 전용 디렉터리 등록 WorkSpaces

BYOL 이미지를 사용하려면 이 용도로 디렉터리를 등록해야 합니다. WorkSpaces

디렉터리를 등록하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리를 선택하고 Actions(작업), Deregister(등록 취소)를 선택합니다.
4. 디렉터리 등록 대화 상자의 전용 WorkSpaces 활성화에서 [예] 를 선택합니다.
5. 등록(Register)을 선택합니다.

전용 하드웨어에서 실행되지 WorkSpaces 않는 AWS Managed Microsoft AD 디렉터리 또는 AD Connector 디렉터리를 이미 등록한 경우 이를 위해 새 AWS Managed Microsoft AD 디렉터리나 AD Connector 디렉터리를 설정할 수 있습니다. 디렉터리를 등록 취소한 다음 전용 디렉터리로 다시 등록할 수도 있습니다. WorkSpaces 리디렉션하는 단계는 다음과 같습니다.

> **Note**
>
> 디렉토리와 연결된 WorkSpaces 디렉토리가 없는 경우에만 이 절차를 수행할 수 있습니다.

디렉터리 등록을 취소하고 전용 디렉터리에 다시 등록하려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 기존 항목을 WorkSpaces 종료합니다.
3. 탐색 창에서 디렉터리를 선택합니다.
4. 디렉터리를 선택하고 [Actions], [Deregister]를 선택합니다.
5. 확인 메시지가 나타나면 [Deregister]를 선택합니다.
6. 디렉터리를 다시 선택하고 Actions(작업), Register(등록)를 선택합니다.
7. 디렉터리 등록 대화 상자의 전용 WorkSpaces 활성화에서 [예] 를 선택합니다.
8. 등록(Register)을 선택합니다.

9단계: BYOL 시작 WorkSpaces

전용 WorkSpaces 디렉터리를 등록한 후 이 디렉터리에서 WorkSpaces BYOL을 시작할 수 있습니다. 시작 WorkSpaces 방법에 대한 자세한 내용은 을 참조하십시오. WorkSpaces를 사용하여 가상 데스크톱 시작

BYOL 계정 연결

BYOL 연결을 사용하여 계정을 연결하고 BYOL 구성을 공유할 수 있습니다. BYOL 구성에는 계정에서 사용하는 CIDR 범위와 Windows 라이선스로 만들 때 사용하는 이미지가 포함됩니다. WorkSpaces 연결된 모든 계정은 동일한 기본 하드웨어 인프라를 공유합니다.

BYOL 연결이 활성화된 계정은 기본 하드웨어 인프라의 기본 소유자이며, 이를 소스 계정이라고 합니다. Source 계정은 기본 하드웨어 인프라에 대한 액세스를 관리합니다. 대상 계정은 소스 계정에 연결된 계정입니다.

Important

BYOL 계정 연결을 위한 API는 현재 에서 사용할 수 없습니다. AWS GovCloud (US) Region

Note

연결하려는 AWS 계정은 조직의 일부이고 동일한 지급인 계정에 속해야 합니다. 동일한 지역 내 계정만 연결할 수 있습니다.

소스 계정과 대상 계정을 연결하려면

1. CreateAccountLinkInvitationAPI를 사용하여 소스 계정에서 Target 계정으로 초대 링크를 보냅니다.
2. AcceptAccountLinkInvitationAPI를 사용하여 Target 계정에서 보류 중인 링크를 수락하십시오.
3. GetAccountLink또는 ListAccountLinksAPI를 사용하여 링크가 설정되었는지 확인하십시오.

모니터링 WorkSpaces

다음 기능을 사용하여 모니터링할 수 있습니다 WorkSpaces.

CloudWatch 지표

Amazon은 CloudWatch WorkSpaces 귀하에 대한 데이터 포인트를 Amazon에 WorkSpaces 게시합니다. CloudWatch 이러한 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 지표를 사용하여 예상대로 WorkSpaces 수행되고 있는지 확인할 수 있습니다. 자세한 설명은 WorkSpaces 사용 CloudWatch 지표 모니터링 섹션을 참조하세요.

CloudWatch 이벤트

Amazon은 사용자가 로그인할 때 Amazon CloudWatch Events에 이벤트를 제출할 WorkSpaces 수 있습니다 WorkSpace. 이를 통해 이벤트가 발생할 경우 대응할 수 있습니다. 자세한 설명은 Amazon WorkSpaces 사용 현황 모니터링 EventBridge 섹션을 참조하세요.

CloudTrail 로그

AWS CloudTrail은 WorkSpaces에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공합니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 WorkSpaces, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 사용별 WorkSpaces API 호출 로깅을 참조하십시오 CloudTrail. AWS CloudTrail스마트 카드 사용자의 로그인 성공 및 실패 이벤트를 기록합니다. 자세한 설명은 스마트 카드 사용자의 AWS 로그인 이벤트에 대한 이해 섹션을 참조하세요.

CloudWatch 인터넷 모니터

Amazon CloudWatch Internet Monitor는 인터넷 문제가 호스팅되는 애플리케이션과 최종 사용자 간의 성능 및 가용성에 어떤 영향을 미치는지에 대한 AWS 가시성을 제공합니다. 또한 CloudWatch 인터넷 모니터를 사용하여 다음을 수행할 수 있습니다.

- 하나 이상의 WorkSpace 디렉터리에 대한 모니터를 생성합니다.
- 인터넷 성능을 모니터링합니다.
- 위치, ASN (일반적으로 인터넷 서비스 공급자 (ISP)), 해당 지역 등 최종 사용자의 도시 네트워크 간 문제에 대한 경보를 받을 수 있습니다. WorkSpace

Internet Monitor는 AWS가 글로벌 네트워킹 공간에서 수집한 연결 데이터를 사용하여 인터넷 트래픽의 성능 및 가용성에 대한 기준선을 계산합니다. Internet Monitor는 현재 개별 최종 사용자에게 인터넷 성능을 제공할 수 없지만 도시 및 ISP 수준에서는 제공할 수 있습니다.

CloudWatch 자동 대시보드를 사용하여 WorkSpaces 건강을 모니터링하세요

원시 데이터를 수집하여 읽을 수 있는 거의 실시간 지표로 처리하는 CloudWatch 자동 대시보드를 WorkSpaces 사용하여 모니터링할 수 있습니다. 지표는 15개월 동안 보관되어 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스의 성능을 모니터링할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

AWS계정을 사용하여 CloudWatch 대시보드를 구성하면 대시보드가 자동으로 생성됩니다 WorkSpaces. 대시보드를 사용하면 지역 전반의 상태 및 성과와 같은 WorkSpaces 지표를 모니터링할 수 있습니다. 대시보드를 다음과 같은 용도로도 사용할 수 있습니다.

- 비정상 WorkSpace 인스턴스를 식별하십시오.
- 비정상 WorkSpace 인스턴스가 있는 실행 모드, 프로토콜 및 운영 체제를 식별합니다.
- 시간 경과에 따른 중요 리소스 사용률을 확인하세요.
- 문제 해결에 도움이 되는 이상 징후를 식별하십시오.

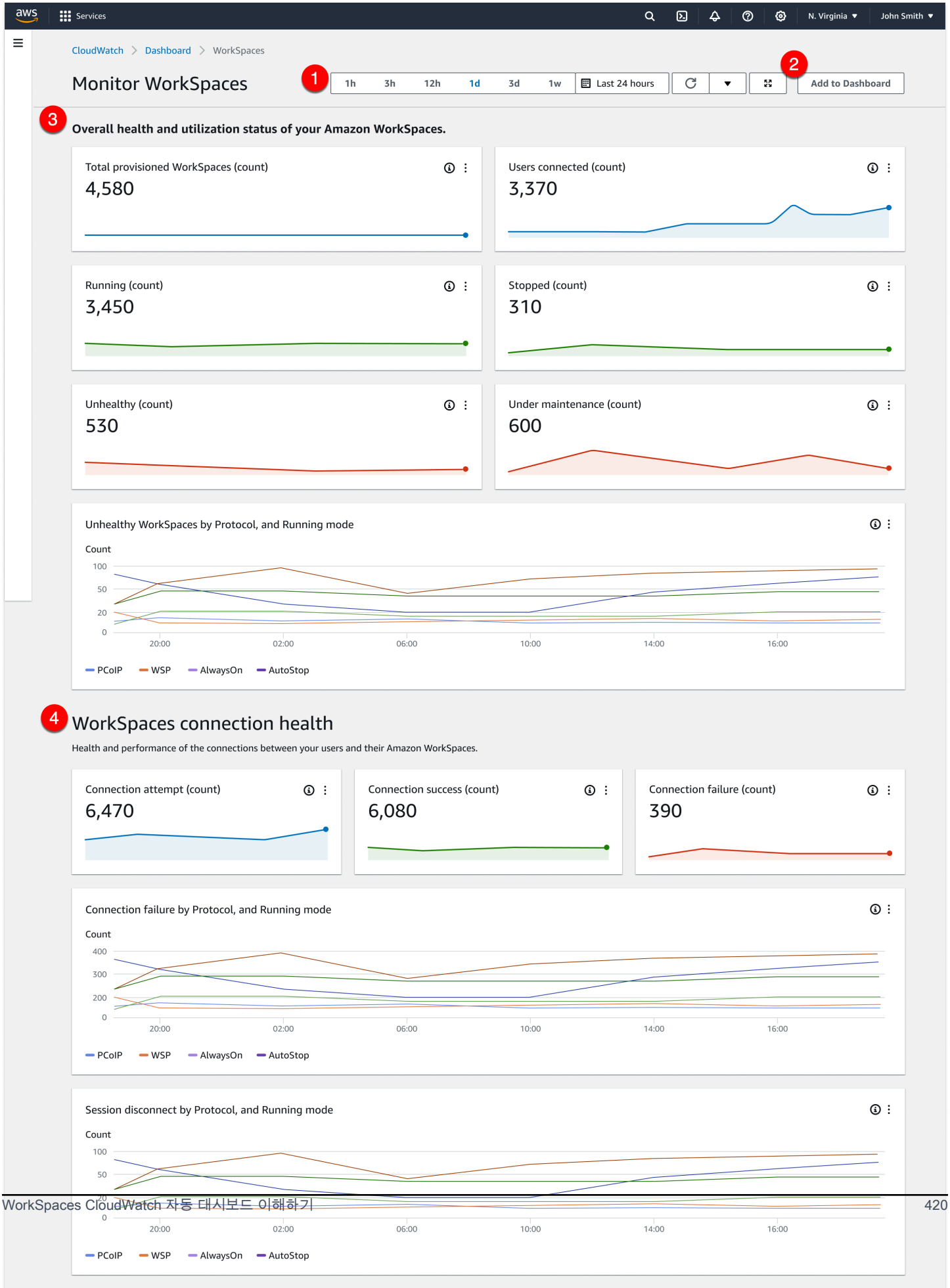
WorkSpaces CloudWatch 자동 대시보드는 모든 상업 지역에서 사용할 수 있습니다. AWS

WorkSpaces CloudWatch 자동 대시보드를 사용하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 대시보드를 선택합니다.
3. 자동 대시보드 탭을 선택합니다.
4. 선택합니다 WorkSpaces.

WorkSpaces CloudWatch 자동 대시보드 이해하기

CloudWatch 자동 대시보드를 사용하면 WorkSpaces 리소스 성과를 파악하고 성능 문제를 식별하는 데 도움이 됩니다.


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

대시보드는 다음과 같은 기능으로 구성되어 있습니다.

1. 시간 및 날짜 범위 제어를 사용하여 과거 데이터를 볼 수 있습니다.
2. 사용자 지정 대시보드에 CloudWatch 사용자 지정 대시보드 보기를 추가합니다.
3. 다음을 WorkSpaces 수행하여 전반적인 상태 및 사용률 상태를 모니터링하십시오.
    a. 프로비저닝된 총 수, 연결된 사용자 수 WorkSpaces, 비정상 및 정상 인스턴스 수를 볼 수 있습니다. WorkSpace
    b. 비정상 WorkSpaces 및 다양한 변수 (예: 프로토콜 및 컴퓨팅 모드) 를 볼 수 있습니다.
    c. 선 차트를 마우스로 가리키면 일정 기간 동안 특정 프로토콜 및 실행 모드의 정상 또는 비정상 WorkSpace 인스턴스 수를 볼 수 있습니다.
    d. 줄임표 메뉴를 선택한 다음 Metrics in metrics를 선택하여 시간 척도 차트에서 지표를 확인합니다.
4. 연결 지표와 해당 환경의 다양한 변수 (예: 해당 WorkSpaces 환경의 연결 시도 횟수, 연결 성공, 연결 실패) 를 언제든지 확인할 수 있습니다.
5. 왕복 시간 (RTT) 과 같이 사용자 환경에 영향을 미치는 InSession 지연 시간을 확인하여 연결 상태 및 패킷 손실을 파악하여 네트워크 상태를 모니터링할 수 있습니다.
6. 호스트 성능 및 리소스 사용률을 확인하여 잠재적인 성능 문제를 식별하고 해결합니다.

WorkSpaces 사용 CloudWatch 지표 모니터링

WorkSpaces CloudWatch Amazon이 통합되어 있으므로 성능 지표를 수집하고 분석할 수 있습니다. CloudWatch 콘솔, CloudWatch 명령줄 인터페이스를 사용하거나 CloudWatch API를 사용하여 프로그래밍 방식으로 이러한 지표를 모니터링할 수 있습니다. CloudWatch 또한 지표에 대해 지정된 임계값에 도달하면 경보를 설정할 수 있습니다.

사용 CloudWatch 및 경보에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

필수 조건

CloudWatch 측정치를 가져오려면 해당 지역의 AMAZON 하위 집합에 있는 포트 443에서 액세스를 활성화하십시오. `us-east-1` 자세한 내용은 IP 주소 및 포트 요구 사항 WorkSpaces 단원을 참조하십시오.

목차

- 메트릭의 WorkSpaces 크기
- 모니터링 예

WorkSpaces 지표

AWS/WorkSpaces 네임스페이스에 포함된 지표는 다음과 같습니다.

지표	설명	차원	Statistics	단위
Available [1]	정상 상태를 WorkSpaces 반환한 개수	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
Unhealthy [1]	비정상 상태를 WorkSpaces 반환한 개수.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
ConnectionAttempt [2]	연결 시도 횟수	DirectoryId WorkspaceId RunningMode Protocol	Average, Sum, Maximum, Minimum, Data Samples	개수

지표	설명	차원	Statistics	단위
		ComputeType BundleId		
ConnectionSuccess [2]	성공적 연결 수	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
ConnectionFailure [2]	실패한 연결 수	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
SessionLaunchTime [2, 6]	WorkSpaces 세션을 시작하는 데 걸리는 시간.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	초(시간)

지표	설명	차원	Statistics	단위
InSessionLatency [2, 6]	WorkSpaces 클라이언트와 고객 간의 왕복 시간 WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	밀리초(시간)
SessionDisconnect [2, 6]	사용자가 시작한 연결, 실패한 연결을 포함하여 닫힌 연결의 수	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
UserConnected [3]	사용자가 연결되어 WorkSpaces 있는 번호입니다.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수

지표	설명	차원	Statistics	단위
Stopped	WorkSpaces 해당 번호는 중지되었습니다.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
Maintenance [4]	WorkSpaces 개수는 점검 중입니다.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average, Sum, Maximum, Minimum, Data Samples	개수
TrustedDeviceValidationAttempt [5, 6]	디바이스 인증 서명 유효성 검사를 시도한 횟수.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	개수
TrustedDeviceValidationSuccess [5, 6]	디바이스 인증 서명 유효성 검사에 성공한 횟수.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	개수
TrustedDeviceValidationFailure [5, 6]	디바이스 인증 서명 유효성 검사에 실패한 횟수.	DirectoryId	Average, Sum, Maximum, Minimum, Data Samples	개수

지표	설명	차원	Statistics	단위
TrustedDeviceCertificateDaysBeforeExpiration [6]	디렉터리와 연결된 루트 인증서가 만료되기까지 남은 일수.	CertificateId	Average, Sum, Maximum, Minimum, Data Samples	개수
CPUUsage	사용된 CPU 리소스의 백분율.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소값	백분율
MemoryUsage	컴퓨터 메모리 사용률.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소값	백분율
RootVolumeDiskUsage	사용된 루트 디스크 볼륨의 백분율.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소값	백분율

지표	설명	차원	Statistics	단위
UserVolumeDiskUsage	사용된 사용자 디스크 볼륨의 백분율.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소값	백분율
UDPPacketLossRate [7]	클라이언트와 게이트웨이 간에 삭제된 패킷의 비율입니다.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소, 데이터 샘플	백분율
UpTime	a를 마지막으로 재부팅한 이후 경과한 시간 WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	평균, 최대값, 최소값, 데이터 샘플	초

[1은] WorkSpaces 주기적으로 a에 상태 요청을 보냅니다 WorkSpace. WorkSpace A는 이러한 요청에 응답할 Available 때와 응답하지 않을 Unhealthy 때 표시됩니다. 이러한 지표는 WorkSpace 수준별로 세분화하여 사용할 수 있으며 조직 내 모든 WorkSpaces 사람을 대상으로 집계되기도 합니다.

[2]는 각각에 대한 연결에 대한 지표를 WorkSpaces 기록합니다. WorkSpace 이러한 지표는 사용자가 클라이언트를 통해 성공적으로 인증하고 WorkSpaces 클라이언트가 세션을 시작한 후에 생성됩니다. 지표는 WorkSpace 수준별로 세분화하여 사용할 수 있으며 디렉토리의 모든 항목에 대해 집계됩니다. WorkSpaces

[3]은 WorkSpaces 주기적으로 a에 연결 상태 요청을 보냅니다. WorkSpace 사용자가 세션을 능동적으로 사용하고 있을 경우 연결된 상태로 보고됩니다. 이 지표는 세부 WorkSpace 수준별로 사용할 수 있으며 조직 WorkSpaces 내 모든 사용자에 대해 집계되기도 합니다.

[4] 이 WorkSpaces 지표는 실행 모드로 구성된 항목에 적용됩니다. AutoStop 에 대해 유지 관리를 활성화한 WorkSpaces 경우 이 지표는 현재 유지 관리 WorkSpaces 중인 항목의 수를 캡처합니다. 이 지표는 유지 관리 시작 시기와 제거 시기를 설명하는 세부 WorkSpace 수준별로 제공됩니다. WorkSpace

[5] 디렉터리에 신뢰할 수 있는 디바이스 기능이 활성화된 경우 WorkSpaces Amazon은 인증서 기반 인증을 사용하여 디바이스의 신뢰 여부를 판단합니다. 사용자가 WorkSpaces 액세스를 시도하면 이러한 지표가 생성되어 신뢰할 수 있는 장치 인증의 성공 또는 실패를 나타냅니다. 이러한 지표는 디렉터리별 세분화 수준에서 사용할 수 있으며 Amazon Windows WorkSpaces 및 macOS 클라이언트 애플리케이션에서만 사용할 수 있습니다.

[6] 웹 액세스에서는 사용할 수 없습니다. WorkSpaces

[7] 이 지표는 평균 패킷 손실을 측정합니다.

- PCoIP: 클라이언트의 게이트웨이에서의 평균 패킷 손실을 측정합니다.
- WSP에서: 클라이언트에서 게이트웨이로의 평균 패킷 손실을 측정합니다.

메트릭의 WorkSpaces 크기

지표 데이터를 필터링하려면 다음 차원을 사용하세요.

차원	설명
`DirectoryId`	지표 데이터를 지정된 WorkSpaces 디렉터리의로 필터링합니다. 디렉터리 ID는 `d-XXXXXXXXXX` 형식입니다.
`WorkspaceId`	메트릭 데이터를 지정된 데이터로 필터링합니다 WorkSpace. WorkSpace ID의 형식은 다음과 같습니다`ws-XXXXXXXXXX` .

차원	설명
CertificateId	지표 데이터를 디렉터리와 연결된 지정된 루트 인증서로 필터링합니다. 인증서 ID는 wsc-XXXXXXXXX 형식입니다.
RunningMode	실행 WorkSpaces 모드별로 메트릭 데이터를 필터링합니다. 실행 모드의 형태는 AutoStop 또는 입니다 AlwaysOn.
BundleId	WorkSpaces 프로토콜별로 메트릭 데이터를 필터링합니다. 번들 형식은 다음과 같습니다wsb-XXXXXXXXXX .
ComputeType	메트릭 데이터를 컴퓨팅 WorkSpaces 유형별로 필터링합니다.
Protocol	프로토콜 WorkSpaces 유형별로 메트릭 데이터를 필터링합니다.

모니터링 예

다음 예제는 를 사용하여 AWS CLI CloudWatch 경보에 응답하고 WorkSpaces 디렉터리에서 연결 장애가 발생한 디렉토리를 확인하는 방법을 보여줍니다.

경보에 응답하려면 CloudWatch

1. describe-alarms 명령을 사용하여 경보가 적용되는 디렉터리를 결정합니다.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
```

```
      ],
      ...
    }
  ]
}
```

2. describe-workspaces 명령을 사용하여 지정된 WorkSpaces 디렉터리의 목록을 가져옵니다.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. 명령을 사용하여 디렉터리에 있는 각 CloudWatch WorkSpace 항목에 대한 메트릭을 가져옵니다. get-metric-statistics

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
```

```
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Amazon WorkSpaces 사용 현황 모니터링 EventBridge

WorkSpaces Amazon의 이벤트를 보고, 검색하고, 다운로드하고, 보관하고, 분석하고, 로그인에 성공하면 응답할 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 이벤트 유형의 액세스 기준에 맞는 파일 또는 WorkSpaces 데이터에만 사용자가 액세스하도록 `WorkSpaces Access` 허용하십시오.
- 를 사용하여 로그인 데이터를 분석하고 자동화된 작업을 수행합니다 AWS Lambda.
- 정책 제어를 사용하여 권한이 없는 IP 주소에서 파일 및 애플리케이션에 대한 액세스를 차단합니다.
- 연결에 사용된 WorkSpaces 클라이언트 버전을 확인하세요 WorkSpaces.

WorkSpaces Amazon은 최선의 노력을 다해 이러한 이벤트를 내보냅니다. 이벤트는 거의 EventBridge 실시간으로 전송됩니다. 를 사용하면 이벤트에 대한 응답으로 EventBridge 프로그래밍 작업을 트리거하는 규칙을 만들 수 있습니다. 예를 들어 SNS 주제를 호출하여 이메일 알림을 보내거나 Lambda 함수를 호출하여 조치를 취하는 규칙을 구성할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.

WorkSpaces 액세스 이벤트

WorkSpaces 클라이언트 애플리케이션은 사용자가 a에 성공적으로 로그인하면 `WorkSpaces Access` 이벤트를 WorkSpace 전송합니다. 모든 WorkSpaces 클라이언트가 이러한 이벤트를 전송합니다.

WorkSpaces 스트리밍 프로토콜 (WSP) 을 WorkSpaces 사용하기 위해 발생하는 이벤트에는 WorkSpaces 클라이언트 애플리케이션 버전 4.0.1 이상이 필요합니다.

이벤트는 JSON 객체로 표현됩니다. 다음은 `WorkSpaces Access` 이벤트의 예제 데이터입니다.

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

이벤트 고유 필드

`clientIpAddress`

클라이언트 애플리케이션의 WAN IP 주소입니다. PCoIP 제로 클라이언트의 경우에는 이것이 Teradici auth 클라이언트의 IP 주소가 됩니다.

`actionType`

이 값은 항상 `successfulLogin`입니다.

`workspacesClientProductName`

다음 값은 대소문자를 구분합니다.

- `WorkSpaces Desktop client` - Windows, macOS 및 Linux 클라이언트
- `Amazon WorkSpaces Mobile client` - iOS 클라이언트
- `WorkSpaces Mobile Client` - Android 클라이언트
- `WorkSpaces Chrome Client` - Chromebook 클라이언트
- `WorkSpacesWebClient` - Web Access 클라이언트
- `AmazonWorkSpacesThinClient`— Amazon WorkSpaces 씬 클라이언트 디바이스
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` - 제로 클라이언트

`loginTime`

사용자가 에 로그인한 시간 WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

의 디렉토리 식별자입니다 WorkSpace. 디렉터리 식별자 앞에 `domain/`을 추가해야 합니다. 예를 들어 `"domain/d-123456789"`입니다.

`clientVersion`

연결하는 데 사용된 클라이언트 버전 WorkSpaces.

`workspaceId`

WorkSpace의 식별자입니다.

WorkSpaces 이벤트를 처리하는 규칙 만들기

다음 절차를 사용하여 WorkSpaces 이벤트를 처리하는 규칙을 만드십시오.

전제 조건

이메일 알림을 받으려면 Amazon Simple Notification Service 주제를 생성합니다.

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. 주제 생성을 선택합니다.
4. 유형에서 표준을 선택합니다.
5. Name(이름)에 주제의 이름을 입력합니다.
6. 주제 생성을 선택합니다.
7. 구독 생성을 선택합니다.
8. 프로토콜에서 이메일을 선택합니다.
9. Endpoint(엔드포인트)에 알림을 받는 데 사용할 이메일 주소를 입력합니다.
10. 구독 생성을 선택합니다.
11. AWS Notification - Subscription Confirmation이라는 제목의 이메일 메시지를 받게 됩니다. 지시에 따라 구독을 확인합니다.

WorkSpaces 이벤트를 처리하는 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. Create rule을 선택합니다.
3. Name(이름)에 규칙의 이름을 입력합니다.
4. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
5. 다음을 선택합니다.
6. 이벤트 패턴(Event pattern)에서 다음을 수행하십시오:
   a. 이벤트 소스(Event source)에서 AWS 서비스를 선택합니다.
   b. AWS 서비스에는 WorkSpaces를 선택합니다.
   c. 이벤트 유형으로는 WorkSpaces 액세스를 선택합니다.

d. 기본적으로 모든 이벤트에 대해 알림을 보냅니다. 원하는 경우 특정 클라이언트 또는 WorkSpaces에 대한 이벤트를 필터링하는 이벤트 패턴을 만들 수 있습니다.

7. 다음을 선택합니다.
8. 다음과 같이 대상을 지정합니다.

   a. 대상 타입(Target types)에서 AWS 서비스를 선택합니다.
   b. 대상 선택(Select a target)에서 SNS 주제(SNS topic)를 선택합니다.
   c. 주제에서 알림에 대해 생성한 SNS 주제를 선택합니다.

9. 다음을 선택합니다.
10. (선택 사항) 규칙에 태그를 추가합니다.
11. 다음을 선택합니다.
12. 규칙 생성을 선택합니다.

스마트 카드 사용자의 AWS 로그인 이벤트에 대한 이해

AWS CloudTrail은 스마트 카드 사용자의 로그인 성공 및 실패 이벤트를 기록합니다. 여기에는 사용자에게 특정 보안 인증 정보 문제나 인증을 해결하라는 메시지가 표시될 때마다 캡처되는 로그인 이벤트와 해당 특정 보안 인증 정보 확인 요청의 상태가 포함됩니다. 사용자는 필요한 보안 인증 정보 문제를 모두 완료한 후에만 로그인되며, 이 경우 `UserAuthentication` 이벤트가 기록됩니다.

다음 표에는 각 로그인 CloudTrail 이벤트 이름과 용도가 나와 있습니다.

이벤트 이름	이벤트 용도
`CredentialChallenge`	사용자가 특정 보안 인증 정보 문제를 해결하도록 AWS 로그인을 요청했음을 알리고 필요한 `CredentialType` (예: SMARTCARD)을 지정합니다.
`CredentialVerification`	사용자가 특정 `CredentialChallenge` 요청을 해결하려고 시도했음을 알리고 해당 보안 인증 정보의 성공 또는 실패 여부를 지정합니다.
`UserAuthentication`	사용자에게 요청한 모든 인증 요구 사항이 성공적으로 완료되었으며 사용자가 성공적으로 로그인했음을 알립니다. 사용자가 필수 보안 인증 정보 문제를 성공적으로 완료하지 못하면 `UserAuthentication` 이벤트가 기록되지 않습니다.

다음 표에는 특정 로그인 CloudTrail 이벤트에 포함된 유용한 추가 이벤트 데이터 필드가 나와 있습니다.

이벤트 이름	이벤트 용도	로그인 이벤트 적용 가능성	예제 값
`AuthWorkflowID`	전체 로그인 시퀀스에서 발생한 모든 이벤트의 상관 관계를 분석합니다. 각 사용자 로그인에 대해 AWS 로그인을 통해 여러 개의 이벤트가 생성될 수 있습니다.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	사용자가 특정 `CredentialChallenge` 요청을 해결하려고 시도했음을 알리고 해당 보안 인증 정보의 성공 또는 실패 여부를 지정합니다.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType": "SMARTCARD" (오늘 가능한 값: SMARTCARD)
`LoginTo`	사용자에게 요청한 모든 인증 요구 사항이 성공적으로 완료되었으며 사용자가 성공적으로 로그인했음을 알립니다. 사용자가 필수 보안 인증 정보 문제를 성공적으로 완료하지 못하면 `UserAuthentication` 이벤트가 기록되지 않습니다.	`UserAuthentication`	"LoginTo": "https://skylight.local“

AWS 로그인 시나리오의 예시 이벤트

다음 예는 각기 다른 로그인 시나리오에 대한 CloudTrail 이벤트의 예상 시퀀스를 보여줍니다.

목차

- 스마트 카드로 인증할 때 로그인에 성공
- 스마트 카드로만 인증할 때 로그인에 실패

스마트 카드로 인증할 때 로그인에 성공

다음 이벤트 시퀀스는 성공적인 스마트 카드 로그인의 예를 보여줍니다.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
```

```
}
```

Successful CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

Successful UserAuthentication


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```


스마트 카드로만 인증할 때 로그인에 실패

다음 이벤트 시퀀스는 실패한 스마트 카드 로그인의 예를 보여줍니다.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


Failed CredentialVerification


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

아마존의 비즈니스 연속성 WorkSpaces

WorkSpaces Amazon은 AWS 지역 및 가용 영역으로 구성된 AWS 글로벌 인프라를 기반으로 합니다. 이러한 리전과 가용 영역은 물리적 격리와 데이터 중복성 측면에서 탄력성을 제공합니다. 자세한 설명은 Amazon WorkSpaces의 복원력 섹션을 참조하세요.

Amazon은 WorkSpaces 또한 도메인 이름 시스템 (DNS) 라우팅 정책과 함께 작동하여 기본 리디렉션을 사용할 수 WorkSpaces 없는 WorkSpaces 경우 WorkSpaces 사용자를 대체 사이트로 리디렉션하는 기능인 지역 간 리디렉션을 제공합니다. 예를 들어 DNS 장애 조치 라우팅 정책을 사용하면 사용자가 기본 WorkSpaces 지역의 사용자에게 액세스할 수 없을 때 지정된 장애 조치 지역에 사용자를 연결할 수 있습니다. WorkSpaces

리전 간 리디렉션을 사용하여 리전의 복원력과 고가용성을 달성할 수 있습니다. 또한 트래픽 분산 또는 유지 관리 WorkSpaces 기간 동안의 대체 서비스 제공과 같은 다른 용도로도 사용할 수 있습니다. DNS 구성에 Amazon Route 53을 사용하는 경우 Amazon CloudWatch 경보를 모니터링하는 상태 확인을 활용할 수 있습니다.

Amazon WorkSpaces Multi-Region Resilience는 보조 WorkSpace 지역에 자동화된 중복 가상 데스크톱 인프라를 제공하며, 정전으로 인해 기본 지역에 연결할 수 없는 경우 사용자를 보조 지역으로 리디렉션하는 프로세스를 간소화합니다.

WorkSpaces 지역 간 리디렉션이 포함된 멀티 리전 레질리언스를 사용하여 보조 리전에 중복 가상 데스크톱 인프라를 배포하고 중단이 발생하는 이벤트에 대비하여 리전 간 장애 조치 전략을 설계할 수 있습니다. WorkSpace 또한 이 솔루션을 트래픽 분산 또는 유지 관리 기간 중 대안 제공과 같은 다른 용도로도 사용할 수 있습니다. WorkSpaces DNS 구성에 Route 53을 사용하는 경우 CloudWatch 경보를 모니터링하는 상태 점검을 활용할 수 있습니다.

내용

Amazon을 위한 지역 간 리디렉션 WorkSpaces

WorkSpacesAmazon의 지역 간 리디렉션 기능을 사용하면 FQDN (정규화된 도메인 이름) 을 등록 코드로 사용할 수 있습니다. WorkSpaces 지역 간 리디렉션은 DNS (Domain Name System) 라우팅 정책과 함께 작동하여 주 서버를 사용할 수 없는 경우 WorkSpaces 사용자를 다른 대안으로 WorkSpaces 리디렉션합니다. WorkSpaces 예를 들어 DNS 장애 조치 라우팅 정책을 사용하면 사용자가 기본

WorkSpaces 지역의 사용자에게 액세스할 수 없을 때 지정된 장애 조치 AWS 지역에 사용자를 연결할 수 있습니다. WorkSpaces

DNS 장애 조치 라우팅 정책과 함께 리전 간 리디렉션을 사용하여 리전의 복원력과 고가용성을 달성할 수 있습니다. 또한 이 기능을 트래픽 분산 또는 유지 관리 WorkSpaces 기간 동안의 대체 제공과 같은 다른 용도로도 사용할 수 있습니다. DNS 구성에 Amazon Route 53을 사용하는 경우 Amazon CloudWatch 경보를 모니터링하는 상태 확인을 활용할 수 있습니다.

이 기능을 사용하려면 2개 (또는 그 이상) AWS 지역의 사용자를 WorkSpaces 위해 설정해야 합니다. 연결 별칭이라는 FQDN 기반 특수 등록 코드도 만들어야 합니다. 이러한 연결 별칭은 사용자의 지역별 등록 코드를 대체합니다. WorkSpaces (리전별 등록 코드는 계속 유효하지만, 리전 간 리디렉션이 작동하려면 사용자가 FQDN을 등록 코드로 대신 사용해야 합니다.)

연결 별칭을 만들려면 FQDN인 연결 문자열(예: `www.example.com` 또는 `desktop.example.com`)을 지정합니다. 리전 간 리디렉션에 이 도메인을 사용하려면 도메인 등록 대행자에 도메인을 등록하고 도메인에 대한 DNS 서비스를 구성해야 합니다.

연결 별칭을 만든 후에는 이를 다른 지역의 WorkSpaces 디렉터리와 연결하여 연결 쌍을 만듭니다. 각 연결 쌍에는 기본 리전과 하나 이상의 장애 조치 리전이 있습니다. 기본 지역에서 중단이 발생하는 경우 DNS 장애 조치 라우팅 정책은 WorkSpaces 사용자를 장애 조치 지역에서 설정한 WorkSpaces 것으로 리디렉션합니다.

기본 리전과 장애 조치 리전을 지정하려면 DNS 장애 조치 라우팅 정책을 구성할 때 리전 우선순위(기본 또는 보조)를 정의하세요.

내용

- 디렉터리에서 연결 별칭 연결 해제
- 연결 별칭 공유 해제
- 연결 별칭 삭제
- 연결 별칭을 연결 및 연결 해제하는 IAM 권한
- 리전 간 리디렉션 사용을 중지하는 경우 보안 고려 사항

사전 조건

- 연결 별칭에서 FQDN으로 사용할 도메인을 소유하고 등록해야 합니다. 다른 도메인 등록 대행자를 아직 사용하고 있지 않은 경우 Amazon Route 53를 사용하여 도메인을 등록할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 Registering domain names using Amazon Route 53를 참조하세요.

  > **Important**
  >
  > Amazon과 함께 사용하는 도메인 이름을 사용하려면 필요한 모든 권한이 있어야 WorkSpaces 합니다. 도메인 이름이 제3자의 법적 권리를 위반하거나 침해하거나 관련 법률을 위반하지 않는다는 데 동의하는 것으로 간주합니다.

  도메인 이름의 총 길이는 255자를 초과할 수 없습니다. 도메인 이름에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 DNS 도메인 이름 형식을 참조하세요.

  리전 간 리디렉션은 퍼블릭 도메인 이름과 프라이빗 DNS 영역의 도메인 이름 모두에서 작동합니다. 프라이빗 DNS 영역을 사용하는 경우, 해당 영역을 포함하는 가상 사설 클라우드 (VPC) 에 대한 VPN (가상 사설망) 연결을 제공해야 합니다. WorkSpaces WorkSpaces 사용자가 퍼블릭 인터넷에서 프라이빗 FQDN을 사용하려고 하면 WorkSpaces 클라이언트 애플리케이션이 다음 오류 메시지를 반환합니다.

  ```
  "We're unable to register the WorkSpace because of a DNS server issue. Contact your administrator for help."
  ```

- DNS 서비스를 설정하고 필요한 DNS 라우팅 정책을 구성해야 합니다. 지역 간 리디렉션은 DNS 라우팅 정책과 함께 작동하여 필요에 따라 사용자를 리디렉션합니다. WorkSpaces
- 지역 간 리디렉션을 설정하려는 각 기본 및 장애 조치 지역에서 사용자를 위한 리디렉션을 생성하십시오. WorkSpaces 각 지역의 각 WorkSpaces 디렉터리에서 동일한 사용자 이름을 사용해야 합니다. Active Directory 사용자 데이터를 동기화된 상태로 유지하려면 AD Connector를 사용하여

WorkSpaces 사용자에 대해 설정한 각 지역의 동일한 Active Directory를 가리키는 것이 좋습니다. 만들기에 대한 자세한 WorkSpaces 내용은 실행을 참조하십시오 WorkSpaces.

> **Important**
>
> 다중 지역 복제를 위해 AWS 관리형 Microsoft AD 디렉터리를 구성하는 경우 기본 지역의 디렉터리만 WorkSpaces Amazon에서 사용하도록 등록할 수 있습니다. Amazon에서 사용하기 위해 복제된 리전에 디렉터리를 등록하려는 WorkSpaces 시도는 실패합니다. AWS관리형 Microsoft AD를 사용한 다중 지역 복제는 복제된 지역 WorkSpaces 내에서 Amazon에서 사용할 수 없습니다.

지역 간 리디렉션 설정을 완료했으면 WorkSpaces 사용자가 기본 지역의 지역 기반 등록 코드 (예:) 대신 FQDN 기반 등록 코드를 사용하고 있는지 확인해야 합니다. `WSpdx+ABC12D` 이렇게 하려면 5 단계: 사용자에게 연결 문자열 전송 WorkSpaces 의 절차를 사용하여 FQDN 연결 문자열이 포함된 이메일을 보내야 합니다.

> **Note**
>
> Active Directory에서 사용자를 생성하는 대신 WorkSpaces 콘솔에서 사용자를 생성하는 경우 새 사용자를 시작할 때마다 지역 기반 등록 코드가 포함된 초대 이메일이 사용자에게 WorkSpaces 자동으로 전송됩니다. WorkSpace 즉, 장애 조치 지역의 사용자를 설정하면 WorkSpaces 사용자도 이러한 장애 조치에 대한 이메일을 자동으로 받게 됩니다. WorkSpaces 리전 기반 등록 코드가 포함된 이메일은 무시하도록 사용자에게 지시해야 합니다.

제한 사항

- 지역 간 리디렉션은 기본 지역으로의 연결에 장애가 발생했는지 여부를 자동으로 확인한 다음 다른 지역으로 WorkSpaces 페일오버하지 않습니다. 즉, 자동 장애 조치가 발생하지 않습니다.

  자동 장애 조치 시나리오를 구현하려면 리전 간 리디렉션과 함께 다른 메커니즘을 사용해야 합니다. 예를 들어, 기본 지역의 CloudWatch 경보를 모니터링하는 Route 53 상태 확인과 함께 Amazon Route 53 장애 조치 DNS 라우팅 정책을 사용할 수 있습니다. 기본 지역의 CloudWatch 경보가 트리거되면 DNS 장애 조치 라우팅 정책이 WorkSpaces 사용자를 장애 조치 지역에서 설정한 WorkSpaces 것으로 리디렉션합니다.

- 지역 간 리디렉션을 사용하는 경우 사용자 데이터는 서로 다른 지역 간에 유지되지 않습니다. WorkSpaces 사용자가 다른 지역에서 파일에 액세스할 수 있도록 하려면 기본 및 장애 조치 지역에서 Amazon을 지원하는 경우 WorkDocs WorkSpaces 사용자용 WorkDocs Amazon을 설정하는 것이 좋습니다. Amazon에 대한 자세한 내용은 Amazon WorkDocs WorkDocs 관리 안내서의 Amazon WorkDocs Drive를 참조하십시오. WorkSpace 사용자가 Amazon을 사용하도록 설정하는 방법에 WorkDocs 대한 자세한 내용은 WorkSpaces에 디렉터리 등록 및 을 참조하십시오AWS Managed Microsoft AD에 Amazon WorkDocs 활성화. WorkSpaces 사용자가 Amazon을 설정하는 방법에 대한 자세한 내용은 Amazon WorkDocs 사용 설명서의 통합 WorkSpaces 대상을 참조하십시오. WorkSpaces WorkDocs
- 지역 간 리디렉션은 Linux, macOS 및 Windows 클라이언트 애플리케이션의 버전 3.0.9 이상에서만 지원됩니다. WorkSpaces Web Access에서도 리전 간 리디렉션을 사용할 수 있습니다.
- 지역 간 리디렉션은 AWS GovCloud (US) Region s 및 중국 (닝샤) AWS지역을 제외하고 WorkSpaces Amazon을 사용할 수 있는 모든 지역에서 사용할 수 있습니다.

1단계: 연결 별칭 생성

동일한 AWS 계정을 사용하여 리전 간 리디렉션을 설정할 각 기본 리전과 장애 조치 리전에서 연결 별칭을 만듭니다.

연결 별칭을 생성하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 콘솔을 엽니다. WorkSpaces
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션에서 연결 별칭 생성을 선택합니다.
5. 연결 문자열에 FQDN을 입력합니다(예: `www.example.com` 또는 `desktop.example.com`). 연결 문자열은 최대 255자입니다. 여기에는 문자(A~Z 및 a~z), 숫자(0~9) 및 .- 기호만 사용할 수 있습니다.

   > **Important**
   >
   > 연결 문자열을 만들고 나면 연결 문자열이 항상 AWS 계정과 연결됩니다. 원래 계정에서 연결 문자열의 모든 인스턴스를 삭제한 경우에도 다른 계정으로 같은 연결 문자열을 다시 만들 수 없습니다. 연결 문자열은 전역적으로 계정에 예약되어 있습니다.

6. (선택 사항) 태그에서 연결 별칭과 연결할 태그를 지정합니다.

7. 연결 별칭 생성을 선택합니다.
8. 이 단계를 반복하되Step 2, 에서는 해당 지역의 페일오버 지역을 선택해야 합니다. WorkSpaces 장애 조치 리전이 여러 개 있을 경우 각 장애 조치 리전에 대해 이 절차를 반복합니다. 동일한 AWS 계정을 사용하여 각 장애 조치 리전에서 연결 별칭을 만들어야 합니다.

(선택 사항) 2단계: 다른 계정과 연결 별칭 공유

연결 별칭을 동일한 AWS 리전의 다른 AWS 계정과 공유할 수 있습니다. 연결 별칭을 다른 계정과 공유하면 해당 계정에 해당 별칭을 동일한 리전에서 해당 계정이 소유한 디렉터리에만 연결하거나 연결을 해제할 수 있는 권한이 부여됩니다. 연결 별칭을 소유한 계정만 별칭을 삭제할 수 있습니다.

> **Note**
>
> 연결 별칭은 AWS 리전당 하나의 디렉터리에만 연결할 수 있습니다. 연결 별칭을 다른 AWS 계정과 공유하는 경우 한 계정(사용자 계정 또는 공유 계정)만 별칭을 해당 리전의 디렉터리와 연결할 수 있습니다.

다른 AWS 계정과 연결 별칭을 공유하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔의 오른쪽 상단 모서리에서 연결 별칭을 다른 AWS 계정과 공유하려는 AWS 리전을 선택합니다.
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열을 선택한 다음 작업, 연결 별칭 공유/공유 해제를 선택합니다.

   연결 별칭의 세부 정보 페이지에서 별칭을 공유할 수도 있습니다. 이렇게 하려면 공유 계정에서 연결 별칭 공유를 선택합니다.
5. 연결 별칭 공유/공유 해제 페이지의 계정과 공유에 이 AWS 리전에서 연결 별칭을 공유할 AWS 계정 ID를 입력합니다.
6. 공유를 선택합니다.

3단계: 연결 별칭을 각 리전의 디렉터리에 연결

둘 이상의 지역에 있는 WorkSpaces 디렉터리에 동일한 연결 별칭을 연결하면 디렉터리 간에 연결 쌍이 생성됩니다. 각 연결 쌍에는 기본 리전과 하나 이상의 장애 조치 리전이 있습니다.

예를 들어 주 지역이 미국 서부 (오레곤) 지역인 경우 미국 서부 (오레곤) 지역의 WorkSpaces 디렉터리를 미국 동부 (버지니아 북부) 지역의 WorkSpaces 디렉터리와 페어링할 수 있습니다. 기본 지역에서 중단이 발생하는 경우, 지역 간 리디렉션은 DNS 장애 조치 라우팅 정책 및 미국 서부 (오레곤) 지역에 적용한 상태 확인과 함께 작동하여 사용자를 미국 동부 (버지니아 북부) 지역에서 WorkSpaces 설정한 것으로 리디렉션합니다. 리전 간 리디렉션 경험에 대한 자세한 내용은 리전 간 리디렉션 중에 발생하는 상황 섹션을 참조하세요.

> **Note**
>
> WorkSpaces 사용자가 페일오버 지역으로부터 상당한 거리 (예: 수천 마일 거리) 에 있는 경우 사용자의 WorkSpaces 경험이 평소보다 응답성이 떨어질 수 있습니다. 현재 위치에서 다양한 AWS 지역으로의 왕복 시간 (RTT) 을 확인하려면 Amazon Connection WorkSpaces 건강 점검을 사용하십시오.

연결 별칭을 디렉터리와 연결하는 방법

연결 별칭을 AWS 리전당 하나의 디렉터리에만 연결할 수 있습니다. 연결 별칭을 다른 AWS 계정과 공유한 경우 한 계정(사용자 계정 또는 공유 계정)만 별칭을 해당 리전의 디렉터리와 연결할 수 있습니다.

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열을 선택한 다음 작업, 연결/연결 해제를 선택합니다.

   연결 별칭의 세부 정보 페이지에서 디렉터리에 연결 별칭을 연결할 수도 있습니다. 이렇게 하려면 연결된 디렉터리에서 디렉터리 연결을 선택합니다.
5. 연결/연결 해제 페이지의 디렉터리에 연결에서 이 AWS 리전의 연결 별칭을 연결할 디렉터리를 선택합니다.

> **Note**
>
> 다중 지역 복제를 위해 AWS 관리형 Microsoft AD 디렉터리를 구성하는 경우 기본 지역의 디렉터리만 WorkSpaces Amazon에서 사용할 수 있습니다. Amazon에서 복제된 지역의 디렉터리를 사용하려는 WorkSpaces 시도는 실패합니다. AWS관리형 Microsoft AD를 사용한 다중 지역 복제는 복제된 지역 WorkSpaces 내에서 Amazon에서 사용할 수 없습니다.

6. Associate(연결)를 선택합니다.
7. 이 단계를 반복하되Step 2, 에서는 해당 장애 조치 지역을 선택해야 합니다. WorkSpaces 장애 조치 리전이 여러 개 있을 경우 각 장애 조치 리전에 대해 이 절차를 반복합니다. 각 장애 조치 리전의 디렉터리에 동일한 연결 별칭을 연결해야 합니다.

4단계: DNS 서비스 구성 및 DNS 라우팅 정책 설정

연결 별칭과 연결 별칭 연결 쌍을 만든 후에는 연결 문자열에 사용한 도메인의 DNS 서비스를 구성할 수 있습니다. 이 용도로는 모든 DNS 서비스 제공업체를 사용할 수 있습니다. 선호하는 DNS 서비스 제공업체가 아직 없는 경우 Amazon Route 53를 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 Amazon Route 53를 DNS 서비스로 구성을 참조하세요.

도메인에 대한 DNS 서비스를 구성한 후에는 리전 간 리디렉션에 사용할 DNS 라우팅 정책을 설정해야 합니다. 예를 들어 Amazon Route 53 상태 확인을 사용하여 사용자가 특정 지역의 해당 사용자에게 연결할 수 있는지 여부를 결정할 수 있습니다. WorkSpaces 사용자가 연결할 수 없는 경우 DNS 장애 조치 정책을 사용하여 한 리전에서 다른 리전으로 DNS 트래픽을 라우팅할 수 있습니다.

DNS 라우팅 정책을 선택하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 라우팅 정책 선택을 참조하세요. Amazon Route 53 상태 확인에 대한 자세한 내용은 Amazon Route 53 개발자 안내서에서 Amazon Route 53가 리소스의 상태를 확인하는 방법을 참조하세요.

DNS 라우팅 정책을 설정할 때는 연결 별칭과 기본 지역의 WorkSpaces 디렉터리 간의 연결을 위한 연결 식별자가 필요합니다. 또한 장애 조치 지역 또는 지역의 연결 별칭과 WorkSpaces 디렉터리 간의 연결을 위한 연결 식별자도 필요합니다.

> **Note**
>
> 연결 식별자는 연결 별칭 ID와 동일하지 않습니다. 연결 별칭 ID는 `wsca-`로 시작합니다.

연결 별칭 연결을 위해 연결 식별자를 찾는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열 텍스트(FQDN)를 선택하여 연결 별칭 세부 정보 페이지를 확인합니다.
5. 연결 별칭 세부 정보 페이지의 연결된 디렉터리에서 연결 식별자에 표시된 값을 기록해 둡니다.
6. 이 단계를 반복하되Step 2, 에서는 해당 지역의 페일오버 지역을 선택해야 합니다. WorkSpaces 장애 조치 리전이 여러 개 있을 경우 각 장애 조치 리전에 대해 이 절차를 반복하여 연결 식별자를 찾습니다.

예: Route 53를 사용하여 DNS 장애 조치 라우팅 정책을 설정하는 방법

다음 예에서는 도메인의 퍼블릭 호스팅 영역을 설정합니다. 하지만 퍼블릭 또는 프라이빗 호스팅 영역을 설정할 수 있습니다. 호스팅 영역 설정에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 호스팅 영역 작업을 참조하세요.

또한 이 예에서는 장애 조치 라우팅 정책을 사용합니다. 리전 간 리디렉션 전략에 다른 라우팅 정책 유형을 사용할 수 있습니다. DNS 라우팅 정책을 선택하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 라우팅 정책 선택을 참조하세요.

Route 53에서 장애 조치 라우팅 정책을 설정하는 경우 기본 리전에 상태 확인 필수입니다. Route 53에서 상태 확인을 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 Amazon Route 53 상태 확인 생성 및 DNS 장애 조치 구성 및 상태 확인의 생성, 업데이트 및 삭제를 참조하세요.

Route 53 상태 확인과 함께 Amazon CloudWatch CloudWatch 경보를 사용하려면 기본 지역의 리소스를 모니터링하는 경보도 설정해야 합니다. 에 대한 CloudWatch 자세한 내용은 Amazon이란 무엇입니까 CloudWatch? 를 참조하십시오. Amazon CloudWatch 사용 설명서에서 확인할 수 있습니다. Route 53이 상태 확인에서 CloudWatch 경보를 사용하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 Route 53이 경보를 모니터링하는 상태 확인의 상태를 확인하는 방법 및 CloudWatch CloudWatch 경보 모니터링을 참조하십시오.

Route 53에서 DNS 장애 조치 라우팅 정책을 설정하려면 먼저 도메인에 호스팅 영역을 생성해야 합니다.

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.

2. 탐색 창에서 호스팅 영역을 선택한 후 호스팅 영역 생성을 선택합니다.
3. 생성된 호스팅 영역 페이지에서 도메인 이름 아래에 도메인 이름(예: `example.com`)을 입력합니다.
4. 유형에서 퍼블릭 호스팅 영역을 선택합니다.
5. 호스팅 영역 생성(Create hosted zone)을 선택합니다.

그런 다음 기본 리전에 대한 상태 확인을 생성합니다.

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택한 다음 상태 확인 생성을 선택합니다.
3. 상태 확인 구성 페이지에서 상태 확인의 이름을 입력합니다.
4. 모니터링 대상에서 엔드포인트, 기타 상태 확인 상태 (계산된 상태 확인) 또는 경보 상태를 CloudWatch 선택합니다.
5. 이전 단계에서 선택한 항목에 따라 상태 확인을 구성하고 다음을 선택합니다.
6. 상태 확인 실패 시 알림 메시지 받음 페이지의 경보 생성에서 예 또는 아니요를 선택합니다.
7. 상태 확인 생성을 선택합니다.

상태 확인을 생성한 후 DNS 장애 조치 레코드를 생성할 수 있습니다.

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 호스팅 영역 페이지에서 도메인 이름을 선택합니다.
4. 도메인 이름의 세부 정보 페이지에서 레코드 생성을 선택합니다.
5. 라우팅 정책 선택 페이지에서 장애 조치를 선택하고 다음을 선택합니다.
6. 레코드 구성 페이지의 기본 구성에서 레코드 이름에 하위 도메인 이름을 입력합니다. 예를 들어, FQDN이 `desktop.example.com`인 경우 **`desktop`**을 입력합니다.

> **Note**
>
> 루트 도메인을 사용하려면 레코드 이름을 비워 두세요. 하지만 도메인을 본인에게만 사용하도록 설정한 경우가 아니라면 `desktop` 또는 `workspaces` 같은 하위 도메인을 사용하는 것이 좋습니다. WorkSpaces

7. 레코드 유형에서 TXT - 이메일 발신자 확인 및 애플리케이션별 값에 사용됨을 선택합니다.
8. TTL 초 설정을 기본값으로 둡니다.
9. ***your_domain_name***에 추가할 장애 조치 레코드에서 장애 조치 레코드 정의를 선택합니다.

이제 기본 및 장애 조치 리전에 대한 장애 조치 레코드를 설정해야 합니다.

예: 기본 리전의 장애 조치 레코드를 설정하는 방법

1. 장애 조치 레코드 정의 대화 상자의 값/트래픽 라우팅 대상에서 레코드 유형에 따라 IP 주소 또는 다른 값을 선택합니다.
2. 샘플 텍스트를 입력할 수 있는 상자가 열립니다. 기본 리전의 연결 별칭 연결을 위한 연결 식별자를 입력합니다.
3. 장애 조치 레코드 유형에서 기본을 선택합니다.
4. 상태 확인에서 기본 리전에 대해 생성한 상태 확인을 선택합니다.
5. 레코드 ID에 이 레코드를 식별할 수 있는 설명을 입력합니다.
6. 장애 조치 레코드 정의를 선택합니다. 새 장애 조치 레코드가 ***your_domain_name***에 추가할 장애 조치 레코드에 나타납니다.

예: 장애 조치 리전의 장애 조치 레코드를 설정하는 방법

1. ***your_domain_name***에 추가할 장애 조치 레코드에서 장애 조치 레코드 정의를 선택합니다.
2. 장애 조치 레코드 정의 대화 상자의 값/트래픽 라우팅 대상에서 레코드 유형에 따라 IP 주소 또는 다른 값을 선택합니다.
3. 샘플 텍스트를 입력할 수 있는 상자가 열립니다. 장애 조치 리전의 연결 별칭 연결을 위한 연결 식별자를 입력합니다.
4. 장애 조치 레코드 유형에서 보조를 선택합니다.
5. (선택 사항) 상태 확인에 장애 조치 리전에 대해 생성한 상태 확인을 입력합니다.
6. 레코드 ID에 이 레코드를 식별할 수 있는 설명을 입력합니다.
7. 장애 조치 레코드 정의를 선택합니다. 새 장애 조치 레코드가 ***your_domain_name***에 추가할 장애 조치 레코드에 나타납니다.

기본 지역에 설정한 상태 점검이 실패하는 경우 DNS 장애 조치 라우팅 정책이 WorkSpaces 사용자를 장애 조치 지역으로 리디렉션합니다. Route 53은 기본 지역의 상태 점검을 계속 모니터링하며, 기

본 지역의 상태 확인이 더 이상 실패하지 않으면 Route 53은 자동으로 WorkSpaces 사용자를 기본 WorkSpaces 지역의 해당 지역으로 다시 리디렉션합니다.

DNS 레코드 생성에 대한 자세한 내용은 Amazon Route 53 개발자 가이드에서 Amazon Route 53 콘솔을 사용하여 레코드 생성을 참조하세요. DNS TXT 레코드 구성에 대한 자세한 정보는 Amazon Route 53 개발자 안내서의 TXT 레코드 유형을 참조하세요.

5단계: 사용자에게 연결 문자열 전송 WorkSpaces

운영 중단 시 필요에 따라 사용자가 WorkSpaces 리디렉션되도록 하려면 사용자에게 연결 문자열 (FQDN) 을 보내야 합니다. 사용자에게 지역 기반 등록 코드 (예:`WSpdx+ABC12D`) 를 이미 발급한 경우 해당 WorkSpaces 코드는 유효합니다. 하지만 지역 간 리디렉션이 제대로 작동하려면 WorkSpaces 사용자가 클라이언트 애플리케이션에 등록할 때 연결 문자열을 등록 코드로 사용해야 합니다 WorkSpaces . WorkSpaces

> **Important**
>
> Active Directory에서 사용자를 생성하는 대신 WorkSpaces 콘솔에서 사용자를 생성하는 경우 새 사용자를 시작할 때마다 지역 기반 등록 코드 (예:`WSpdx+ABC12D`) 가 포함된 초대 이메일이 WorkSpaces 자동으로 사용자에게 전송됩니다. WorkSpace 지역 간 리디렉션을 이미 설정한 경우에도 새 리디렉션을 위해 자동으로 전송되는 초대 이메일에는 연결 문자열 대신 이 지역 기반 등록 코드가 WorkSpaces 포함됩니다.
>
> WorkSpaces 사용자가 지역 기반 등록 코드 대신 연결 문자열을 사용하도록 하려면 아래 절차를 사용하여 연결 문자열이 포함된 다른 이메일을 보내야 합니다.

사용자에게 연결 문자열을 보내려면 WorkSpaces

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 WorkSpaces를 선택합니다.
4. WorkSpaces페이지에서 검색 상자를 사용하여 초대를 보내려는 사용자를 검색한 다음 검색 WorkSpace 결과에서 해당하는 사용자를 선택합니다. 한 WorkSpace 번에 하나만 선택할 수 있습니다.
5. Actions(작업), Invite User(사용자 초대)를 선택합니다.
6. 사용자를 해당 사용자에게 초대 WorkSpaces 페이지에 사용자에게 보낼 이메일 템플릿이 표시됩니다.

7. (선택 사항) WorkSpaces 디렉터리와 연결된 연결 별칭이 두 개 이상 있는 경우 연결 별칭 문자열 목록에서 사용자가 사용할 연결 문자열을 선택합니다. 이메일 템플릿이 업데이트되어 선택한 문자열이 표시됩니다.
8. 이메일 템플릿 텍스트를 복사한 후 이메일 애플리케이션을 사용하여 사용자에게 보내는 이메일에 붙여 넣습니다. 이메일 애플리케이션에서 필요에 따라 텍스트를 수정할 수 있습니다. 초대 이메일이 준비되면 사용자에게 발송합니다.

지역 간 리디렉션 아키텍처 다이어그램

다음 다이어그램은 지역 간 리디렉션의 배포 프로세스를 설명합니다.

> **Note**
>
> 지역 간 리디렉션은 지역 간 장애 조치 및 폴백만 용이하게 합니다. 보조 WorkSpaces 지역에서의 생성 및 유지 관리를 용이하게 하지 않으며 지역 간 데이터 복제도 허용하지 않습니다. WorkSpaces 주 리전과 보조 리전 모두 별도로 관리해야 합니다.

지역 간 리디렉션 시작

중단이 발생하는 경우 DNS 레코드를 수동으로 업데이트하거나 장애 조치 지역을 결정하는 상태 점검에 기반한 자동 라우팅 정책을 사용할 수 있습니다. Amazon Route 53을 사용한 재해 복구 메커니즘 생성에 설명된 재해 복구 메커니즘을 따르는 것이 좋습니다.

리전 간 리디렉션 중에 발생하는 상황

지역 장애 조치 중에는 기본 지역의 WorkSpaces 사용자와 연결이 WorkSpaces 끊깁니다. 재연결을 시도하면 다음 오류 메시지가 표시됩니다.

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

그런 다음 사용자에게 다시 로그인하라는 메시지가 표시됩니다. FQDN을 등록 코드로 사용하는 경우, 사용자가 다시 로그인하면 DNS 장애 조치 라우팅 정책이 장애 조치 지역에서 설정한 사용자로 리디렉션합니다. WorkSpaces

> **Note**
>
> 경우에 따라 사용자가 다시 로그인할 때 다시 연결하지 못할 수도 있습니다. 이 동작이 발생하면 WorkSpaces 클라이언트 애플리케이션을 닫고 다시 시작한 다음 다시 로그인을 시도해야 합니다.

디렉터리에서 연결 별칭 연결 해제

디렉터리를 소유한 계정만 디렉터리에서 연결 별칭의 연결을 해제할 수 있습니다.

연결 별칭을 다른 계정과 공유하고 해당 계정이 자체적으로 소유한 디렉터리와 연결 별칭을 연결한 경우 해당 계정을 사용하여 디렉터리에서 연결 별칭의 연결을 해제해야 합니다.

디렉터리에서 연결 별칭 연결을 해제하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔의 오른쪽 상단 모서리에서 연결을 해제하려는 연결 별칭을 포함하는 AWS 리전을 선택합니다.
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열을 선택한 다음 작업, 연결/연결 해제를 선택합니다.

   연결 별칭 세부 정보 페이지에서도 연결 별칭의 연결을 해제할 수 있습니다. 이렇게 하려면 연결된 디렉터리에서 연결 해제를 선택합니다.
5. 연결/연결 해제 페이지에서 연결 해제를 선택합니다.
6. 연결 해제를 확인하라는 메시지가 표시된 대화 상자에서 연결 해제를 선택합니다.

연결 별칭 공유 해제

연결 별칭 소유자만 별칭 공유를 해제할 수 있습니다. 계정과 연결 별칭의 공유를 해제하면 해당 계정은 더 이상 연결 별칭을 디렉터리에 연결할 수 없습니다.

연결 별칭 공유를 해제하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔의 오른쪽 상단 모서리에서 공유를 해제하려는 연결 별칭을 포함하는 AWS 리전을 선택합니다.

3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열을 선택한 다음 작업, 연결 별칭 공유/공유 해제를 선택합니다.

   연결 별칭 세부 정보 페이지에서도 연결 별칭의 공유를 해제할 수 있습니다. 이렇게 하려면 공유 계정에서 공유 해제를 선택합니다.
5. 연결 별칭 공유/공유 해제제 페이지에서 공유 해제를 선택합니다.
6. 연결 별칭 공유 해제를 확인하라는 메시지가 표시된 대화 상자에서 공유 해제를 선택합니다.

연결 별칭 삭제

사용자 계정에서 연결 별칭을 소유하고 연결 별칭이 디렉터리와 연결되어 있지 않은 경우에만 연결 별칭을 삭제할 수 있습니다.

연결 별칭을 다른 계정과 공유하고 해당 계정이 자체적으로 소유한 디렉터리와 연결 별칭을 연결한 경우 해당 계정이 먼저 디렉터리에서 연결 별칭의 연결을 해제해야 연결 별칭을 삭제할 수 있습니다.

> **Important**
>
> 연결 문자열을 만들고 나면 연결 문자열이 항상 AWS 계정과 연결됩니다. 원래 계정에서 연결 문자열의 모든 인스턴스를 삭제한 경우에도 다른 계정으로 같은 연결 문자열을 다시 만들 수 없습니다. 연결 문자열은 전역적으로 계정에 예약되어 있습니다.

> **Warning**
>
> 더 이상 FQDN을 WorkSpaces 사용자 등록 코드로 사용하지 않을 경우 잠재적인 보안 문제를 방지하기 위해 특정 예방 조치를 취해야 합니다. 자세한 설명은 리전 간 리디렉션 사용을 중지하는 경우 보안 고려 사항 섹션을 참조하세요.

연결 별칭을 삭제하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔의 오른쪽 상단 모서리에서 삭제하려는 연결 별칭을 포함하는 AWS 리전을 선택합니다.
3. 탐색 창에서 Account Settings(계정 설정)를 선택합니다.
4. 리전 간 리디렉션 연결에서 연결 문자열을 선택한 다음 삭제를 선택합니다.

연결 별칭 세부 정보 페이지에서도 연결 별칭을 삭제할 수 있습니다. 페이지 오른쪽 상단 모서리에서 삭제를 선택하면 됩니다.

> **Note**
>
> 삭제 버튼이 비활성화된 경우 자신이 별칭의 소유자인지 확인하고 별칭이 디렉터리와 연결되어 있지 않은지 확인하세요.

5. 삭제를 확인하라는 대화 상자에서 삭제를 선택합니다.

연결 별칭을 연결 및 연결 해제하는 IAM 권한

IAM 사용자를 사용하여 연결 별칭을 연결하거나 연결 해제하는 경우 사용자에게 `workspaces:AssociateConnectionAlias` 및 `workspaces:DisassociateConnectionAlias`에 대한 권한이 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

> **Important**
>
> 연결 별칭을 소유하지 않는 계정의 연결 별칭을 연결하거나 연결 해제하기 위한 IAM 정책을 생성하는 경우 ARN에서 계정 ID를 지정할 수 없습니다. 대신 다음 예시 정책에 표시된 대로 계정 ID에 * 기호를 사용해야 합니다.
>
> ```
> {
> ```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

해당 계정이 연결 또는 연결 해제할 연결 별칭을 소유한 경우에만 ARN에서 계정 ID를 지정할 수 있습니다.

IAM 작업에 관한 자세한 내용은 WorkSpaces의 Identity and Access Management 단원을 참조하세요.

리전 간 리디렉션 사용을 중지하는 경우 보안 고려 사항

더 이상 FQDN을 WorkSpaces 사용자 등록 코드로 사용하지 않을 경우 다음과 같은 예방 조치를 취하여 잠재적인 보안 문제를 방지해야 합니다.

- WorkSpaces 사용자에게 WorkSpaces 디렉터리의 지역별 등록 코드 (예:`WSpdx+ABC12D`) 를 발급하고 FQDN을 등록 코드로 사용하지 않도록 지시해야 합니다.
- 이 도메인을 아직 소유하고 있는 경우 피싱 공격에 악용되지 않도록 DNS TXT 레코드를 업데이트하여 이 도메인을 제거해야 합니다. DNS TXT 레코드에서 이 도메인을 제거하고 WorkSpaces 사용자가 FQDN을 등록 코드로 사용하려고 시도하면 연결 시도는 문제 없이 실패합니다.
- 이 도메인을 더 이상 소유하지 않는 경우 WorkSpaces 사용자는 해당 지역별 등록 코드를 사용해야 합니다. FQDN을 등록 코드로 계속 사용하려고 하면 연결 시도가 악성 사이트로 리디렉션될 수 있습니다.

Amazon을 위한 다중 지역 레질리언스 WorkSpaces

Amazon WorkSpaces Multi-Region Resilience (MRR) 를 사용하면 운영 중단으로 인해 기본 WorkSpaces 지역에 접속할 수 없는 경우 사용자가 예비 리전에 로그인할 때 등록 코드를 전환할 필

요 없이 사용자를 보조 지역으로 리디렉션할 수 있습니다. WorkSpaces 스탠바이 WorkSpaces 모드는 Amazon WorkSpaces 멀티 리전 레질리언스의 기능으로, 스탠바이 배포 생성 및 관리를 간소화합니다. 보조 리전에 사용자 디렉터리를 설정한 후, 기본 리전에서 예비 리전을 생성하려는 디렉터리를 선택합니다. WorkSpace WorkSpace 시스템은 기본 WorkSpace 번들 이미지를 보조 지역에 자동으로 미러링합니다. 그러면 보조 지역에 새 예비 WorkSpace 복제본을 자동으로 프로비저닝합니다.

Amazon WorkSpaces 다중 리전 복원력은 DNS 상태 점검 및 장애 조치 기능을 활용하는 교차 리전 리디렉션을 기반으로 구축되었습니다. 이를 통해 FQDN (정규화된 도메인 이름) 을 등록 코드로 사용할 수 있습니다. WorkSpaces 사용자가 로그인하면 FQDN의 DNS (도메인 이름 시스템) 정책에 따라 지원되는 WorkSpaces 지역 간에 사용자를 리디렉션할 수 있습니다. WorkSpaces Amazon Route 53을 사용하는 경우 리전 간 리디렉션 전략을 고안할 때 Amazon CloudWatch 경보를 모니터링하는 상태 확인을 사용하는 것이 좋습니다. WorkSpaces 자세한 내용은 Amazon Route 53 개발자 안내서의 Amazon Route 53 상태 확인 생성 및 DNS 장애 조치 구성을 참조하십시오.

데이터 복제는 데이터를 기본 리전에서 보조 리전으로 단방향으로 WorkSpaces 복제하는 스탠바이 리전의 추가 기능입니다. 데이터 복제를 활성화한 후에는 12시간마다 시스템 및 사용자 볼륨의 EBS 스냅샷이 생성됩니다. 다중 지역 복원력은 새 스냅샷이 있는지 정기적으로 확인합니다. 스냅샷이 발견되면 보조 지역으로의 복사가 시작됩니다. 사본이 보조 지역에 도착하면 보조 지역을 업데이트하는 데 사용됩니다. WorkSpace

내용

필수 조건

- 스탠바이 리전을 생성하기 전에 기본 리전의 WorkSpaces 사용자용으로 생성해야 WorkSpaces 합니다. 생성에 대한 자세한 내용은 WorkSpaces 을 참조하십시오WorkSpaces를 사용하여 가상 데스크톱 시작.

- 대기 모드에서 WorkSpaces 데이터 복제를 활성화하려면 자체 관리되는 Active Directory 또는 대기 지역에 복제하도록 구성된 AWS 관리형 Microsoft AD가 있어야 합니다. 자세한 내용은 AWS 관리형 Microsoft AD 디렉터리 만들기 및 복제된 지역 추가를 참조하십시오.
- 기본 드라이버에서 ENA, NVMe, PV 드라이버와 같은 네트워킹 종속성 드라이버를 업데이트해야 합니다. WorkSpaces 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 Windows 인스턴스용 ENA (엘라스틱 네트워크 어댑터) 드라이버 설치 또는 업그레이드 및 Windows 인스턴스의 PV 드라이버 업그레이드를 참조하십시오.AWS NVMe 드라이버
- EC2Config, EC2Launch 및 EC2Launch V2 에이전트를 정기적으로 최신 버전으로 업데이트하십시오. 최소 6개월에 한 번 이상 이 작업을 수행해야 합니다. 자세한 내용은 EC2Config 및 EC2Launch 업데이트를 참조하십시오.
- 데이터 복제가 제대로 이루어지도록 하려면 기본 및 보조 지역의 액티브 디렉터리가 FQDN, OU 및 사용자 SID에 대해 동기화되었는지 확인하십시오.
- 스탠바이의 기본 할당량 (제한) 은 0입니다. WorkSpaces 대기 모드를 생성하기 전에 서비스 할당량 증가를 요청해야 WorkSpace 합니다. 자세한 정보는 아마존 WorkSpaces 쿼터을 참조하세요.
- 고객 관리 키를 사용하여 기본 키와 예비 WorkSpaces 키를 모두 암호화하고 있는지 확인하십시오. 단일 지역 키 또는 다중 지역 키를 사용하여 기본 및 예비 복제본을 암호화할 수 있습니다. WorkSpaces

제한 사항

- WorkSpaces Standby는 기본 이미지의 번들 WorkSpaces 이미지만 복사하고 기본 이미지의 시스템 볼륨 (C 드라이브) 또는 사용자 볼륨 (D 드라이브) 은 복사하지 않습니다. WorkSpaces 시스템 볼륨 (C 드라이브) 또는 사용자 볼륨 (D 드라이브) 을 기본 WorkSpaces 볼륨에서 대기 모드로 WorkSpaces 복사하려면 데이터 복제를 활성화해야 합니다.
- 예비 WorkSpace 복제본은 직접 수정, 재구축, 복원 또는 마이그레이션할 수 없습니다.
- 리전 간 리디렉션의 장애 조치는 DNS 설정에 의해 제어됩니다. 자동 장애 조치 시나리오를 구현하려면 리전 간 리디렉션과 함께 다른 메커니즘을 사용해야 합니다. 예를 들어, 기본 지역의 CloudWatch 경보를 모니터링하는 Route 53 상태 확인과 함께 Amazon Route 53 장애 조치 DNS 라우팅 정책을 사용할 수 있습니다. 기본 지역의 CloudWatch 경보가 호출되면 DNS 장애 조치 라우팅 정책이 WorkSpaces 사용자를 장애 조치 지역에서 설정한 WorkSpaces 것으로 리디렉션합니다.
- 데이터 복제는 데이터를 기본 지역에서 보조 지역으로 복사하는 일방적인 방식으로만 이루어집니다. 스탠바이 WorkSpaces 페일오버 중에는 12시간에서 24시간 사이에 데이터 및 애플리케이션에 액세스할 수 있습니다. 운영 중단이 발생한 후에는 보조 서버에서 생성한 모든 데이터를 수동으로 WorkSpace 백업하고 로그아웃하십시오. 기본 WorkSpace 드라이브에서 데이터에 액세스할 수 있도록 네트워크 드라이브와 같은 외장 드라이브에 작업을 저장하는 것이 좋습니다.

- 데이터 복제는 AWS Simple AD를 지원하지 않습니다.
- 스탠바이 모드에서 WorkSpaces 데이터 복제를 활성화하면 기본 볼륨 WorkSpaces (루트 및 시스템 볼륨 모두) 의 EBS 스냅샷이 12시간마다 생성됩니다. 특정 데이터 볼륨의 초기 스냅샷은 꽉 찼고 후속 스냅샷은 증분 스냅샷입니다. 따라서 특정 항목의 첫 번째 복제는 후속 복제보다 WorkSpace 시간이 더 오래 걸립니다. 스냅샷은 내부 일정에 따라 시작되며 타이밍을 WorkSpaces 제어할 수 없습니다.
- 기본 WorkSpace 및 대기 모드가 동일한 도메인을 사용하여 WorkSpace 조인하는 경우 도메인 컨트롤러와의 연결이 끊기지 않도록 지정된 WorkSpace 시점의 기본 WorkSpace 또는 대기 모드에만 연결하는 것이 좋습니다.
- 다중 지역 복제를 구성한 경우 기본 지역의 디렉터리만 사용하도록 등록할 수 있습니다. AWS Managed Microsoft AD WorkSpaces 에서 사용할 복제된 리전에 디렉터리를 등록하려고 WorkSpaces 하면 실패합니다. 복제한 지역 WorkSpaces 내에서는 다중 지역 복제를 사용할 수 AWS Managed Microsoft AD 없습니다.
- 교차 리전 리디렉션을 이미 설정하고 예비 리전을 사용하지 않고 기본 리전과 보조 리전 WorkSpaces 모두에서 생성한 경우 보조 리전의 기존 WorkSpace 리전을 스탠바이 WorkSpaces 리전으로 직접 변환할 수 없습니다. WorkSpace 대신 보조 리전에서 를 종료하고 기본 리전에서 스탠바이 리전을 생성하려는 리전을 선택한 다음 스탠바이 리전을 사용하여 스탠바이 WorkSpace 리전을 WorkSpaces 생성해야 합니다. WorkSpace WorkSpace WorkSpace
- 운영 중단이 발생한 후에는 보조 서버에서 생성한 모든 데이터를 수동으로 WorkSpace 백업하고 로그아웃하십시오. 기본 WorkSpace 드라이브에서 데이터에 액세스할 수 있도록 네트워크 드라이브와 같은 외장 드라이브에 작업을 저장하는 것이 좋습니다.
- WorkSpaces 다중 지역 복원력은 현재 다음 지역에서 사용할 수 있습니다.
  - 미국 동부(버지니아 북부) 리전
  - US West (Oregon) Region
  - Europe (Frankfurt) Region
  - Europe (Ireland) Region
- WorkSpaces 다중 지역 복원력은 Linux, macOS 및 Windows 클라이언트 애플리케이션의 버전 3.0.9 이상에서만 지원됩니다. WorkSpaces Web Access와 함께 다중 리전 복원력을 사용할 수도 있습니다.
- WorkSpaces 다중 지역 복원력은 Windows 및 BYOL (기존 보유 라이선스 사용) 을 지원합니다. WorkSpaces 아마존 리눅스, 우분투 또는 GPU 지원 WorkSpaces (예: 그래픽 WorkSpaces GraphicsPro, 그래픽.G4dn 또는.g4dn) 은 지원하지 않습니다. GraphicsPro
- 페일오버 또는 페일백이 완료된 후 15~30분 정도 기다린 후 컴퓨터에 연결하십시오. WorkSpace

멀티 리전 레질리언스 스탠바이를 구성하십시오. WorkSpace

멀티 리전 레질리언스 스탠바이를 구성하려면 WorkSpace

1. 기본 및 보조 지역 모두에 사용자 디렉터리를 설정합니다. 각 지역의 각 WorkSpaces 디렉터리에 동일한 사용자 이름을 사용해야 합니다.

   Active Directory 사용자 데이터를 동기화된 상태로 유지하려면 AD Connector를 사용하여 WorkSpaces 사용자에 대해 설정한 각 지역의 동일한 Active Directory를 가리키는 것이 좋습니다. 디렉터리 만들기에 대한 자세한 내용은 디렉터리 등록을 참조하십시오 WorkSpaces.

   > **Important**
   >
   > 다중 지역 복제를 위해 AWS Managed Microsoft AD 디렉터리를 구성하는 경우 기본 지역의 디렉터리만 사용할 수 있도록 등록할 수 있습니다. WorkSpaces 에서 사용할 복제된 리전에 디렉터리를 등록하려는 시도는 실패합니다. WorkSpaces 다중 지역 복제는 복제된 지역 WorkSpaces 내에서 사용할 수 AWS Managed Microsoft AD 없습니다.

2. 기본 지역의 사용자를 WorkSpaces 위해 생성하세요. WorkSpaces생성에 대한 자세한 내용은 Launch를 참조하십시오 WorkSpaces.
3. 보조 리전에 스탠바이 WorkSpace 리전을 생성하십시오. 스탠바이 생성에 대한 자세한 내용은 WorkSpace 스탠바이 생성을 참조하십시오 WorkSpace.
4. 연결 문자열 (FQDN) 을 생성하여 기본 및 보조 지역의 사용자 디렉터리에 연결합니다.

   스탠바이 WorkSpaces 모드는 지역 간 리디렉션을 기반으로 하므로 계정에서 지역 간 리디렉션을 활성화해야 합니다. Amazon의 지역 간 리디렉션 지침의 1~3단계를 따르십시오. WorkSpaces
5. DNS 서비스를 구성하고 DNS 라우팅 정책을 설정합니다.

   DNS 서비스를 설정하고 필요한 DNS 라우팅 정책을 구성해야 합니다. 지역 간 리디렉션은 DNS 라우팅 정책과 함께 작동하여 필요에 따라 WorkSpaces 사용자를 리디렉션합니다.
6. 리전 간 리디렉션 설정을 완료하면 사용자에게 FQDN 연결 문자열이 포함된 이메일을 보내야 합니다. 자세한 내용은 5단계: 사용자에게 연결 문자열 보내기를 참조하십시오. WorkSpaces WorkSpaces 사용자가 기본 지역의 지역 기반 등록 코드 (예: WSPDX+ABC12d) 대신 FQDN 기반 등록 코드를 사용하고 있는지 확인하세요.

> **Important**
>
> - Active Directory에서 사용자를 생성하는 대신 WorkSpaces 콘솔에서 사용자를 생성하는 경우 새 사용자를 시작할 때마다 지역 기반 등록 코드가 포함된 초대 이메일이 WorkSpaces 자동으로 사용자에게 전송됩니다. WorkSpace 즉, 보조 지역의 WorkSpaces 사용자를 설정하면 보조 지역의 사용자도 해당 보조 지역의 이메일을 자동으로 받게 됩니다. WorkSpaces 리전 기반 등록 코드가 포함된 이메일은 무시하도록 사용자에게 지시해야 합니다.
> - 지역별 등록 코드는 계속 유효하지만 지역 간 리디렉션이 작동하려면 사용자가 등록 코드로 대신 FQDN을 사용해야 합니다.

스탠바이 생성하기 WorkSpace

WorkSpace스탠바이 리전을 생성하기 전에 기본 리전과 보조 리전 모두에서 사용자 디렉터리를 생성하고, 기본 리전의 사용자를 WorkSpaces 위한 프로비저닝, 계정의 크로스 리전 리디렉션 구성, 서비스 쿼터를 통한 대기 WorkSpaces 한도 증가 요청 등의 사전 요구 사항을 완료했는지 확인하세요.

스탠바이 그룹을 만들려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 WorkSpaces를 선택합니다.
4. 대기 모드를 WorkSpace WorkSpace 만들려는 서버를 선택합니다.
5. 작업을 선택한 다음 대기 모드 만들기를 선택합니다 WorkSpace.
6. 대기 모드를 생성할 보조 지역을 선택하고 WorkSpace 다음을 선택합니다.
7. 보조 리전의 사용자 디렉터리를 선택하고 다음을 선택합니다.
8. (선택 사항) 암호화 키를 추가하고, 데이터 암호화를 활성화하고, 태그를 관리합니다.
   - 암호화 키를 추가하려면 입력 암호화 키에 해당 키를 입력합니다.
   - 데이터 복제를 활성화하려면 데이터 복제 활성화를 선택합니다. 그런 다음 체크박스를 선택하여 추가 월별 요금을 승인했는지 확인합니다.
   - 새 태그를 추가하려면 새 태그 추가를 선택합니다.

그리고 다음을 선택합니다.

> **Note**
>
> - WorkSpace 원본이 암호화된 경우 이 필드는 미리 채워집니다. 하지만 자체 암호화 키로 교체할 수 있습니다.
> - 데이터 복제 상태를 업데이트하는 데 몇 분 정도 걸립니다.
> - 예비 WorkSpace 복제본이 기본 WorkSpace 스냅샷으로 성공적으로 업데이트되면 복구 스냅샷에서 스냅샷의 타임스탬프를 찾을 수 있습니다.

9. 예비 복제본의 설정을 검토한 다음 [Create] WorkSpaces 를 선택합니다.

> **Note**
>
> - 스탠바이 WorkSpaces 기기에 대한 정보를 보려면 기본 WorkSpace 세부 정보 페이지로 이동하십시오.
> - 스탠바이 모드는 WorkSpace 프라이머리의 번들 WorkSpace 이미지만 복사하고 프라이머리의 시스템 볼륨 (C 드라이브) 또는 사용자 볼륨 (D 드라이브) 은 복사하지 않습니다 WorkSpaces. 기본적으로 데이터 복제는 꺼져 있습니다. 시스템 볼륨 (C 드라이브) 또는 사용자 볼륨 (드라이브 D) 을 기본 볼륨에서 WorkSpaces WorkSpaces 스탠바이로 복사하려면 데이터 복제를 활성화해야 합니다.

스탠바이 디바이스 관리 WorkSpace

예비 WorkSpace 복제본을 직접 수정, 재구축, 복원 또는 마이그레이션할 수 없습니다.

스탠바이 스탠바이의 데이터 복제를 활성화하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 기본 지역으로 이동하여 기본 WorkSpace ID를 선택합니다.
3. 아래로 스크롤하여 대기 WorkSpace 섹션으로 이동한 다음 대기 편집을 선택합니다 WorkSpace.
4. 데이터 복제 활성화를 선택합니다. 그런 다음 체크박스를 선택하여 추가 월별 요금을 승인했는지 확인합니다. 그런 다음 저장을 선택합니다.

Note

- 대기 모드는 최대 절전 모드로 WorkSpaces 전환할 수 없습니다. 대기 모드를 WorkSpace 중지하면 저장되지 않은 작업은 보존되지 않습니다. 사용자는 대기 모드를 종료하기 전에 항상 작업을 저장하는 것이 좋습니다. WorkSpaces
- 대기 모드에서 WorkSpaces 데이터 복제를 활성화하려면 자체 관리되는 Active Directory 또는 대기 지역에 복제하도록 구성된 AWS 관리형 Microsoft AD가 있어야 합니다. 디렉터리를 설정하려면 Amazon AWS 및 디렉터리 서비스를 통한 비즈니스 연속성 구축의 안내 섹션의 1~3단계를 따르거나 WorkSpaces Amazon에서 AWS 다중 지역 관리형 Active Directory 사용을 참조하십시오. WorkSpaces 다중 지역 복제는 AWS 관리형 Microsoft AD의 엔터프라이즈 에디션에서만 지원됩니다.
- 데이터 복제 상태를 업데이트하는 데 몇 분 정도 걸립니다.
- 예비 WorkSpace 복제본이 기본 WorkSpace 스냅샷으로 성공적으로 업데이트되면 복구 스냅샷에서 스냅샷의 타임스탬프를 찾을 수 있습니다.

스탠바이 파일 삭제 WorkSpace

레귤러를 종료하는 것과 같은 방법으로 WorkSpace 스탠바이를 종료할 수 WorkSpace 있습니다.

스탠바이 그룹을 삭제하려면 WorkSpace

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 엽니다.
2. 콘솔 오른쪽 상단에서 해당 기본 AWS 지역을 선택합니다. WorkSpaces
3. 탐색 창에서 WorkSpaces를 선택합니다.
4. 대기 모드를 WorkSpace 선택하고 삭제를 선택합니다. 대기 모드를 삭제하는 데 약 5분이 걸립니다 WorkSpace. 삭제 중에는 대기의 상태가 종료중으로 설정됩니다. WorkSpace 삭제가 완료되면 콘솔에서 스탠바이 모드가 WorkSpace 사라집니다.

Note

대기 모드 WorkSpace 삭제는 영구적인 작업이며 취소할 수 없습니다. 스탠바이 WorkSpace 유저의 데이터는 유지되지 않고 파기됩니다. 사용자 데이터를 백업하는 데 도움이 필요하면 AWS Support에 문의하세요.

스탠바이용 단방향 데이터 복제 WorkSpaces

멀티 리전 레질리언스에서 데이터 복제를 활성화하면 기본 리전에서 보조 리전으로 데이터를 복제할 수 있습니다. 안정된 상태에서는 다중 지역 복원력이 12시간마다 주 서버의 시스템 (C 드라이브) 및 데이터 (D 드라이브) 스냅샷을 캡처합니다. WorkSpaces 이러한 스냅샷은 보조 지역으로 전송되어 스탠바이 리전을 업데이트하는 데 사용됩니다. WorkSpaces 기본적으로 WorkSpaces 스탠바이 모드에서는 데이터 복제가 비활성화됩니다.

WorkSpaces스탠바이에 대한 데이터 복제가 활성화되면 특정 데이터 볼륨의 초기 스냅샷이 완료되고 후속 스냅샷은 증분 스냅샷이 완료됩니다. 따라서 특정 항목의 첫 번째 복제는 후속 복제보다 WorkSpace 시간이 더 오래 걸립니다. 스냅샷은 범위 내에서 미리 정해진 간격으로 WorkSpaces 트리거되며 타이밍은 사용자가 제어할 수 없습니다.

페일오버 중에 사용자가 보조 지역으로 리디렉션되면 12~24시간 전의 데이터 및 WorkSpaces 애플리케이션으로 예비 복제본에 액세스할 수 있습니다. 사용자가 대기 모드를 WorkSpaces 사용하는 동안에는 Multi-Region Resilience에서 강제로 스탠바이 모드에서 WorkSpaces 로그아웃하거나 기본 리전의 WorkSpaces 스냅샷으로 스탠바이 모드를 업데이트하지 않아도 됩니다.

운영 중단이 발생한 후 사용자는 예비 복제본에서 WorkSpaces 로그아웃하기 전에 보조 서버에서 생성한 모든 데이터를 수동으로 백업해야 합니다. WorkSpaces 다시 로그인하면 기본 리전과 기본 리전으로 이동됩니다. WorkSpaces

복구를 위해 Amazon EC2 용량을 예약할 계획

Amazon 멀티 리전 레질리언스 (MRR) 는 기본적으로 Amazon EC2 온디맨드 풀을 사용합니다. 복구를 지원하는 데 특정 Amazon EC2 인스턴스 유형을 사용할 수 없는 경우 MRR은 사용 가능한 인스턴스 유형을 찾을 때까지 자동으로 인스턴스 확장을 반복적으로 시도하지만, 극단적인 상황에서는 인스턴스를 항상 사용할 수 없는 경우도 있습니다. 가장 중요한 WorkSpaces 인스턴스에 필요한 필수 인스턴스 유형의 가용성을 높이려면 Support에 문의하면 용량 계획을 AWS 지원해 드리겠습니다.

Amazon WorkSpaces의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. WorkSpaces에 적용되는 규정 준수 프로그램에 대해 알아보려면 AWS Services in Scope by Compliance Program(규정 준수 프로그램 제공 범위 내 서비스)(규정 준수 프로그램 제공 범위 내 서비스)를 참조하세요.
- 클라우드 내 보안 - 사용자의 책임은 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 WorkSpaces 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 WorkSpaces를 구성하는 방법을 보여줍니다. 또한 WorkSpaces 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

목차

아마존에서의 데이터 보호 WorkSpaces

AWS공동 책임 모델 Amazon의 데이터 보호에 적용됩니다 WorkSpaces. 이 모델이 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참

조하십시오. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 보안 인증 정보를 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)을 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정합니다.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2 섹션을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔AWS CLI, API WorkSpaces 또는 AWS 서비스 AWS SDK를 사용하거나 다른 사람을 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 보안 인증를 URL에 포함시켜서는 안 됩니다.

FIPS 엔드포인트 암호화에 대한 자세한 내용은 WorkSpaces 을 참조하십시오. FedRAMP 승인 또는 DoD SRG 준수를 위해 Amazon WorkSpaces 설정

저장 시 암호화

AWS KMS키를 WorkSpaces 사용하여 스토리지 볼륨을 암호화할 수 있습니다. AWS Key Management Service 자세한 설명은 암호화된 WorkSpaces 섹션을 참조하세요.

암호화된 WorkSpaces 볼륨으로 생성하는 경우 Amazon Elastic Block Store (Amazon EBS) 를 WorkSpaces 사용하여 해당 볼륨을 생성하고 관리합니다. EBS는 산업 표준 AES-256 알고리즘을 사용하여 데이터 키로 볼륨을 암호화합니다. 자세한 내용을 알아보려면 Amazon EC2 - Windows 인스턴스용 사용 설명서의 Amazon EBS 암호화를 참조하세요.

전송 중 암호화

PCoIP의 경우 전송 중 데이터는 TLS 1.2 암호화 및 SigV4 요청 서명을 사용하여 암호화됩니다. PCoIP 프로토콜은 AES 암호화와 함께 암호화된 UDP 트래픽을 픽셀 스트리밍에 사용합니다. 포트 4172(TCP 및 UDP)를 사용하는 스트리밍 연결은 AES-128 및 AES-256 암호를 사용하여 암호화되지만 암호화는 기본적으로 128비트로 설정됩니다. WorkSpacesWindows용 PCoIP 보안 설정 구성 그룹 정책 설정을 사용하거나 Amazon Linux용 파일의 PCoIP 보안 설정을 수정하여 이 기본값을 256비트로 변경할 수 있습니다. `pcoip-agent.conf` WorkSpaces

WorkSpacesAmazon의 그룹 정책 관리에 대한 자세한 내용은 을 참조하십시오 PCoIP 보안 설정 구성원도우 관리하기 WorkSpaces. `pcoip-agent.conf` 파일 수정에 대한 자세한 내용은 아마존 리눅스에서의 PCoIP 에이전트 동작 제어 WorkSpaces 및 Teradici 설명서의 PCoIP Security Settings를 참조하세요.

WorkSpaces 스트리밍 프로토콜 (WSP) 의 경우 전송 중인 스트리밍 및 제어 데이터는 UDP 트래픽에는 DTLS 1.2 암호화를 사용하고 TCP 트래픽에는 TLS 1.2 암호화를 사용하여 AES-256 암호를 사용하여 암호화됩니다.

WorkSpaces의 Identity and Access Management

기본적으로 IAM 사용자는 WorkSpaces 리소스 및 작업에 대한 권한이 없습니다. IAM 사용자에게 WorkSpaces 리소스를 관리하도록 허용하려면 권한을 명시적으로 부여하는 IAM 정책을 생성한 다음, 해당 권한이 필요한 IAM 사용자 또는 그룹에 정책을 연결해야 합니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가합니다.

- AWS IAM Identity Center의 사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.

- 자격 증명 공급자를 통해 IAM에서 관리되는 사용자:

  아이덴티티 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.

- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.

- (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

IAM 정책에 대한 자세한 내용은 IAM 사용 설명서에서 정책 및 권한을 참조하세요.

또한 WorkSpaces는 IAM 역할인 `workspaces_DefaultRole`을 생성하여 WorkSpaces 서비스가 필요한 리소스에 액세스할 수 있도록 합니다.

IAM에 대한 자세한 내용은 IAM 사용 설명서의 Identity and Access Management(IAM)를 참조하세요. IAM 권한 정책에 사용할 수 있는 WorkSpaces 관련 리소스, 작업 및 조건 컨텍스트 키는 IAM 사용 설명서의 Amazon WorkSpaces에 사용되는 작업, 리소스 및 조건 키에서 확인할 수 있습니다.

IAM 정책을 생성하는 데 도움이 되는 도구는 AWS 정책 생성기를 참조하세요. 또한 IAM 정책 시뮬레이터를 사용하여 정책이 AWS에 대한 특정 요청을 허용하는지 또는 거부하는지를 테스트할 수 있습니다.

> **Note**
>
> Amazon WorkSpaces에서는 WorkSpace로의 IAM 보안 인증 정보 프로비저닝을 지원하지 않습니다(예: 인스턴스 프로파일 포함).

목차

정책 예제

다음 예시는 IAM 사용자가 갖는 Amazon WorkSpaces 관련 권한을 제어하는 데 사용할 수 있는 정책 문을 보여 줍니다.

Example 1: 모든 WorkSpaces 작업 수행

다음 정책 문은 IAM 사용자에게 디렉터리 생성 및 관리를 포함한 모든 WorkSpaces 작업을 수행할 수 있는 권한을 부여합니다. 또한 빠른 설정 절차를 실행할 수 있는 권한도 부여합니다.

Amazon WorkSpaces는 API 및 명령줄 도구를 사용할 때 `Action` 및 `Resource` 요소를 완전히 지원하지만 AWS Management Console에서 Amazon WorkSpaces를 사용하려면 IAM 사용자에게 다음 작업 및 리소스에 대한 권한이 있어야 합니다.

- 작업: `"workspaces:*"` 및 `"ds:*"`
- 리소스: `"Resource": "*"`

다음 예시 정책은 IAM 사용자가 AWS Management Console에서 Amazon WorkSpaces를 사용할 수 있도록 허용하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
```

```
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2: WorkSpaces 관련 작업 수행

다음 정책 문은 IAM 사용자에게 WorkSpace 관련 작업(예: WorkSpaces 시작 및 제거)을 수행할 수 있는 권한을 부여합니다. 정책 문에서 `ds:*` 작업은 계정의 모든 Directory Services 객체를 완전히 제어할 수 있는 폭넓은 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

또한 사용자에게 WorkSpaces 내부 사용자에 대해 Amazon WorkDocs를 활성화할 수 있는 권한을 부여하려면 다음 예시에 표시된 workdocs 작업을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

또한 사용자에게 WorkSpaces 시작 마법사를 사용할 수 있는 권한을 부여하려면 다음 예제에 표시된 대로 kms 작업을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: BYOL WorkSpaces에 대한 모든 WorkSpaces 작업 수행

다음 정책 문은 IAM 사용자에게 기존 보유 라이선스 사용(BYOL) WorkSpaces를 생성하는 데 필요한 Amazon EC2 작업을 포함하여 모든 WorkSpaces 작업을 수행할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
```

```
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

IAM 정책에서 WorkSpaces 리소스 지정

정책 문의 `Resource` 요소에서 WorkSpaces 리소스를 지정하려면 리소스의 Amazon 리소스 이름(ARN)을 사용합니다. IAM 정책 문의 `Action` 요소에 지정된 API 작업을 사용할 수 있는 권한을 허용하거나 거부하여 WorkSpaces 리소스에 대한 액세스를 제어합니다. WorkSpaces는 WorkSpaces, 번들, IP 그룹 및 디렉터리에 대한 ARN을 정의합니다.

WorkSpaces ARN

WorkSpace ARN에는 다음 예제와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

리전

WorkSpace가 위치한 리전(예: `us-east-1`)

account_id

하이픈을 제외한 AWS 계정의 ID(예: `123456789012`)

workspace_identifier

WorkSpaces의 ID(예: `ws-a1bcd2efg`).

정책 설명에서 특정 WorkSpace를 식별하는 Resource 요소의 형식은 다음과 같습니다.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 WorkSpaces를 지정할 수 있습니다.

이미지 ARN

WorkSpace 이미지 ARN에는 다음 예시와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

리전

WorkSpace 이미지가 위치한 리전(예: us-east-1)

account_id

하이픈을 제외한 AWS 계정의 ID(예: 123456789012)

bundle_identifier

WorkSpaces 이미지의 ID(예: wsi-a1bcd2efg).

정책 문에서 특정 이미지를 식별하는 Resource 요소의 형식은 다음과 같습니다.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 이미지를 지정할 수 있습니다.

번들 ARN

번들 ARN에는 다음 예제와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

리전

WorkSpace가 위치한 리전(예: us-east-1)

account_id

하이픈을 제외한 AWS 계정의 ID(예: 123456789012)

bundle_identifier

WorkSpaces 번들의 ID(예: `wsb-a1bcd2efg`).

정책 설명에서 특정 번들을 식별하는 `Resource` 요소의 형식은 다음과 같습니다.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 번들을 지정할 수 있습니다.

IP 그룹 ARN

IP 그룹 ARN에는 다음 예제와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

리전

WorkSpace가 위치한 리전(예: `us-east-1`)

account_id

하이픈을 제외한 AWS 계정의 ID(예: `123456789012`)

ipgroup_identifier

IP 그룹의 ID(예: `wsipg-a1bcd2efg`).

정책 설명에서 특정 IP 그룹을 식별하는 `Resource` 요소의 형식은 다음과 같습니다.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 IP 그룹을 지정할 수 있습니다.

디렉터리 ARN

디렉터리 ARN에는 다음 예제와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

리전

WorkSpace가 위치한 리전(예: us-east-1)

account_id

하이픈을 제외한 AWS 계정의 ID(예: 123456789012)

directory_identifier

디렉터리의 ID(예: d-12345a67b8).

정책 설명에서 특정 디렉터리를 식별하는 Resource 요소의 형식은 다음과 같습니다.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 디렉터리를 지정할 수 있습니다.

연결 별칭 ARN

연결 별칭 ARN에는 다음 예시와 같은 구문이 있습니다.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

리전

연결 별칭이 속한 리전(예: us-east-1)

account_id

하이픈을 제외한 AWS 계정의 ID(예: 123456789012)

connectionalias_identifier

연결 별칭의 ID(예: wsca-12345a67b8)

정책 문에서 특정 연결 별칭을 식별하는 Resource 요소의 형식은 다음과 같습니다.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

* 와일드카드를 사용하여 특정 리전의 특정 계정에 속하는 모든 연결 별칭을 지정할 수 있습니다.

리소스 수준 권한이 지원되지 않는 API 작업

다음 API 작업에는 리소스 ARN을 지정할 수 없습니다.

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

리소스 수준 권한을 지원하지 않는 API 작업의 경우 다음 예제와 같이 리소스 명령문을 지정해야 합니다.

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

공유 리소스에 대한 계정 수준 제한을 지원하지 않는 API 작업

다음 API 작업의 경우 계정이 리소스를 소유하지 않은 경우 리소스 ARN에 계정 ID를 지정할 수 없습니다.

- AssociateConnectionAlias
- CopyWorkspaceImage

- `DisassociateConnectionAlias`

이러한 API 작업의 경우 해당 계정이 작업 대상 리소스를 소유한 경우에만 리소스 ARN에 계정 ID를 지정할 수 있습니다. 계정이 리소스를 소유하지 않는 경우, 다음 예시처럼 계정 ID에 *를 지정해야 합니다.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

workspaces_DefaultRole 역할 생성

API를 사용하여 디렉터리를 등록하려면 먼저 이름이 `workspaces_DefaultRole`인 역할이 존재하는지 확인해야 합니다. 이 역할은 빠른 설정을 통해 생성되거나 AWS Management Console을 사용하여 WorkSpaces를 시작하는 경우 생성되며, 사용자 대신 특정 AWS 리소스에 액세스할 수 있는 권한을 Amazon WorkSpaces에 부여합니다. 이 역할이 없는 경우, 다음 절차에 따라 만들 수도 있습니다.

workspaces_DefaultRole 역할을 생성하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 역할을 선택합니다.
3. 역할 생성을 선택합니다.
4. Select type of trusted entity(신뢰할 수 있는 엔터티 유형 선택) 아래에서 다른 Another AWS account (AWS 계정)를 선택합니다.
5. 계정 ID에 하이픈이나 공백 없이 계정 ID를 입력합니다.
6. 옵션에서 Multi-Factor Authentication(MFA)을 지정하지 마십시오.
7. 다음: 권한을 선택합니다.
8. 권한 정책 연결 페이지에서 AWS 관리형 정책인 AmazonWorkSpacesServiceAccess 및 AmazonWorkSpacesSelfServiceAccess를 선택합니다.
9. 이 역할에 연결된 정책과 충돌할 가능성이 있으므로 권한 경계 설정에서 권한 경계를 사용하지 않는 것이 좋습니다. 충돌이 발생할 경우 역할에 필요한 특정 권한이 차단될 수 있습니다.
10. Next: Tags(다음: 태그)를 선택합니다.
11. 필요한 경우 Add tags (optional)(태그 추가(선택 사항)) 페이지에서 태그를 추가합니다.
12. Next: Review(다음: 검토)를 선택합니다.
13. 검토 페이지의 역할 이름에 **`workspaces_DefaultRole`**을 입력합니다.

14. (선택 사항) 역할 설명에 설명을 입력합니다.
15. 역할 생성을 선택합니다.
16. workspaces_DefaultRole 역할에 대한 요약 페이지에서 신뢰 관계 탭을 선택합니다.
17. 신뢰 관계(Trust relationships) 탭에서 신뢰 관계 편집(Edit trust relationship)을 선택합니다.
18. Edit Trust Relationship(신뢰 관계 편집) 페이지에서 기존 정책 설명을 다음 설명으로 바꿉니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. 신뢰 정책 업데이트(Update Trust Policy)를 선택합니다.

AmazonWorkSpacesPCAAccess 서비스 역할 생성

사용자가 인증서 기반 인증을 사용하여 로그인할 수 있으려면 먼저 이름이 `AmazonWorkSpacesPCAAccess`인 역할이 존재하는지 확인해야 합니다. 이 역할은 AWS Management Console을 사용하여 디렉터리에서 인증서 기반 인증을 활성화할 때 생성되며, 사용자 대신 AWS Private CA 리소스에 액세스할 수 있는 권한을 Amazon WorkSpaces에 부여합니다. 콘솔을 사용하여 인증서 기반 인증을 관리하지 않아 이 역할이 존재하지 않는 경우 다음 절차를 사용하여 생성할 수 있습니다.

AWS CLI를 사용하여 AmazonWorkSpacesPCAAccess 서비스 역할을 생성하는 방법

1. 다음 텍스트로 이름이 `AmazonWorkSpacesPCAAccess.json`인 JSON 파일을 생성합니다.

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

```
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 필요에 따라 AmazonWorkSpacesPCAAccess.json 경로를 조정하고 다음 AWS CLI 명령을 실행하여 서비스 역할을 생성하고 AmazonWorkspacesPCAAccess 관리형 정책을 연결합니다.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

WorkSpaces AWS 관리형 정책

AWS 관리형 정책을 사용하면 정책을 직접 작성하는 것보다 사용자, 그룹 또는 역할에 권한을 추가하기가 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 신속하게 시작하려면 AWS 관리형 정책을 사용하세요. 이러한 정책은 일반적인 사용 사례에 적용되며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 정보는 IAM 사용 설명서에서 AWS 관리형 정책을 참조하세요.

AWS 서비스 유지 관리 및 AWS 관리형 정책 업데이트입니다. AWS 관리형 정책에서 권한을 변경할 수 없습니다. 서비스는 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 자격 증명(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 태스크를 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않기 때문에 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 AWS는 여러 서비스의 직무에 대한 관리형 정책을 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스 권한을 제공합니다. 서비스에서 새 기능을 시작하면 AWS 가 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonWorkSpacesAdmin

이 정책은 Amazon WorkSpaces 관리 작업에 대한 액세스를 제공합니다. 다음 권한을 제공합니다.

- `workspaces` - WorkSpaces 리소스에 대한 관리 작업을 수행할 수 있는 액세스를 허용합니다.
- `kms` - KMS 키와 목록 별칭을 나열하고 설명할 수 있는 액세스를 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AmazonWorkspacesPCAAccess

이 관리형 정책은 인증서 기반 인증을 위해 AWS 계정의 AWS Certificate Manager Private Certificate Authority(Private CA) 리소스에 대한 액세스를 제공합니다. 이 정책은 AmazonWorkSpacesPCAAccess 역할에 포함되며 다음과 같은 권한을 제공합니다.

- acm-pca - 인증서 기반 인증을 관리할 수 있도록 AWS Private CA에 액세스를 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

AWS 관리형 정책: AmazonWorkSpacesSelfServiceAccess

이 정책은 사용자가 시작한 WorkSpaces 셀프 서비스 작업을 수행할 수 있는 Amazon WorkSpaces 서비스에 대한 액세스를 제공합니다. 이 정책은 workspaces_DefaultRole 역할에 포함되며 다음과 같은 권한을 제공합니다.

- workspaces - 사용자를 위한 셀프 서비스 WorkSpace 관리 기능에 액세스를 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AmazonWorkSpacesServiceAccess

이 정책은 WorkSpace를 시작하기 위한 Amazon WorkSpaces 서비스에 대한 고객 계정 액세스를 제공합니다. 이 정책은 `workspaces_DefaultRole` 역할에 포함되며 다음과 같은 권한을 제공합니다.

- `ec2` - WorkSpace와 연결된 Amazon EC2 리소스(예: 네트워크 인터페이스)를 관리할 수 있는 액세스를 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책 관련 WorkSpaces 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 WorkSpaces의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다.

변경 사항	설명	날짜
the section called “AmazonWorkSpacesAdmin” - 정책 업데이트	WorkSpaces에서 Amazon WorkspacesAdmin 관리형 정책에 `workspaces:RestoreWorkspace` 작업을 추가하	2023년 6월 25일

변경 사항	설명	날짜
	여 관리자에게 WorkSpaces를 복원할 수 있는 액세스를 부여했습니다.	
the section called “AmazonWorkspacesPCAAccess” - 새 정책 추가	WorkSpaces에서 인증서 기반 인증을 관리하기 위해 AWS Private CA를 관리할 `acm-pca` 권한을 부여하는 새로운 관리형 정책을 추가했습니다.	2022년 11월 18일
WorkSpaces, 변경 사항 추적 시작	WorkSpaces 관리형 정책에 대한 변경 사항 추적을 WorkSpaces에서 시작했습니다.	2021년 3월 1일

Amazon WorkSpaces 규정 준수 검증

서드 파티 감사자는 여러 AWS 규정 준수 프로그램의 일환으로 Amazon WorkSpaces의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램의 범위 내에 있는 AWS 서비스 목록은 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하세요. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

WorkSpaces 및 FedRAMP에 대한 자세한 내용은 FedRAMP 승인 또는 DoD SRG 준수를 위해 Amazon WorkSpaces 설정 섹션을 참조하세요.

Amazon WorkSpaces 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS는 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 AWS에서 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계 - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 생성하는 방법을 설명합니다.

- AWS 규정 준수 리소스 - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 콜렉션입니다.
- AWS Config 개발자 가이드의 규칙을 사용하여 리소스 평가 – AWS Config를 사용하여 리소스 구성이 내부 사례, 업계 지침, 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

Amazon WorkSpaces의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Amazon WorkSpaces는 또한 리전 간 리디렉션을 제공합니다. 리전 간 리디렉션은 도메인 이름 시스템(DNS) 장애 조치 라우팅 정책과 함께 작동하여 기본 WorkSpaces를 사용할 수 없는 경우 WorkSpaces 사용자를 다른 AWS 리전의 대체 WorkSpaces로 리디렉션하는 기능입니다. 자세한 내용은 Amazon을 위한 지역 간 리디렉션 WorkSpaces 섹션을 참조하세요.

Amazon WorkSpaces의 인프라 보안

관리형 서비스인 Amazon WorkSpaces는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 WorkSpaces에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

네트워크 격리

Virtual Private Cloud(VPC)는 AWS 클라우드에서 논리적으로 격리된 고유한 영역의 가상 네트워크입니다. VPC의 프라이빗 서브넷에 WorkSpaces를 배포할 수 있습니다. 자세한 내용은 다음에 대해 VPC를 구성합니다. WorkSpaces 섹션을 참조하세요.

특정 주소 범위(예: 회사 네트워크에서)의 트래픽만 허용하려면 VPC에 대한 보안 그룹을 업데이트하거나 IP 액세스 제어 그룹을 사용합니다.

WorkSpace 액세스를 유효한 인증서가 있는 신뢰할 수 있는 디바이스로 제한할 수 있습니다. 자세한 내용은 신뢰할 수 있는 장치에 WorkSpaces 대한 액세스 제한 섹션을 참조하세요.

물리적 호스트에서 격리

동일한 물리적 호스트에 있는 서로 다른 WorkSpaces는 하이퍼바이저를 통해 서로 격리됩니다. 마치 별도의 물리적 호스트에 있는 것처럼 보입니다. WorkSpace가 삭제되면 새 WorkSpace에 메모리가 할당되기 전에 하이퍼바이저에 의해 WorkSpace에 할당된 메모리가 스크러빙(0으로 설정)됩니다.

기업 사용자의 권한 부여

WorkSpaces를 사용하면 디렉터리가 AWS Directory Service를 통해 관리됩니다. 사용자를 위한 독립 실행형 관리형 디렉터리를 생성할 수 있습니다. 기존 Active Directory 환경과 통합할 수 있으므로 사용자가 현재 자격 증명을 사용하여 회사 리소스에 원활하게 액세스할 수 있습니다. 자세한 내용은 WorkSpaces 디렉터리 관리 섹션을 참조하세요.

WorkSpaces에 대한 액세스를 추가로 제어하려면 Multi-Factor Authentication을 사용합니다. 자세한 내용은 How to Enable Multi-Factor Authentication for AWS Services를 참조하세요.

VPC 인터페이스 엔드포인트를 통해 Amazon WorkSpaces API 요청 전송

인터넷을 통해 연결하는 대신 Virtual Private Cloud(VPC)의 인터페이스 엔드포인트를 통해 Amazon WorkSpaces API 엔드포인트에 직접 연결할 수 있습니다. VPC 인터페이스 엔드포인트를 사용하는 경우 VPC와 Amazon WorkSpaces API 엔드포인트 간의 통신은 모두 AWS 네트워크에서 안전하게 수행됩니다.

> **Note**
>
> 이 기능은 WorkSpaces API 엔드포인트에 연결하는 데만 사용할 수 있습니다. WorkSpaces 클라이언트를 사용하여 WorkSpaces에 연결하려면 IP 주소 및 포트 요구 사항 WorkSpaces의 설명과 같이 인터넷 연결이 필요합니다.

Amazon WorkSpaces API 엔드포인트는 AWS PrivateLink에서 구동되는 Amazon Virtual Private Cloud(Amazon VPC) 인터페이스 엔드포인트를 지원합니다. 각 VPC 엔드포인트는 VPC 서브넷의 프라이빗 IP 주소와 함께 하나 이상의 네트워크 인터페이스(ENI(탄력적 네트워크 인터페이스)라고도 함)로 표시됩니다.

VPC 인터페이스 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 VPC를 직접 Amazon WorkSpaces API 엔드포인트에 연결합니다. VPC에 있는 인스턴스는 퍼블릭 IP 주소가 없어도 Amazon WorkSpaces API 엔드포인트와 통신할 수 있습니다.

AWS Management Console 또는 AWS Command Line Interface(AWS CLI) 명령을 사용하여 Amazon WorkSpaces에 연결할 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 인터페이스 엔드포인트 생성을 참조하십시오.

VPC 엔드포인트를 생성한 후에는 `endpoint-url` 파라미터를 사용하는 다음 예시 CLI 명령을 사용하여 Amazon WorkSpaces API 엔드포인트에 대한 인터페이스 엔드포인트를 지정할 수 있습니다.

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

VPC 엔드포인트에 프라이빗 DNS 호스트 이름을 활성화하면 엔드포인트 URL을 지정할 필요가 없습니다. CLI 및 Amazon WorkSpaces SDK에서 기본적으로 사용하는 Amazon WorkSpaces API DNS 호스트 이름(https://api.workspaces.*Region*.amazonaws.com)은 VPC 엔드포인트로 확인됩니다.

Amazon WorkSpaces API 엔드포인트는 Amazon VPC와 Amazon WorkSpaces를 모두 사용할 수 있는 모든 AWS 리전에서 VPC 엔드포인트를 지원합니다. Amazon WorkSpaces는 VPC 내부에 있는 모든 퍼블릭 API에 대한 직접 호출을 지원합니다.

AWS PrivateLink에 대한 자세한 내용은 AWS PrivateLink 설명서를 참조하세요. VPC 엔드포인트 요금은 VPC 요금을 참조하십시오. VPC와 엔드포인트에 대한 자세한 내용은 Amazon VPC를 참조하십시오.

리전별 Amazon WorkSpaces API 엔드포인트 목록을 보려면 WorkSpaces API 엔드포인트를 참조하세요.

> **Note**
>
> AWS PrivateLink를 사용하는 Amazon WorkSpaces API 엔드포인트는 Federal Information Processing Standard(FIPS) Amazon WorkSpaces API 엔드포인트에 지원되지 않습니다.

Amazon WorkSpaces에 대한 VPC 엔드포인트 정책 생성

Amazon WorkSpaces에 대한 Amazon VPC 엔드포인트 정책을 생성하여 다음을 지정할 수 있습니다.

- 태스크를 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업입니다.
- 태스크를 수행할 있는 리소스.

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

> **Note**
>
> VPC 엔드포인트 정책은 Federal Information Processing Standard(FIPS) Amazon WorkSpaces 엔드포인트에 지원되지 않습니다.

다음 예시 VPC 엔드포인트 정책에서는 VPC 인터페이스 엔드포인트에 대한 액세스 권한이 있는 모든 사용자가 `ws-f9abcdefg`로 명명된 Amazon WorkSpaces에 호스팅된 엔드포인트를 호출할 수 있도록 지정합니다.

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

이 예제에서 다음 작업은 거부됩니다.

- `ws-f9abcdefg` 외의 Amazon WorkSpaces에 호스팅된 엔드포인트를 호출합니다.
- 지정된 리소스(WorkSpace ID: `ws-f9abcdefg`) 이외의 모든 리소스에 대한 작업 수행

> **Note**
>
> 이 예시에서 사용자는 VPC 외부로부터의 다른 Amazon WorkSpaces API 작업을 계속 사용할 수 있습니다. API 호출을 VPC 내의 호출로 제한하려면 WorkSpaces의 Identity and Access Management에서 자격 증명 기반 정책을 사용하여 Amazon WorkSpaces API 엔드포인트에 대한 액세스를 제어하는 방법을 참조하세요.

VPC에 프라이빗 네트워크 연결

VPC를 통해 Amazon WorkSpaces API를 호출하려면 VPC 내 인스턴스에서 연결하거나 AWS Virtual Private Network(AWS VPN) 또는 AWS Direct Connect를 사용하여 VPC에 프라이빗 네트워크를 연결해야 합니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 VPN 연결을 참조하세요. AWS Direct Connect에 대한 자세한 내용은 AWS Direct Connect 사용 설명서의 연결 생성을 참조하세요.

에서 업데이트 관리 WorkSpaces

운영 체제와 애플리케이션을 정기적으로 패치하고 업데이트하고 보호하는 것이 좋습니다 WorkSpaces. 정기 유지 관리 WorkSpaces 기간 중에 WorkSpaces 업데이트되도록 구성하거나 직접 업데이트할 수 있습니다. 자세한 설명은 WorkSpace 유지 관리 섹션을 참조하세요.

에 설치된 응용 프로그램의 경우 제공된 자동 업데이트 서비스를 사용하거나 응용 프로그램 공급업체에서 제공하는 업데이트 설치 권장 사항을 따를 수 있습니다. WorkSpaces

문제 해결 WorkSpaces

다음 정보는 관련 문제를 해결하는 데 도움이 될 수 있습니다 WorkSpaces.

고급 로깅 활성화

사용자가 겪을 수 있는 문제를 해결하는 데 도움이 되도록 모든 Amazon WorkSpaces 클라이언트에서 고급 로깅을 활성화할 수 있습니다.

고급 로깅은 상세 성능 데이터를 비롯하여 진단 정보와 디버깅 수준 세부 정보가 포함된 로그 파일을 생성합니다. 1.0+ 및 2.0+ 클라이언트의 경우 이러한 고급 로깅 파일은 의 데이터베이스에 자동으로 업로드됩니다. AWS

> **Note**
>
> 고급 로깅 파일을 AWS 검토하고 WorkSpaces 클라이언트 문제에 대한 기술 지원을 받으려면 문의하십시오. AWS Support자세한 내용은 AWS Support Center를 참조하세요.

Web Access에 대한 고급 로깅을 활성화하는 방법

Web Access에 대한 고급 로깅을 활성화하는 방법

1. Amazon WorkSpaces 웹 액세스 클라이언트를 엽니다.
2. WorkSpaces 로그인 페이지 상단에서 진단 로깅을 선택합니다.
3. 팝업 대화 상자에서 진단 로깅이 활성화되어 있는지 확인합니다.
4. 로그 수준에서 고급 로깅을 선택합니다.

Google Chrome, Microsoft Edge, Firefox에서 로그 파일에 액세스하는 방법

1. 브라우저에서 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열거나 키보드에서 Ctrl+Shift+I(Mac의 경우 command+옵션+I)를 눌러 개발자 도구 패널을 엽니다.
2. 개발자 도구 패널에서 콘솔 탭을 선택하여 로그 파일을 찾습니다.

Safari에서 로그 파일에 액세스하는 방법

1. Safari, 설정을 선택합니다.

2. Settings 창에서 Advanced를 선택합니다.
3. Show Develop menu in menu bar를 선택합니다.
4. 메뉴 막대의 Develop 탭에서 Develop > Show Web Inspector를 선택합니다.
5. Safari Web Inspector 패널에서 Console 탭을 선택하여 로그 파일을 찾습니다.

4.0+ 클라이언트에서 고급 로깅을 활성화하는 방법

Windows 클라이언트 로그는 다음 위치에 저장됩니다.

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 명령 프롬프트 앱을 엽니다.
3. `-l3`플래그를 사용하여 WorkSpaces 클라이언트를 시작합니다.

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 모든 사용자가 아닌 한 명의 사용자용으로 설치한 경우 WorkSpaces 다음 명령을 사용하십시오.
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

macOS 클라이언트 로그는 다음 위치에 저장됩니다.

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

macOS 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 터미널을 엽니다.
3. 다음 명령을 실행합니다.

```
open -a workspaces --args -l3
```

Android 클라이언트에서 고급 로깅을 활성화하는 방법

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. Android 클라이언트 메뉴를 엽니다.
3. 지원을 선택합니다.
4. 로깅 설정를 선택합니다.
5. 고급 로깅 활성화를 선택합니다.

고급 로깅을 활성화한 후 Android 클라이언트의 로그를 검색하는 방법

- 압축된 로그를 로컬에 저장하려면 로그 추출을 선택합니다.

Linux 클라이언트 로그는 다음 위치에 저장됩니다.

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Linux 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 터미널을 엽니다.
3. 다음 명령을 실행합니다.

```
/opt/workspacesclient/workspacesclient -l3
```

3.0 클라이언트에서 고급 로깅을 활성화하는 방법

Windows 클라이언트 로그는 다음 위치에 저장됩니다.

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 명령 프롬프트 앱을 엽니다.
3. `-l3`플래그를 사용하여 WorkSpaces 클라이언트를 시작합니다.

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 모든 사용자가 아닌 한 명의 사용자용으로 설치한 경우 WorkSpaces 다음 명령을 사용하십시오.
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

macOS 클라이언트 로그는 다음 위치에 저장됩니다.

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

macOS 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 터미널을 엽니다.
3. 다음 명령을 실행합니다.

```
open -a workspaces --args -l3
```

Android 클라이언트에서 고급 로깅을 활성화하는 방법

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. Android 클라이언트 메뉴를 엽니다.

3. 지원을 선택합니다.
4. 로깅 설정를 선택합니다.
5. 고급 로깅 활성화를 선택합니다.

고급 로깅을 활성화한 후 Android 클라이언트의 로그를 검색하는 방법

- 압축된 로그를 로컬에 저장하려면 로그 추출을 선택합니다.

Linux 클라이언트 로그는 다음 위치에 저장됩니다.

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Linux 클라이언트에 대한 고급 로깅을 활성화하려면

1. Amazon WorkSpaces 클라이언트를 닫습니다.
2. 터미널을 엽니다.
3. 다음 명령을 실행합니다.

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

1.0+ 및 2.0+ 클라이언트에 대한 고급 로깅을 활성화하려면

1. WorkSpaces 클라이언트를 엽니다.
2. 클라이언트 애플리케이션의 오른쪽 위 모서리에 있는 기어 아이콘을 선택합니다.
3. 고급 설정(Advanced Settings)을 선택합니다.
4. Enable Advanced Logging(고급 로깅 활성화) 확인란을 선택합니다.
5. 저장을 선택합니다.

Windows 클라이언트 로그는 다음 위치에 저장됩니다.

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

macOS 클라이언트 로그는 다음 위치에 저장됩니다.

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

구체적인 문제 해결

다음 정보는 관련 문제를 해결하는 데 도움이 될 수 있습니다 WorkSpaces.

문제

- 사용자 이름에 잘못된 문자가 WorkSpace 있어서 Amazon Linux를 생성할 수 없습니다.
- Amazon WorkSpace Linux용 셸을 변경했는데 이제 PCoIP 세션을 프로비저닝할 수 없습니다.
- 내 아마존 리눅스가 WorkSpaces 시작되지 않아요
- 연결된 WorkSpaces 디렉터리에서 시작하는 데 종종 실패합니다.
- 내부 오류로 WorkSpaces 인해 시작이 실패합니다.
- 디렉터리를 등록하려고 하면 등록이 실패하고 디렉터리가 오류 상태로 남는 경우
- 내 사용자는 대화형 로그온 배너가 WorkSpace 있는 Windows에 연결할 수 없습니다.
- 내 사용자는 Windows에 연결할 수 없습니다. WorkSpace
- 사용자가 WorkSpaces Web WorkSpaces Access에서 로그온하려고 할 때 문제가 발생했습니다.
- Amazon WorkSpaces 클라이언트는 로그인 화면으로 돌아가기 전에 잠시 회색 “로드 중...” 화면을 표시합니다. 다른 오류 메시지는 나타나지 않습니다.
- 내 사용자에게 "WorkSpace 상태: 비정상” 메시지가 표시됩니다. 귀하의 WorkSpace 계정에 연결하지 못했습니다. 몇 분 후에 다시 시도하세요.'라는 오류 메시지가 표시되는 경우
- 내 사용자에게 “이 장치는 액세스 권한이 없습니다.” 라는 메시지가 표시됩니다. WorkSpace Please contact your administrator for assistance.(이 디바이스는 WorkSpace에 액세스할 수 있는 권한이 없습니다. 관리자에게 지원을 요청하십시오.)”라는 메시지가 표시됩니다.
- 사용자가 WSP WorkSpace에 연결하려고 할 때 '네트워크가 없습니다. 네트워크 연결이 끊어졌습니다. 네트워크 연결을 확인하거나 관리자에게 도움을 요청하세요.'라는 오류 메시지가 나타나는 경우 WSP에 연결하려고 할 때 WorkSpace
- WorkSpaces 클라이언트에서 사용자에게 네트워크 오류가 발생하지만 사용자는 자신의 장치에서 다른 네트워크 지원 앱을 사용할 수 있습니다.
- WorkSpace 사용자에게 다음과 같은 오류 메시지가 표시됩니다. “디바이스를 등록 서비스에 연결할 수 없습니다. Check your network settings.(디바이스에서 등록 서비스에 연결할 수 없습니다. 네트워크 설정을 확인하십시오.)"라는 오류 메시지가 표시됩니다.
- PCoIP 제로 클라이언트 사용자에게 “The supplied certificate is invalid due to timestamp.(제공된 인증서가 타임스탬프로 인해 유효하지 않습니다.)”라는 오류 메시지가 표시되는 경우
- USB 프린터 및 기타 USB 주변 디바이스가 PCoIP 제로 클라이언트에서 작동하지 않는 경우

- 사용자가 Windows 또는 macOS 클라이언트 애플리케이션 업데이트를 건너뛰었고 최신 버전을 설치하라는 메시지가 표시되지 않습니다.
- 사용자는 Chromebook에서 Android 클라이언트 애플리케이션을 설치할 수 없습니다.
- 사용자에게 초대 이메일 또는 암호 재설정 이메일이 수신되지 않습니다.
- 사용자에게 클라이언트 로그인 화면의 암호 찾기 옵션이 표시되지 않습니다.
- Windows에 응용 프로그램을 설치하려고 하면 “시스템 관리자가 이 설치를 금지하도록 정책을 설정했습니다.” 라는 메시지가 나타납니다. WorkSpace
- 내 디렉터리에서 인터넷에 연결할 수 없습니다 WorkSpaces .
- WorkSpace My의 인터넷 연결이 끊겼습니다.
- 온프레미스 디렉터리에 연결할 때 "DNS unavailable" 오류가 표시되는 경우
- 내 온프레미스 디렉터리에 연결할 때 "Connectivity issues detected" 오류가 표시되는 경우
- 내 온프레미스 디렉터리에 연결할 때 "SRV record" 오류가 표시되는 경우
- Windows가 WorkSpace 유휴 상태로 남아 있으면 절전 모드로 전환됩니다.
- 제 중 한 명이 WorkSpaces 다음과 같은 상태입니다. UNHEALTHY
- 내 WorkSpace 것이 예기치 않게 충돌하거나 재부팅됩니다.
- 동일한 사용자 이름이 두 개 이상 WorkSpace 있지만 사용자는 다음 중 하나에만 로그인할 수 있습니다. WorkSpaces
- Amazon에서 Docker를 사용하는 데 문제가 있습니다. WorkSpaces
- 일부 API ThrottlingException 호출에서 오류가 발생합니다.
- 백그라운드에서 실행하도록 놔두면 WorkSpace 계속 연결이 끊깁니다.
- SAML 2.0 페더레이션 기능이 작동하지 않고 내 사용자는 WorkSpaces 데스크톱을 스트리밍할 권한이 없어요.
- 60분마다 사용자의 WorkSpaces 세션 연결이 끊깁니다.
- 사용자가 SAML 2.0 ID 공급자 (IdP) 에서 시작한 흐름을 사용하여 페더레이션할 때 리디렉션 URI 오류가 발생하거나 IdP로 페더레이션한 후 사용자가 클라이언트에서 로그인을 시도할 때마다 WorkSpaces 클라이언트 애플리케이션의 추가 인스턴스가 시작된다는 문제가 발생합니다.
- 사용자가 IdP에 페더레이션한 후 WorkSpaces 클라이언트 애플리케이션에 로그인하려고 하면 WorkSpace “문제가 발생했습니다: 시작하는 동안 오류가 발생했습니다.”라는 메시지를 받습니다.
- 사용자가 IdP에 페더레이션한 후 WorkSpaces 클라이언트 애플리케이션에 로그인하려고 하면 “태그를 검증할 수 없습니다.” 라는 메시지를 받습니다.
- 사용자가 '클라이언트와 서버가 공통 알고리즘을 가지고 있지 않기 때문에 통신할 수 없음'이라는 메시지를 받는 경우

- Windows에서 마이크 또는 웹캠이 작동하지 않습니다. WorkSpaces
- 내 사용자는 인증서 기반 인증을 사용하여 로그인할 수 없으며 데스크톱 세션에 연결할 때 WorkSpaces 클라이언트 또는 Windows 로그인 화면에서 암호를 입력하라는 메시지가 표시됩니다.
- Windows 설치 미디어가 필요하지만 제공하지 WorkSpaces 않는 작업을 하려고 합니다.
- 지원되지 않는 WorkSpaces 지역에서 생성된 기존 AWS 관리 디렉터리를 WorkSpaces 사용하여 시작하고 싶습니다.
- Amazon Linux 2에서 Firefox를 업데이트하고 싶은 경우
- 내 사용자는 에 구성된 세분화된 암호 정책 (FFGP) 설정을 무시하고 WorkSpaces 클라이언트를 사용하여 암호를 재설정할 수 있습니다. AWS Managed Microsoft AD
- 사용자가 웹 액세스를 사용하여 Windows/Linux에 액세스하려고 할 때 WorkSpace “이 OS/플랫폼은 사용자 시스템에 액세스할 권한이 없습니다”라는 오류 메시지를 받습니다. WorkSpace

사용자 이름에 잘못된 문자가 WorkSpace 있어서 Amazon Linux를 생성할 수 없습니다.

Amazon Linux의 WorkSpaces 경우 사용자 이름:

- 최대 20자를 포함할 수 있음
- UTF-8로 표현할 수 있는 문자, 공백 및 숫자를 포함할 수 있음
- 특수 문자(_.-#)를 포함할 수 있음
- 사용자 이름의 첫 문자로 대시 기호(-)를 사용할 수 없음

> **Note**
>
> 이러한 제한은 Windows에는 적용되지 않습니다 WorkSpaces. Windows는 사용자 이름의 모든 문자에 대해 @ 및 - 기호를 WorkSpaces 지원합니다.

Amazon WorkSpace Linux용 셸을 변경했는데 이제 PCoIP 세션을 프로비저닝할 수 없습니다.

WorkSpacesLinux용 기본 셸을 재정의하려면 을 참조하십시오. Amazon Linux용 기본 셸 재정의 WorkSpaces

내 아마존 리눅스가 WorkSpaces 시작되지 않아요

2020년 7월 20일부터 Amazon WorkSpaces Linux는 새 라이선스 인증서를 사용할 예정입니다. 이러한 새 인증서는 PCoIP 에이전트 2.14.1.1, 2.14.7, 2.14.9, 20.10.6 이상 버전과만 호환됩니다.

지원되지 않는 버전의 PCoIP 에이전트를 사용하는 경우 새 인증서와 호환되는 최신 수정 사항 및 성능 개선 사항이 포함된 최신 버전(20.10.6)으로 업그레이드해야 합니다. 7월 20일까지 이러한 업그레이드를 하지 않으면 Linux용 세션 프로비저닝이 실패하고 최종 사용자가 Linux에 연결할 수 없게 WorkSpaces 됩니다. WorkSpaces

PCoIP 에이전트를 최신 버전으로 업그레이드하는 방법

1. https://console.aws.amazon.com/workspaces/ 에서 WorkSpaces 콘솔을 여십시오.
2. 탐색 창에서 WorkSpaces를 선택합니다.
3. Linux를 선택하고 [액션] WorkSpace, [재부팅] 을 선택하여 WorkSpaces재부팅합니다. WorkSpace 상태가 인 경우 [작업]STOPPED, [WorkSpaces먼저 시작] 을 선택하고 상태가 AVAILABLE 될 때까지 기다려야 다시 부팅할 수 있습니다.
4. 를 WorkSpace 재부팅하고 상태가 AVAILABLE 인 후에는 이 업그레이드를 수행하는 ADMIN_MAINTENANCE 동안 상태를 WorkSpace 로 변경하는 것이 좋습니다. 작업을 마치면 의 WorkSpace 상태를 로 변경하십시오. AVAILABLE ADMIN_MAINTENANCE 모드에 대한 자세한 내용은 수동 유지 관리를 참조하세요.

   a의 상태를 WorkSpace To로 ADMIN_MAINTENANCE 변경하려면 다음과 같이 하십시오.

   a. 를 WorkSpace 선택하고 작업, 수정을 선택합니다 WorkSpace.
   b. Modify State(상태 수정)를 선택합니다.
   c. 예정 상태에서 ADMIN_MAINTENANCE를 선택합니다.
   d. 수정을 선택합니다.
5. SSH를 WorkSpace 통해 리눅스에 연결합니다. 자세한 정보는 리눅스용 SSH 연결 활성화 WorkSpaces을 참조하세요.
6. PCoIP 에이전트를 업데이트하려면 다음 명령을 실행합니다.

   ```
   sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
   ```
7. 에이전트 버전을 확인하고 업데이트가 성공했는지 확인하려면 다음 명령을 실행하세요.

   ```
   rpm -q pcoip-agent-standard
   ```

확인 명령은 다음과 같은 결과를 생성해야 합니다.

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. 연결을 WorkSpace 끊고 다시 부팅합니다.
9. 상태를 in으로 설정한 `ADMIN_MAINTENANCE` Step 4 경우 다시 WorkSpace Step 4 반복하여 의도 상태를 로 `AVAILABLE` 설정하십시오.

PCoIP 에이전트를 업그레이드한 후에도 WorkSpace 여전히 Linux가 시작되지 않으면 AWS Support에 문의하십시오.

연결된 WorkSpaces 디렉터리에서 시작하는 데 종종 실패합니다.

디렉터리에 연결할 때 지정한 각 서브넷에서 온프레미스 디렉터리의 두 DNS 서버 또는 도메인 컨트롤러에 액세스할 수 있는지 확인합니다. 두 DNS 서버의 IP 주소를 사용하여 각 서브넷에서 Amazon EC2 인스턴스를 시작하고 디렉터리에 인스턴스를 조인하여 이 연결을 확인할 수 있습니다.

내부 오류로 WorkSpaces 인해 시작이 실패합니다.

서브넷에서 시작된 인스턴스에 자동으로 IPv6 주소를 할당하도록 서브넷이 구성되었는지 확인합니다. 이 설정을 확인하려면 Amazon VPC 콘솔을 열고 서브넷을 선택한 다음 서브넷 작업, 자동 할당 IP 설정 수정을 선택합니다. 이 설정을 활성화하면 퍼포먼스 또는 그래픽 번들을 WorkSpaces 사용하여 시작할 수 없습니다. 이 설정을 비활성화하고 인스턴스를 시작할 때 수동으로 IPv6 주소를 지정하십시오.

디렉터리를 등록하려고 하면 등록이 실패하고 디렉터리가 오류 상태로 남는 경우

다중 지역 복제를 위해 구성된 AWS 관리형 Microsoft AD 디렉터리를 등록하려는 경우 이 문제가 발생할 수 있습니다. 기본 지역의 디렉터리를 WorkSpaces Amazon에서 사용할 수 있도록 성공적으로 등록할 수 있지만 복제된 지역에 디렉터리를 등록하려고 하면 실패합니다. AWS 관리형 Microsoft AD를 사용한 다중 지역 복제는 복제된 지역 WorkSpaces 내에서 Amazon에서 사용할 수 없습니다.

내 사용자는 대화형 로그온 배너가 WorkSpace 있는 Windows에 연결할 수 없습니다.

로그온 배너를 표시하도록 대화형 로그온 메시지를 구현한 경우 사용자가 Windows에 액세스할 수 없게 됩니다. WorkSpaces 에서는 현재 대화형 로그온 메시지 그룹 정책 설정이 지원되지 않습니다.

WorkSpaces Interactive logon: Message text for users attempting to log on그룹 정책이 적용되지 않는 조직 단위 (OU) 로 이동하십시오. WorkSpaces

내 사용자는 Windows에 연결할 수 없습니다. WorkSpace

사용자가 Windows에 연결하려고 하면 다음과 같은 오류 메시지가 나타납니다 WorkSpaces.

```
"An error occurred while launching your WorkSpace. Please try again."
```

이 오류는 PCoIP를 사용하여 Windows 데스크톱을 WorkSpace 로드할 수 없을 때 자주 발생합니다. 다음을 확인하세요.

- 이 메시지는 Windows용 PCoIP 표준 에이전트 서비스가 실행되고 있지 않은 경우에 나타납니다. RDP를 사용하여 연결하여 서비스가 실행 중인지, 서비스가 자동으로 시작되도록 설정되어 있는지, 관리 인터페이스(eth0)를 통해 통신할 수 있는지 확인합니다.

- PCoIP 에이전트가 제거된 경우 Amazon WorkSpaces 콘솔을 통해 WorkSpace 다시 부팅하면 에이전트가 자동으로 다시 설치됩니다.

- 아웃바운드 트래픽을 제한하도록 WorkSpaces보안 그룹을 수정한 경우 오랜 시간이 지난 후 Amazon WorkSpaces 클라이언트에서 이 오류가 표시될 수도 있습니다. 아웃바운드 트래픽을 제한하면 Windows가 로그인을 위해 디렉터리 컨트롤러와 통신할 수 없습니다. 보안 그룹이 기본 네트워크 인터페이스를 통해 필요한 모든 포트의 디렉터리 컨트롤러와 WorkSpaces 통신할 수 있도록 허용하는지 확인하십시오.

이 오류의 또 다른 원인은 사용자 권한 할당 그룹 정책과 관련이 있습니다. 다음 그룹 정책을 잘못 구성하면 사용자가 자신의 WorkSpaces Windows에 액세스할 수 없게 됩니다.

컴퓨터 구성\Windows 설정\보안 설정\로컬 정책\사용자 권한 할당

- 잘못된 정책:

  정책: 네트워크에서 이 컴퓨터 액세스

  설정: ### ##\도메인 컴퓨터

  최우선 GPO: 파일 액세스 허용
- 올바른 정책:

정책: 네트워크에서 이 컴퓨터 액세스

설정: ### ##\도메인 사용자

최우선 GPO: 파일 액세스 허용

> **Note**
>
> 이 정책 설정은 도메인 컴퓨터 대신 도메인 사용자에게 적용해야 합니다.

자세한 내용은 Microsoft Windows 설명서의 네트워크에서 이 컴퓨터 액세스 - 보안 정책 설정 및 보안 정책 설정 구성을 참조하십시오.

사용자가 WorkSpaces Web WorkSpaces Access에서 로그온하려고 할 때 문제가 발생했습니다.

WorkSpaces Amazon은 사용자가 웹 액세스 클라이언트에서 성공적으로 로그온할 수 있도록 특정 로그온 화면 구성을 사용합니다.

웹 액세스 사용자가 자신의 WorkSpaces 웹 액세스 사용자에 로그온할 수 있도록 하려면 그룹 정책 설정과 세 가지 보안 정책 설정을 구성해야 합니다. 이러한 설정을 올바르게 구성하지 않으면 사용자가 자신의 WorkSpaces 계정에 로그온하려고 할 때 로그온 시간이 길어지거나 화면이 검은색으로 표시될 수 있습니다. 이러한 설정을 구성하려면 Amazon WorkSpaces 웹 액세스 활성화 및 구성 단원을 참조하십시오.

> **Important**
>
> 2020년 10월 1일부터 고객은 더 이상 Amazon WorkSpaces Web Access 클라이언트를 사용하여 Windows 7 커스텀 WorkSpaces 또는 Windows 7 사용자 지정 라이선스 사용 (BYOL) 에 연결할 수 없습니다. WorkSpaces

Amazon WorkSpaces 클라이언트는 로그인 화면으로 돌아가기 전에 잠시 회색 “로드 중...” 화면을 표시합니다. 다른 오류 메시지는 나타나지 않습니다.

이 동작은 일반적으로 WorkSpaces 클라이언트가 포트 443을 통해 인증할 수 있지만 포트 4172 (PCoIP) 또는 포트 4195 (WSP) 를 통해 스트리밍 연결을 설정할 수 없음을 나타냅니다. 이러한 상황은 네트워크 사전 요구 사항이 충족되지 않을 때 발생할 수 있습니다. 클라이언트 측 문제로 인해 클라이언트의 네트워크 확인이 실패하는 경우가 자주 있습니다. 어떤 상태 확인이 실패하는지 확인하려면 네트워크 검사 아이콘(일반적으로 2.0+ 클라이언트의 경우 로그인 화면 오른쪽 하단 모서리에 느낌표가 있는 빨간색 삼각형, 3.0+ 클라이언트의 경우 오른쪽 상단 모서리에 있는 네트워크 아이콘

)

을 선택합니다.

> **Note**
>
> 이 문제의 가장 일반적인 원인은 포트 4172 또는 4195(TCP 및 UDP)를 통한 액세스를 차단하는 클라이언트 측 방화벽 또는 프록시입니다. 이 상태 확인에 실패하면 로컬 방화벽 설정을 확인합니다.

네트워크 검사를 통과하면 의 네트워크 구성에 문제가 있을 수 있습니다. WorkSpace 예를 들어 Windows 방화벽 규칙이 관리 인터페이스에서 포트 UDP 4172 또는 4195를 차단할 수 있습니다. RDP (원격 데스크톱 프로토콜) WorkSpace 를 사용하여 클라이언트에 연결하여 가 필요한 포트 요구 WorkSpace 사항을 충족하는지 확인합니다.

내 사용자에게 "WorkSpace 상태: 비정상” 메시지가 표시됩니다. 귀하의 WorkSpace 계정에 연결하지 못했습니다. 몇 분 후에 다시 시도하세요.'라는 오류 메시지가 표시되는 경우

이 오류는 일반적으로 SkyLightWorkSpacesConfigService 서비스가 상태 확인에 응답하지 않음을 나타냅니다.

방금 재부팅했거나 시작한 경우 몇 분 정도 기다린 다음 다시 시도하세요 WorkSpace.

실행한 지 얼마 되지 WorkSpace 않았는데도 이 오류가 계속 표시되면 RDP를 사용하여 연결하여 서비스가 제대로 작동하는지 확인하십시오. SkyLightWorkSpacesConfigService

- 실행 중

- 자동으로 시작되도록 설정됨
- 관리 인터페이스(eth0)를 통해 통신할 수 있음
- 타사 바이러스 백신 소프트웨어에 의해 차단되지 않음

내 사용자에게 “이 장치는 액세스 권한이 없습니다.” 라는 메시지가 표시됩니다. WorkSpace Please contact your administrator for assistance.(이 디바이스는 WorkSpace에 액세스할 수 있는 권한이 없습니다. 관리자에게 지원을 요청하십시오.)”라는 메시지가 표시됩니다.

이 오류는 WorkSpace 디렉터리에 IP 액세스 제어 그룹이 구성되어 있지만 클라이언트 IP 주소가 허용 목록에 포함되지 않았음을 나타냅니다.

디렉터리 설정을 확인합니다. 사용자가 연결하는 데 사용하는 공용 IP 주소가 에 대한 액세스를 허용하는지 확인하십시오. WorkSpace

사용자가 WSP WorkSpace에 연결하려고 할 때 '네트워크가 없습니다. 네트워크 연결이 끊어졌습니다. 네트워크 연결을 확인하거나 관리자에게 도움을 요청하세요.'라는 오류 메시지가 나타나는 경우 WSP에 연결하려고 할 때 WorkSpace

이 오류가 발생하고 사용자에게 연결 문제가 없는 경우 네트워크 방화벽에서 포트 4195가 열려 있는지 확인하세요. WorkSpaces 스트리밍 프로토콜 (WSP) WorkSpaces 사용을 위해 클라이언트 세션을 스트리밍하는 데 사용되는 포트가 4172에서 4195로 변경되었습니다.

WorkSpaces 클라이언트에서 사용자에게 네트워크 오류가 발생하지만 사용자는 자신의 장치에서 다른 네트워크 지원 앱을 사용할 수 있습니다.

WorkSpaces 클라이언트 애플리케이션은 AWS클라우드의 리소스에 대한 액세스를 사용하며 최소 1Mbps의 다운로드 대역폭을 제공하는 연결이 필요합니다. 기기가 네트워크에 간헐적으로 연결되는 경우 WorkSpaces 클라이언트 애플리케이션이 네트워크 문제를 보고할 수 있습니다.

WorkSpaces 2018년 5월부터 아마존 트러스트 서비스에서 발급한 디지털 인증서를 사용하도록 시행합니다. Amazon Trust Services는 에서 지원하는 운영 체제에서 이미 신뢰할 수 있는 루트

WorkSpaces CA입니다. 운영 체제의 루트 CA 목록이 최신 상태가 아닌 경우 디바이스를 연결할 WorkSpaces 수 없고 클라이언트에서 네트워크 오류가 발생합니다.

인증서 실패로 인한 연결 문제를 인식하려면

- PCoIP 제로 클라이언트 - 다음 오류 메시지가 표시됩니다.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- 기타 클라이언트 - 상태 확인이 실패하고 인터넷에 대해 삼각형의 빨간색 경고가 표시됩니다.

인증서 실패를 해결하려면

- Windows 클라이언트 애플리케이션
- PCoIP 제로 클라이언트
- 기타 클라이언트 애플리케이션

Windows 클라이언트 애플리케이션

인증서 실패에 대한 다음 솔루션 중 하나를 사용합니다.

솔루션 1: 클라이언트 애플리케이션 업데이트

https://clients.amazonworkspaces.com/ 에서 최신 Windows 클라이언트 애플리케이션을 다운로드하여 설치합니다. us-iso-eastworkspaces-client-updates-dcaus-isob-eastworkspaces-client-updates-lck 설치하는 동안 클라이언트 애플리케이션에서는 운영 체제가 Amazon Trust Services에서 발급한 인증서를 신뢰할 수 있도록 보장합니다.

솔루션 2: 로컬 루트 CA 목록에 Amazon Trust Services 추가

1. https://www.amazontrust.com/repository/를 엽니다.
2. DER 형식의 Starfield 인증서를 다운로드합니다 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Microsoft Management Console을 엽니다. (명령 프롬프트에서 mmc를 실행합니다.)
4. 파일, Add/Remove Snap-in(스냅인 추가/제거), 인증서, 추가를 선택합니다.

5. Certificates snap-in(인증서 스냅인) 페이지에서 Computer account(컴퓨터 계정)를 선택한 후 다음을 선택합니다. 기본값인 Local computer(로컬 컴퓨터)를 유지합니다. 마침을 클릭합니다. 확인을 선택합니다.
6. Certificates (Local Computer)(인증서(로컬 컴퓨터))를 확장하고 Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)를 선택합니다. 작업, All Tasks(모든 작업), 가져오기를 선택합니다.
7. 마법사가 안내하는 대로 다운로드한 인증서를 가져옵니다.
8. 클라이언트 애플리케이션을 종료하고 다시 시작합니다. WorkSpaces

솔루션 3: 그룹 정책을 사용하여 Amazon Trust Services를 신뢰할 수 있는 CA로 배포

그룹 정책을 사용하여 도메인에 대한 신뢰할 수 있는 루트 CA에 Starfield 인증서를 추가합니다. 자세한 내용은 Use Policy to Distribute Certificates를 참조하십시오.

PCoIP 제로 클라이언트

WorkSpace 사용 중인 펌웨어 버전 6.0 이상에 직접 연결하려면 Amazon Trust Services에서 발급한 인증서를 다운로드하여 설치하십시오.

Amazon Trust Services를 신뢰할 수 있는 루트 CA로 추가하려면

1. https://certs.secureserver.net/repository/를 엽니다.
2. Starfield 인증서 체인에서 지문 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58이 있는 인증서를 다운로드합니다.
3. 제로 클라이언트에 인증서를 업로드합니다. 자세한 내용은 Teradici 설명서의 Uploading Certificates를 참조하십시오.

기타 클라이언트 애플리케이션

Amazon Trust Services에서 Starfield 인증서 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)를 추가합니다. 루트 CA 추가 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- Android: 인증서 추가 및 삭제
- Chrome OS: Chrome 기기에서 클라이언트 인증서 관리
- macOS 및 iOS: 테스트 디바이스에 CA의 루트 인증서 설치

WorkSpace 사용자에게 다음과 같은 오류 메시지가 표시됩니다. “디바이스를 등록 서비스에 연결할 수 없습니다. Check your network settings.(디바이스에서 등록 서비스에 연결할 수 없습니다. 네트워크 설정을 확인하십시오.)"라는 오류 메시지가 표시됩니다.

등록 서비스에 장애가 발생하면 WorkSpace 사용자에게 Connection Health Check 페이지에 다음과 같은 오류 메시지가 표시될 수 있습니다. “장치를 WorkSpaces 등록 서비스에 연결할 수 없습니다. 장치를 등록할 수 없습니다 WorkSpaces. 네트워크 설정을 확인하십시오."

이 오류는 WorkSpaces 클라이언트 애플리케이션이 등록 서비스에 연결할 수 없을 때 발생합니다. 일반적으로 이 오류는 WorkSpaces 디렉터리가 삭제되었을 때 발생합니다. 이 오류를 해결하려면 등록 코드가 유효하고 AWS 클라우드에서 실행 중인 디렉터리에 해당하는지 확인하세요.

PCoIP 제로 클라이언트 사용자에게 “The supplied certificate is invalid due to timestamp.(제공된 인증서가 타임스탬프로 인해 유효하지 않습니다.)”라는 오류 메시지가 표시되는 경우

Teradici에서 NTP(Network Time Protocol)가 활성화되지 않은 경우 PCoIP 제로 클라이언트 사용자에게 인증서 실패 오류가 표시될 수 있습니다. NTP를 설정하려면 WorkSpaces용 PCoIP 제로 클라이언트 설정 단원을 참조하십시오.

USB 프린터 및 기타 USB 주변 디바이스가 PCoIP 제로 클라이언트에서 작동하지 않는 경우

Amazon은 PCoIP 에이전트 버전 20.10.4부터 Windows 레지스트리를 통해 USB 리디렉션을 기본적으로 WorkSpaces 비활성화합니다. 이 레지스트리 설정은 사용자가 PCoIP 제로 클라이언트 디바이스를 사용하여 USB 주변 기기에 연결할 때 USB 주변 기기의 동작에 영향을 줍니다. WorkSpaces

PCoIP 에이전트 버전 20.10.4 이상을 사용하는 경우 USB 리디렉션을 WorkSpaces 사용하도록 설정하기 전까지는 USB 주변 장치가 PCoIP 제로 클라이언트 장치와 작동하지 않습니다.

> **Note**
>
> 32비트 가상 프린터 드라이버를 사용하는 경우 해당 드라이버도 64비트 버전으로 업데이트해야 합니다.

PCoIP 제로 클라이언트 디바이스의 USB 리디렉션을 활성화하는 방법

그룹 정책을 통해 이러한 레지스트리 변경 내용을 자신에게 적용하는 것이 좋습니다. WorkSpaces 자세한 내용은 Teradici 설명서의 Configuring the agent 및 Configurable settings를 참조하세요.

1. 다음 레지스트리 키 값을 1(사용)로 설정합니다.

   KeyPath = HKEY_LOCAL_MACHINE\ 소프트웨어\ 정책\ 테라디치\ PCoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = 디워드

   KeyValue = 1
2. 다음 레지스트리 키 값을 1(사용)로 설정합니다.

   KeyPath = HKEY_LOCAL_MACHINE\ 소프트웨어\ 정책\ 테라디치\ PCoIP\ pcoip_admin_defaults

   KeyName = pcopip.enable_usb

   KeyType = 디워드

   KeyValue = 1
3. 아직 로그인하지 않았다면 에서 로그아웃한 WorkSpace 다음 다시 로그인하십시오. 이제 USB 디바이스가 작동할 것입니다.

사용자가 Windows 또는 macOS 클라이언트 애플리케이션 업데이트를 건너뛰었고 최신 버전을 설치하라는 메시지가 표시되지 않습니다.

사용자가 Amazon WorkSpaces Windows 클라이언트 애플리케이션에 대한 업데이트를 건너뛰면 SkipThisVersion레지스트리 키가 설정되고 새 버전의 클라이언트가 출시될 때 클라이언트를 업데이트하라는 메시지가 더 이상 표시되지 않습니다. 최신 버전으로 업데이트하려면 Amazon 사용 WorkSpaces 설명서의 WorkSpaces Windows 클라이언트 애플리케이션을 최신 버전으로 업데이트에 설명된 대로 레지스트리를 편집하면 됩니다. 다음 PowerShell 명령을 실행할 수도 있습니다.

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

사용자가 Amazon WorkSpaces macOS 클라이언트 애플리케이션에 대한 업데이트를 건너뛰면 기본 설정이 지정되고 새 버전의 클라이언트가 출시될 때 클라이언트를 업데이트하라는 메시지가 더 이상 표시되지 않습니다. `SUSkippedVersion` 최신 버전으로 업데이트하려면 Amazon WorkSpaces User Guide의 WorkSpaces macOS 클라이언트 애플리케이션을 최신 버전으로 업데이트하는 방법에 설명된 대로 이 기본 설정을 재설정할 수 있습니다.

사용자는 Chromebook에서 Android 클라이언트 애플리케이션을 설치할 수 없습니다.

버전 2.4.13은 Amazon WorkSpaces 크롬북 클라이언트 애플리케이션의 최종 릴리스입니다. Google이 Chrome 앱에 대한 지원을 단계적으로 중단하고 있기 때문에 WorkSpaces Chromebook 클라이언트 애플리케이션에 대한 추가 업데이트는 없을 것이며 사용도 지원되지 않습니다.

Android 애플리케이션 설치를 지원하는 Chromebook의 경우 Android 클라이언트 애플리케이션을 대신 사용하는 것이 좋습니다. WorkSpaces

경우에 따라 사용자의 Chromebook이 Android 애플리케이션을 설치해야 할 수 있습니다. 자세한 정보는 Chromebook을 위한 Android 설정을 참조하세요.

사용자에게 초대 이메일 또는 암호 재설정 이메일이 수신되지 않습니다.

AD Connector 또는 신뢰할 수 있는 도메인을 사용하여 만든 환영 이메일이나 암호 재설정 이메일은 사용자에게 자동으로 전송되지 않습니다. WorkSpaces 사용자가 이미 Active Directory에 있는 경우에도 초대 이메일이 자동으로 전송되지 않습니다.

이러한 사용자에게 환영 이메일을 수동으로 발송하려면 초대 이메일 전송 단원을 참조하십시오.

사용자 암호를 재설정하려면 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

사용자에게 클라이언트 로그인 화면의 암호 찾기 옵션이 표시되지 않습니다.

AD Connector 또는 신뢰할 수 있는 도메인을 사용하는 경우 사용자가 자신의 암호를 재설정할 수 없습니다. (비밀번호를 잊으셨나요? WorkSpaces 클라이언트 애플리케이션 로그인 화면의 옵션을 사용할 수 없습니다. 사용자 암호를 재설정하는 방법에 대한 자세한 내용은 WorkSpaces용 Active Directory 관리 도구 설정 단원을 참조하십시오.

Windows에 응용 프로그램을 설치하려고 하면 “시스템 관리자가 이 설치를 금지하도록 정책을 설정했습니다.” 라는 메시지가 나타납니다. WorkSpace

Windows Installer 그룹 정책 설정을 수정하여 이 문제를 해결할 수 있습니다. 이 정책을 디렉터리의 여러 WorkSpaces 곳에 배포하려면 도메인에 가입된 EC2 인스턴스에서 OU (WorkSpaces 조직 구성 단위) 에 연결된 그룹 정책 개체에 이 설정을 적용하십시오. AD Connector를 사용하는 경우 도메인 컨트롤러에서 이렇게 변경할 수 있습니다. Active Directory 관리 도구를 사용하여 그룹 정책 개체를 처리하는 방법에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 Active Directory 관리 도구 설치를 참조하세요.

다음 절차는 그룹 정책 개체에 대한 Windows Installer 설정을 구성하는 방법을 보여줍니다. WorkSpaces

1. 도메인에 가장 최근의 WorkSpaces 그룹 정책 관리 템플릿이 설치되어 있는지 확인하십시오.
2. Windows WorkSpace 클라이언트에서 그룹 정책 관리 도구를 열고 WorkSpaces 컴퓨터 계정의 WorkSpaces 그룹 정책 개체로 이동하여 선택합니다. 주 메뉴에서 [Action], [Edit]를 선택합니다.
3. 그룹 정책 관리 편집기에서 Computer Configuration(컴퓨터 구성), Policies(정책), Administrative Templates(관리 템플릿), Classic Administrative Templates(클래식 관리 템플릿), Windows Components(Windows 구성 요소), Windows Installer를 선택합니다.
4. Turn Off Windows Installer(Windows Installer 끄기) 설정을 엽니다.
5. Turn Off Windows Installer(Windows Installer 끄기) 대화 상자에서 Not Configured(구성되지 않음)를 Enabled(활성)로 변경한 다음 Disable Windows Installer(Windows Installer 비활성화)를 Never(없음)로 설정합니다.
6. 확인을 선택합니다.
7. 그룹 정책 변경 사항을 적용하려면 다음 중 하나를 수행합니다.
   - 를 다시 부팅합니다 WorkSpace (WorkSpaces 콘솔에서 를 선택한 다음 작업 WorkSpace, 재부팅을 선택합니다 WorkSpaces).
   - 관리 명령 프롬프트에서 gpupdate /force를 입력합니다.

내 디렉터리에서 인터넷에 연결할 수 없습니다 WorkSpaces .

WorkSpaces 기본적으로 인터넷과 통신할 수 없습니다. 인터넷 액세스를 명시적으로 제공해야 합니다. 자세한 정보는 귀하의 인터넷 액세스 제공 WorkSpace을 참조하세요.

WorkSpace My의 인터넷 연결이 끊겼습니다.

인터넷에 액세스할 수 WorkSpace 없고 RDP를 사용하여 연결할 수 없는 경우 이 문제는 공용 IP 주소가 손실되었기 때문일 수 있습니다. WorkSpace WorkSpace 디렉터리 수준에서 엘라스틱 IP 주소 자동 할당을 활성화한 경우, 시작 시 엘라스틱 IP 주소 (Amazon 제공 풀) 가 사용자에게 할당됩니다. WorkSpace 하지만 소유한 엘라스틱 IP 주소를 에 연결한 WorkSpace 다음 나중에 해당 엘라스틱 IP 주소를 에서 분리하면 퍼블릭 IP 주소가 WorkSpace 손실되고 Amazon 제공 풀에서 새 주소를 자동으로 가져오지 않습니다. WorkSpace

Amazon에서 제공한 풀의 새 퍼블릭 IP 주소를 와 연결하려면 를 WorkSpace 재구축해야 합니다. WorkSpace 를 다시 빌드하지 않으려면 소유한 WorkSpace 다른 엘라스틱 IP 주소를 에 연결해야 합니다. WorkSpace

를 시작한 WorkSpace 후에는 a의 Elastic network 인터페이스를 수정하지 않는 WorkSpace 것이 좋습니다. 엘라스틱 IP 주소가 WorkSpace a에 할당된 후에는 동일한 퍼블릭 IP 주소를 WorkSpace 유지합니다. 단, 다시 빌드하여 새 퍼블릭 IP 주소를 갖게 됩니다. WorkSpace

온프레미스 디렉터리에 연결할 때 "DNS unavailable" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음과 비슷한 오류 메시지가 표시됩니다.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector에서 포트 53을 통해 TCP 및 UDP를 경유하여 온프레미스 DNS 서버와 통신할 수 있어야 합니다. 보안 그룹 및 온프레미스 방화벽에서 이 포트를 통한 TCP 및 UDP 통신을 허용하는지 확인합니다.

내 온프레미스 디렉터리에 연결할 때 "Connectivity issues detected" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음과 비슷한 오류 메시지가 표시됩니다.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector에서 다음 포트를 통해 TCP 및 UDP를 경유하여 온프레미스 도메인 컨트롤러와 통신할 수 있어야 합니다. 보안 그룹 및 온프레미스 방화벽에서 이러한 포트를 통한 TCP 및 UDP 통신을 허용하는지 확인합니다.

- 88(Kerberos)
- 389(LDAP)

내 온프레미스 디렉터리에 연결할 때 "SRV record" 오류가 표시되는 경우

온프레미스 디렉터리에 연결할 때 다음 중 하나 이상과 비슷한 오류 메시지가 표시됩니다.

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

디렉터리에 연결할 때 AD Connector에서 `_ldap._tcp.`*dns-domain-name* 및 `_kerberos._tcp.`*dns-domain-name* SRV 레코드를 가져와야 합니다. 서비스에서 디렉터리에 연결할 때 지정한 DNS 서버에서 이러한 레코드를 가져올 수 없는 경우에 이 오류가 표시됩니다. DNS 서버에 이러한 SRV 레코드가 포함되어 있는지 확인합니다. 자세한 내용은 TechNet Microsoft의 SRV 리소스 레코드를 참조하십시오.

Windows가 WorkSpace 유휴 상태로 남아 있으면 절전 모드로 전환됩니다.

이 문제를 해결하려면 에 연결하고 다음 절차를 사용하여 전원 관리 옵션을 고성능으로 변경하십시오. WorkSpace

1. 에서 제어판을 연 다음 하드웨어를 선택하거나 하드웨어 및 사운드를 선택합니다 (이름은 Windows 버전에 따라 다를 수 있음). WorkSpace
2. Power Options(전원 옵션)에서 Choose a power plan(전원 계획 선택)을 선택합니다.
3. 전원 계획 선택 또는 사용자 지정 창에서 고성능 전원 계획을 선택한 후 계획 설정 변경을 선택합니다.
   - 고성능 전원 계획을 선택하는 옵션이 비활성화된 경우 현재 사용할 수 없는 설정 변경을 선택한 다음 고성능 전원 계획을 선택합니다.
   - 고성능 계획이 보이지 않는 경우, 추가 계획 표시의 오른쪽에 있는 화살표를 선택하여 표시하거나, 왼쪽 탐색 영역에서 전원 계획 생성을 선택한 후 고성능을 선택하고 전원 계획에 이름을 지정한 후 다음을 선택합니다.
4. 계획 설정 변경: 고성능 페이지에서 디스플레이 끄기 및 컴퓨터 절전 모드로 전환(가능한 경우)이 안 함으로 설정되어 있는지 확인합니다.
5. 고성능 요금제를 변경한 경우 변경 사항 저장을 선택하고, 새 요금제를 만들려면 경우 생성을 선택합니다.

앞에 나온 단계에서 문제가 해결되지 않으면 다음을 수행합니다.

1. 에서 제어판을 연 다음 하드웨어를 선택하거나 하드웨어 및 사운드를 선택합니다 (이름은 Windows 버전에 따라 다를 수 있음). WorkSpace
2. Power Options(전원 옵션)에서 Choose a power plan(전원 계획 선택)을 선택합니다.
3. 전원 계획 선택 또는 사용자 지정 창에서 고성능 전원 계획 오른쪽에 있는 계획 설정 변경 링크를 선택한 다음 고급 전원 설정 변경 링크를 선택합니다.
4. Power Options(전원 옵션) 대화 상자의 설정 목록에서 Hard disk(하드 디스크) 왼쪽의 더하기 기호를 선택하여 관련 설정을 표시합니다.
5. 전원 연결 후 하드 디스크 끄기 값이 배터리 전원 켜기 값보다 큰지 확인하십시오 (기본값은 20분).
6. PCI Express 왼쪽의 더하기 기호를 선택하고, Link State Power Management(링크 상태 전원 관리)에도 똑같이 합니다.
7. Link State Power Management(링크 상태 전원 관리) 설정이 해제인지 확인합니다.
8. 확인(또는 설정을 변경한 경우 적용)을 선택하고 대화 상자를 닫습니다.
9. 설정을 변경한 경우 Change settings for the plan(계획 설정 변경) 창에서 변경 사항 저장을 선택합니다.

제 중 한 명이 WorkSpaces 다음과 같은 상태입니다. **UNHEALTHY**

이 WorkSpaces 서비스는 주기적으로 a에 상태 요청을 보냅니다 WorkSpace. WorkSpaceA가 이러한 요청에 응답하지 못하면 A로 표시됩니다UNHEALTHY. 이 문제의 일반적인 원인은 다음과 같습니다.

- 의 WorkSpace 애플리케이션이 네트워크 포트를 차단하여 상태 요청에 응답할 수 없습니다. WorkSpace
- CPU 사용률이 높으면 상태 요청에 적시에 응답할 수 없습니다. WorkSpace
- 의 컴퓨터 이름이 WorkSpace 변경되었습니다. 이렇게 하면 WorkSpaces 와 사이에 보안 채널이 설정되지 WorkSpace 않습니다.

다음과 같은 방법으로 상황을 해결할 수 있습니다.

- WorkSpace WorkSpaces 콘솔에서 를 재부팅합니다.
- 다음 절차를 WorkSpace 사용하여 비정상에 연결하십시오. 이 절차는 문제 해결 목적으로만 사용해야 합니다.

  1. WorkSpace비정상과 동일한 WorkSpace 디렉토리의 운영 체제에 연결합니다.

2. 작동 WorkSpace 상태에서 원격 데스크톱 프로토콜 (RDP) 을 사용하여 비정상 IP 주소를 WorkSpace 사용하여 비정상에 연결합니다. WorkSpace 문제의 정도에 따라 비정상 네트워크에 연결하지 못할 수도 있습니다. WorkSpace
3. 비정상 상태인 WorkSpace 경우 최소 포트 요구 사항이 충족되는지 확인하십시오.

- SkyLightWorkSpacesConfigService 서비스가 상태 확인에 응답할 수 있는지 확인하십시오. 이 문제를 해결하려면 내 사용자에게 "WorkSpace 상태: 비정상" 메시지가 표시됩니다. 귀하의 WorkSpace 계정에 연결하지 못했습니다. 몇 분 후에 다시 시도하세요.'라는 오류 메시지가 표시되는 경우 섹션을 참조하세요.
- WorkSpace WorkSpaces 콘솔에서 다시 빌드하세요. 를 다시 빌드하면 데이터가 손실될 WorkSpace 수 있으므로 이 옵션은 다른 모든 문제 해결 시도가 실패한 경우에만 사용해야 합니다.

내 WorkSpace 것이 예기치 않게 충돌하거나 재부팅됩니다.

WorkSpace 구성된 PCoIP가 반복적으로 충돌하거나 재부팅되고 오류 로그 또는 크래시 덤프가 문제를 가리키거나 하는 경우, 또는 다음과 같은 오류 메시지가 표시되는 경우`spacedeskHookUmode.dll`, 다음에 대한 웹 액세스를 비활성화해야 할 수 있습니다. `spacedeskHookKmode.sys` WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - 이러한 문제 해결 단계는 스트리밍 프로토콜 (WSP) 용으로 구성된 단계에는 적용되지 않습니다. WorkSpaces WorkSpaces 이 지침은 PCoIP용으로 구성된 경우에만 적용됩니다 WorkSpaces .
> - 사용자가 웹 액세스를 사용하도록 허용하지 않는 경우에만 웹 액세스를 비활성화해야 합니다.

에 대한 웹 액세스를 사용하지 않도록 설정하려면 WorkSpaces 디렉터리에서 웹 액세스를 사용하지 않도록 설정하고 를 다시 부팅해야 합니다. WorkSpace WorkSpace

동일한 사용자 이름이 두 개 이상 WorkSpace 있지만 사용자는 다음 중 하나에만 로그인할 수 있습니다. WorkSpaces

Active Directory (AD) 에서 사용자를 먼저 삭제하지 않고 삭제한 다음 해당 WorkSpace 사용자를 Active Directory에 다시 추가하고 해당 WorkSpace 사용자에 대해 새 사용자를 만들면 동일한 디렉터리에 동일한 사용자 이름이 두 개 WorkSpaces 있게 됩니다. 하지만 사용자가 원래 계정에 연결하려고 WorkSpace 하면 다음과 같은 오류 메시지가 나타납니다.

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

또한 Amazon WorkSpaces 콘솔에서 사용자 이름을 검색하면 두 사용자 이름이 모두 WorkSpaces 존재하더라도 새 WorkSpace 이름만 반환됩니다. (사용자 이름 대신 WorkSpace ID를 WorkSpace 검색하면 원본을 찾을 수 있습니다.)

Active Directory에서 사용자 이름을 먼저 삭제하지 않고 이름을 바꾸는 경우에도 이 동작이 발생할 수 있습니다 WorkSpace. 그런 다음 사용자 이름을 원래 사용자 이름으로 다시 변경하고 해당 사용자의 사용자 이름을 새로 WorkSpace 만들면 디렉터리에 동일한 사용자 이름이 두 개 WorkSpaces 있게 됩니다.

Active Directory는 사용자 이름이 아니라 사용자의 보안 식별자(SID)를 사용하여 사용자를 고유하게 식별하기 때문에 이 문제가 발생합니다. 사용자를 삭제하고 Active Directory에서 사용자를 다시 생성하면 사용자 이름이 동일하게 유지되더라도 사용자에게 새 SID가 할당됩니다. Amazon WorkSpaces 콘솔은 사용자 이름을 검색하는 동안 SID를 사용하여 Active Directory에서 일치하는 사용자 이름을 검색합니다. 또한 Amazon WorkSpaces 클라이언트는 사용자가 연결할 때 SID를 사용하여 사용자를 식별합니다 WorkSpaces.

이 문제를 해결하려면 다음 중 하나를 수행하십시오.

- 사용자가 삭제되고 Active Directory에서 다시 생성되었기 때문에 이 문제가 발생한 경우, Active Directory의 휴지통 기능을 활성화했다면 원래의 삭제된 사용자 객체를 복원할 수도 있습니다. 원래 사용자 객체를 복원할 수 있는 경우 사용자가 WorkSpace 원본에 연결할 수 있는지 확인하십시오. 가능하면 사용자 데이터를 수동으로 백업하고 새 데이터에서 원래 데이터로 전송한 WorkSpace 후 WorkSpace (필요한 경우) 새 WorkSpace 데이터를 삭제할 수 있습니다.
- 원래 사용자 개체를 복원할 수 없는 경우 사용자의 원본을 WorkSpace 삭제하십시오. 사용자는 새 객체에 연결하여 새 계정을 WorkSpace 대신 사용할 수 있어야 합니다. 모든 사용자 데이터를 원본에서 새 데이터로 수동으로 백업하고 WorkSpace 전송해야 WorkSpace 합니다.

> **Warning**
>
> WorkSpace 삭제는 영구적인 작업이며 취소할 수 없습니다. WorkSpace 사용자 데이터는 유지되지 않고 파기됩니다. 사용자 데이터를 백업하는 데 도움이 필요한 경우 AWS Support에 문의하세요.

Amazon에서 Docker를 사용하는 데 문제가 있습니다. WorkSpaces

윈도우 WorkSpaces

Windows에서는 중첩된 가상화 (Docker 사용 포함) 가 지원되지 않습니다. WorkSpaces 자세한 내용은 Docker 설명서를 참조하세요.

리눅스 WorkSpaces

WorkSpacesLinux에서 Docker를 사용하려면 Docker에서 사용하는 CIDR 블록이 관련 두 개의 ENI (엘라스틱 네트워크 인터페이스) 에 사용되는 CIDR 블록과 겹치지 않도록 해야 합니다. WorkSpace Linux에서 Docker를 사용할 때 문제가 발생하는 경우 Docker에 문의하여 도움을 받으세요. WorkSpaces

일부 API ThrottlingException 호출에서 오류가 발생합니다.

API 호출의 기본 허용 속도는 초당 WorkSpaces API 호출 2회의 일정한 비율이며, 허용되는 최대 “버스트” 속도는 초당 5회의 API 호출입니다. 다음 표에서는 API 요청에 대해 버스트 속도 제한이 작동하는 방식을 보여줍니다.

초	전송된 요청 수	허용된 순 요청 수	Details
1	0	5	첫 번째 초(second 1) 동안 5회 요청이 허용되며, 초당 호출 5회의 최대 버스트 속도까지 허용됩니다.
2	2	5	왜냐하면 2회 이하의 호출은 second 1에서 발급되었기 때문에 호출 5회의 전체 버스트 용량이 여전히 사용 가능합니다.

초	전송된 요청 수	허용된 순 요청 수	Details
3	5	5	왜냐하면 2회 호출만 second 2에서 발급되었기 때문에 호출 5회의 전체 버스트 용량이 여전히 사용 가능합니다.
4	2	2	전체 버스트 용량이 second 3에서 사용되었기 때문에 초당 호출 2회의 일정한 속도만 사용 가능합니다.
5	3	2	남아 있는 버스트 용량이 없기 때문에 지금은 호출이 2회만 허용됩니다. 따라서 3회의 API 호출 중 한 건은 정체됩니다. 정체된 한 건의 호출은 잠시 후에 응답합니다.
6	0	1	second 5에서의 호출 중 한 건이 second 6에서 재시도 중이기 때문에 초당 호출 2회의 일정한 속도 제한으로 인해 second 6에는 단 한 건의 추가 호출에 대한 용량이 있습니다.
7	0	3	대기열에 더 이상 정체된 API 호출이 없으므로 속도 제한은 호출 5회의 버스트 속도 제한까지 계속 증가합니다.
8	0	5	second 7에서 발급된 호출이 없기 때문에 최대 요청 수가 허용됩니다.
9	0	5	second 8에서 발급된 호출이 없더라도 속도 제한은 5회 이상으로 증가하지 않습니다.

백그라운드에서 실행하도록 놔두면 WorkSpace 계속 연결이 끊깁니다.

Mac 사용자의 경우 Power Nap 기능이 켜져 있는지 확인하세요. 켜져 있는 경우 클릭하여 끕니다. Power Nap을 끄려면 터미널을 열고 다음 명령을 실행합니다.

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 페더레이션 기능이 작동하지 않고 내 사용자는 WorkSpaces 데스크톱을 스트리밍할 권한이 없어요.

이 상황은 SAML 2.0 페더레이션 IAM 역할에 대해 포함되는 인라인 정책이 디렉터리 Amazon 리소스 이름(ARN)에서 스트리밍할 권한을 포함하지 않기 때문에 발생할 수 있습니다. IAM 역할은 디렉터리에 액세스하는 연동 사용자가 맡습니다. WorkSpaces 디렉터리 ARN을 포함하도록 역할 권한을 편집하고 사용자가 디렉터리에 ARN을 WorkSpace 가지고 있는지 확인하십시오. 자세한 내용은 SAML 2.0 인증 및 SAML 2.0 페더레이션 문제 해결을 참조하십시오. AWS

60분마다 사용자의 WorkSpaces 세션 연결이 끊깁니다.

ID 공급자 (IdP) 에 따라 SAML 2.0 인증을 구성한 경우 IdP가 인증 응답의 일부로 SAML 속성으로 전달하는 정보를 구성해야 AWS 할 수 있습니다. WorkSpaces 여기에는 `SessionDuration` 속성이 `https://aws.amazon.com/SAML/Attributes/SessionDuration`으로 설정된 속성 요소를 구성하는 것도 포함됩니다.

`SessionDuration`은 재인증이 필요하기 전에 사용자의 페더레이션 스트리밍 세션이 활성 상태로 유지될 수 있는 최대 시간을 지정합니다. `SessionDuration`은 선택적 속성이지만 SAML 인증 응답에 포함시키는 것이 좋습니다. 이 속성을 지정하지 않으면 세션 기간은 기본값인 60분으로 설정됩니다.

이 문제를 해결하려면 SAML 인증 응답에 `SessionDuration` 값을 포함하도록 IdP를 구성하고 필요에 따라 값을 설정합니다. 자세한 내용은 5단계: SAML 인증 응답을 위한 어설션 생성을 참조하세요.

사용자가 SAML 2.0 ID 공급자 (IdP) 에서 시작한 흐름을 사용하여 페더레이션할 때 리디렉션 URI 오류가 발생하거나 IdP로 페더레이션한 후 사용자가 클라이언트에서 로그인을 시도할 때마다 WorkSpaces 클라이언트 애플리케이션의 추가 인스턴스가 시작된다는 문제가 발생합니다.

이 오류는 유효하지 않은 릴레이 상태 URL로 인해 발생합니다. 디렉터리 속성에서 IdP 페더레이션 설정의 릴레이 상태가 올바른지, 사용자 액세스 URL 및 릴레이 상태 매개변수 이름이 IdP 페더레이션에 맞게 구성되었는지 확인합니다. WorkSpaces 유효하지만 문제가 지속되면 AWS Support에 문의하십시오. 자세한 내용은 SAML 설정을 참조하세요.

사용자가 IdP에 페더레이션한 후 WorkSpaces 클라이언트 애플리케이션에 로그인하려고 하면 WorkSpace “문제가 발생했습니다: 시작하는 동안 오류가 발생했습니다.”라는 메시지를 받습니다.

페더레이션에 대한 SAML 2.0 어설션을 검토하세요. SAML 주체 NameID 값은 사용자 이름과 WorkSpaces 일치해야 하며, 일반적으로 Active Directory 사용자의 AccountName SaM 속성과 동일합니다. 또한 속성이 로 설정된 **`PrincipalTag:Email`**속성 요소는 디렉터리에 정의된 WorkSpaces 사용자의 이메일 주소와 `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` 일치해야 합니다. WorkSpaces 자세한 내용은 SAML 설정을 참조하세요.

사용자가 IdP에 페더레이션한 후 WorkSpaces 클라이언트 애플리케이션에 로그인하려고 하면 “태그를 검증할 수 없습니다.” 라는 메시지를 받습니다.

페더레이션에 대한 SAML 2.0 어설션의 `PrincipalTag` 속성 값(예: `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`)을 검토하세요. 태그 값에는 `_ . : / = + - @`, 문자, 숫자 및 공백의 조합이 포함될 수 있습니다. 자세한 내용은 IAM 및 태깅 규칙을 참조하십시오. AWS STS

사용자가 '클라이언트와 서버가 공통 알고리즘을 가지고 있지 않기 때문에 통신할 수 없음'이라는 메시지를 받는 경우

TLS 1.2를 활성화하지 않으면 이 문제가 발생할 수 있습니다.

Windows에서 마이크 또는 웹캠이 작동하지 않습니다. WorkSpaces

시작 메뉴를 열어 개인 정보 설정을 확인하세요.

- 시작 > 설정 > 개인 정보 보호 > 카메라
- 시작 > 설정 > 개인 정보 보호 > 마이크

꺼져 있으면 켜세요.

또는 WorkSpaces 관리자가 필요에 따라 마이크 및/또는 웹캠을 활성화하는 그룹 정책 개체 (GPO) 를 만들 수도 있습니다.

내 사용자는 인증서 기반 인증을 사용하여 로그인할 수 없으며 데스크톱 세션에 연결할 때 WorkSpaces 클라이언트 또는 Windows 로그인 화면에서 암호를 입력하라는 메시지가 표시됩니다.

세션에서 인증서 기반 인증이 실패했습니다. 문제가 계속되면 다음 문제 중 하나로 인해 인증서 기반 인증 실패가 발생할 수 있습니다.

- OR WorkSpaces 클라이언트는 지원되지 않습니다. 인증서 기반 인증은 최신 Windows 클라이언트 애플리케이션을 사용하는 Windows WorkSpaces 온 WorkSpaces 스트리밍 프로토콜 (WSP) 번들에서 지원됩니다. WorkSpaces
- 디렉터리에서 WorkSpaces 인증서 기반 인증을 활성화한 후 다시 부팅해야 합니다. WorkSpaces
- WorkSpaces 인증서와 통신할 수 없거나 인증서를 AWS Private CA AWS Private CA 발급하지 않았습니다. 인증서가 발급되었는지 AWS CloudTrail에서 확인하세요. 자세한 정보는 인증서 기반 인증 관리을 참조하세요.
- 도메인 컨트롤러에 스마트 카드 로그온을 위한 도메인 컨트롤러 인증서가 없거나 만료되었습니다. 자세한 내용은 필수 조건의 7단계, 'Configure domain controllers with a domain controller certificate to authenticate smart card users'를 참조하세요.
- 인증서를 신뢰할 수 없습니다. 자세한 내용은 필수 조건의 7단계, 'Publish the CA to Active Directory'를 참조하세요. 도메인 `certutil -viewstore -enterprise NTAuth` 컨트롤러에서 실행하여 CA가 게시되었는지 확인합니다.
- 캐시에 인증서가 있지만 인증서를 무효화한 사용자의 속성이 변경되었습니다. 인증서 만료 전 (24시간) 에 AWS Support 문의하여 캐시를 지우십시오. 자세한 내용은 AWS Support Center를 참조하세요.
- `UserPrincipalName`SAML 속성의 userPrincipalName 형식이 제대로 지정되지 않았거나 사용자의 실제 도메인으로 해석되지 않습니다. 자세한 내용은 필수 조건의 1단계를 참조하세요.
- SAML 어설션의 `ObjectSid` 속성(선택 사항)이 SAML_Subject `NameID`에 지정된 사용자의 Active Directory 보안 식별자(SID)와 일치하지 않습니다. SAML 페더레이션에서 속성 매핑이 올바른지, SAML ID 제공업체가 Active Directory 사용자의 SID 속성을 동기화하고 있는지 확인하세요.
- 스마트 카드 로그온을 위한 기본 Active Directory 설정을 수정하거나 스마트 카드 판독기에서 스마트 카드를 제거한 경우 조치를 취하는 그룹 정책 설정이 있습니다. 이러한 설정으로 인해 위에 나열된 오류 외에도 예상치 못한 동작이 추가로 발생할 수 있습니다. 인증서 기반 인증은 인스턴스 운영 체제에 가상 스마트 카드를 제공하고 로그온이 완료된 후 제거합니다. Primary Group Policy settings for smart cards와 스마트 카드 제거 동작을 포함한 Additional smart card Group Policy settings and registry keys를 확인합니다.

- 사설 CA의 CRL 배포 지점은 온라인 상태가 아니며 WorkSpaces 또는 도메인 컨트롤러에서 액세스할 수 없습니다. 자세한 내용은 필수 조건의 5단계를 참조하십시오.
- 도메인이나 포리스트에 오래된 CA가 있는지 확인하려면 CA를 `PKIVIEW.msc` 실행하여 확인하십시오. 오래된 CA가 있는 경우 `PKIVIEW.msc` mmc를 사용하여 수동으로 삭제하십시오.
- Active Directory 복제가 작동 중이고 도메인에 오래된 도메인 컨트롤러가 없는지 확인하려면 를 실행하십시오. `repadmin /replsum`

추가 문제 해결 단계에는 WorkSpaces 인스턴스 Windows 이벤트 로그를 검토하는 것이 포함됩니다. 로그온 실패 여부를 검토하는 일반적인 이벤트는 Windows Security 로그의 Event 4625: An account failed to logon입니다.

문제가 지속되면 문의하세요. AWS Support자세한 내용은 AWS Support Center를 참조하세요.

Windows 설치 미디어가 필요하지만 제공하지 WorkSpaces 않는 작업을 하려고 합니다.

AWS제공된 퍼블릭 번들을 사용하는 경우 필요할 때 Amazon EC2에서 제공하는 Windows Server OS 설치 미디어 EBS 스냅샷을 사용할 수 있습니다.

이러한 스냅샷으로 EBS 볼륨을 생성하여 Amazon EC2에 연결하고 필요에 따라 파일이 있는 곳으로 파일을 WorkSpace 전송합니다. BYOL에서 WorkSpaces Windows 10을 사용하고 있는데 설치 미디어가 필요한 경우 설치 미디어를 직접 준비해야 합니다. 자세한 내용은 설치 미디어를 사용하여 Windows 구성 요소 추가를 참조하세요. EBS 볼륨을 에 직접 연결할 수 없으므로 Amazon EC2 인스턴스에 연결하고 파일을 복사해야 합니다. WorkSpace

지원되지 않는 WorkSpaces 지역에서 생성된 기존 AWS 관리 디렉터리를 WorkSpaces 사용하여 시작하고 싶습니다.

현재 지원되지 않는 지역의 디렉터리를 WorkSpaces 사용하여 Amazon을 WorkSpaces 시작하려면 아래 단계를 따르십시오.

> **Note**
>
> AWS Command Line Interface 명령을 실행할 때 오류가 발생하는 경우 최신 AWS CLI 버전을 사용하고 있는지 확인하십시오. 자세한 내용은 최신 버전의 AWS CLI를 실행 중인지 확인합니다를 참조하세요.

1단계: 계정의 다른 VPC와 Virtual Private Cloud(VPC) 피어링 생성

1. 다른 리전의 VPC와 VPC 피어링 연결을 생성합니다. 자세한 내용은 동일한 계정 및 상이한 리전의 VPC로 생성을 참조하세요.
2. VPC 피어링 연결을 수락합니다. 자세한 정보는 VPC 피어링 연결 수락을 참조하세요.
3. VPC 피어링 연결을 활성화한 후 Amazon VPC 콘솔, 또는 API를 사용하여 VPC 피어링 연결을 볼 수 있습니다. AWS CLI

2단계: 두 리전의 VPC 피어링에 대한 라우팅 테이블 업데이트

IPv4 또는 IPv6를 통한 피어 VPC와의 통신을 활성화하도록 라우팅 테이블을 업데이트합니다. 자세한 내용은 VPC 피어링 연결을 위한 라우팅 테이블 업데이트를 참조하세요.

3단계: AD 커넥터 생성 및 Amazon 등록 WorkSpaces

1. AD Connector 사전 조건을 검토하려면 AD Connector prerequisites를 참조하세요.
2. AD Connector를 사용하여 기존 디렉터리를 연결합니다. 자세한 내용은 Create an AD Connector를 참조하세요.
3. AD Connector 상태가 활성으로 변경되면 AWS Directory Service 콘솔을 열고 디렉터리 ID의 하이퍼링크를 선택합니다.
4. AWS 앱 및 서비스의 경우 WorkSpacesAmazon을 선택하여 이 디렉터리에 WorkSpaces 대한 액세스를 활성화하십시오.
5. 디렉터리를 등록하십시오 WorkSpaces. 자세한 내용은 디렉터리 등록을 참조하십시오 WorkSpaces.

Amazon Linux 2에서 Firefox를 업데이트하고 싶은 경우

1단계: 자동 업데이트 활성화 확인

자동 업데이트가 활성화되었는지 확인하려면 에서 명령을 `systemctl status *os-update-mgmt.timer | grep enabled` 실행하십시오. WorkSpace 출력에는 `enabled`라는 단어가 포함된 두 줄이 있어야 합니다.

2단계: 업데이트 시작

Firefox는 일반적으로 유지 관리 기간 동안 Amazon Linux 2에서 시스템의 다른 모든 소프트웨어 패키지와 WorkSpaces 함께 자동으로 업데이트됩니다. 하지만 이는 사용 WorkSpaces 중인 유형에 따라 다릅니다.

- 의 경우 AlwaysOn WorkSpaces, 주간 유지 관리 기간은 해당 시간대의 일요일 00:00 ~ 04:00 입니다. WorkSpace
- 매월 세 번째 월요일부터 최대 2주 동안 유지 관리 기간은 해당 지역의 시간대를 기준으로 매일 약 00:00 부터 05:00 까지 운영됩니다 AutoStop WorkSpaces. AWS WorkSpace

유지 관리 기간에 대한 자세한 내용은 유지 관리를 참조하십시오. WorkSpace

서버를 WorkSpace 재부팅하고 15분 후에 다시 연결하여 즉각적인 업데이트 주기를 시작할 수도 있습니다. `sudo yum update`를 입력하여 업데이트를 시작할 수도 있습니다. Firefox 전용 업데이트를 시작하려면 `sudo yum install firefox`를 입력합니다.

Amazon Linux 2 리포지토리에 대한 액세스를 구성할 수 없고 Mozilla에서 빌드한 바이너리를 사용하여 Firefox를 설치하려는 경우 Mozilla Support에서 Mozilla 빌드로 Firefox 설치하기를 참조하세요. 실수로 오래된 버전을 실행하지 않도록 RPM 패키지 버전의 Firefox를 완전히 제거하는 것이 좋습니다. `sudo yum remove firefox` 명령을 실행하여 제거할 수 있습니다.

다른 시스템에서 `yumdownloader firefox` 명령을 실행하여 Amazon Linux 2 리포지토리에서 필요한 RPM 패키지를 다운로드할 수도 있습니다. 그런 다음 리포지토리를 사이드로 로드하여 와 WorkSpaces 같은 표준 명령을 사용하여 설치할 수 있습니다. YUM `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> 정확한 파일 이름은 패키지 버전에 따라 달라집니다.

3단계: Firefox 리포지토리가 사용되었는지 확인

아마존 리눅스 엑스트라는 아마존 리눅스 2에 대한 파이어폭스 업데이트를 자동으로 제공합니다. WorkSpaces 2023년 7월 31일 이후에 WorkSpaces 생성된 Amazon Linux 2에는 이미 Firefox Extra 리포지토리가 활성화되어 있을 것입니다. Firefox Extra 리포지토리를 사용하고 WorkSpace 있는지 확인하려면 다음 명령을 실행하십시오.

```
yum repolist | grep amzn2extra-firefox
```

명령 출력은 Firefox Extra 리포지토리를 사용하는 경우 `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10`과 비슷합니다. Firefox Extra 리포지토리를 사용하지 않으면 출력이 비어 있습니다. Firefox Extra 리포지토리를 사용하지 않는 경우 다음 명령을 사용하여 수동으로 활성화할 수 있습니다.

```
sudo amazon-linux-extras install firefox
```

Firefox Extra 리포지토리 활성화가 여전히 실패하는 경우, 인터넷 액세스를 확인하고 VPC 엔드포인트가 구성 해제되었는지 확인하세요. YUM 리포지토리를 WorkSpaces 통해 Amazon Linux 2용 Firefox 업데이트를 계속 받으려면 Amazon Linux 2 리포지토리에 연결할 수 WorkSpaces 있는지 확인하십시오. 인터넷 액세스 없이 Amazon Linux 2 리포지토리에 액세스하는 방법에 대한 자세한 내용은 이 지식 센터 문서를 참조하세요.

내 사용자는 에 구성된 세분화된 암호 정책 (FFGP) 설정을 무시하고 WorkSpaces 클라이언트를 사용하여 암호를 재설정할 수 있습니다. AWS Managed Microsoft AD

사용자 WorkSpaces 클라이언트가 연결되어 있는 AWS Managed Microsoft AD경우 기본 복잡성 설정을 사용하여 암호를 재설정해야 합니다.

기본 복잡성 암호는 대소문자를 구분하며 길이가 8~64자 사이여야 합니다 (포함). 다음 각 범주의 문자를 하나 이상 포함해야 합니다.

- 소문자(a-z)
- 대문자(A-Z)
- 숫자(0-9)
- 영숫자 외의 특수 문자(~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

암호에는 공백, 캐리지 리턴 탭, 줄 바꿈, Null 문자 등 인쇄할 수 없는 유니코드 문자가 포함되지 않도록 하십시오.

조직에서 FFGP를 적용하도록 요구하는 경우 Active Directory 관리자에게 문의하여 클라이언트 대신 Active Directory에서 직접 사용자 암호를 재설정하도록 요청하십시오. WorkSpaces WorkSpaces

사용자가 웹 액세스를 사용하여 Windows/Linux에 액세스하려고 할 때 WorkSpace “이 OS/플랫폼은 사용자 시스템에 액세스할 권한이 없습니다”라는 오류 메시지를 받습니다. WorkSpace

사용자가 사용하려는 운영 체제 버전이 웹 액세스와 호환되지 않습니다. WorkSpaces WorkSpace 디렉터리의 기타 플랫폼 설정에서 웹 액세스를 활성화해야 합니다. 웹 액세스를 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오Amazon WorkSpaces 웹 액세스 활성화 및 구성. WorkSpace

Amazon WorkSpaces 클라이언트 애플리케이션 수명 종료 정책

Amazon WorkSpaces 수명 종료(EOL) 정책은 더 이상 지원을 받지 않고 새 버전과의 호환성 테스트를 더 이상 받지 않는 WorkSpaces의 특정 메이저 버전(및 모든 마이너 버전)에 적용됩니다.

WorkSpaces 클라이언트 버전의 수명 주기는 일반 지원, 기술 지침 및 수명 종료(EOL)의 3단계로 구성됩니다. 일반 지원 단계는 WorkSpaces 클라이언트의 최초 정식 출시일에 시작되며 정해진 기간 동안 지속됩니다. 일반 지원 단계에서 WorkSpaces 지원팀은 구성 문제에 대한 전체 지원을 제공합니다. 결함 해결 및 기능 요청은 WorkSpaces 클라이언트의 해당 메이저 버전 및 관련 마이너 버전에 구현됩니다.

기술 지침은 일반 지원 단계 종료일부터 EOL 날짜까지 제공됩니다. 기술 지침 단계에서는 지원되는 구성에 대해서만 지원 및 지침을 받습니다. 결함 해결 및 기능 요청은 가장 최신 버전의 WorkSpaces 클라이언트에만 구현됩니다. 이전 버전에는 구현되지 않습니다. 기술 지침 단계에서 수정이 필요한 경우 AWS는 예정된 정식 버전 릴리스에 해당 사항을 수정할 일정을 잡고 사용자는 최신 WorkSpaces 버전으로 업그레이드하여 수정 사항과 관련된 지원을 받을 수 있습니다.

메이저 버전의 EOL은 일반 지원과 기술 지침이 모두 종료되었을 때 발생합니다. EOL 날짜 이후에는 추가 지원이나 유지 관리가 제공되지 않습니다. AWS는 호환성 문제에 대한 테스트를 중단합니다. 지속적인 지원을 받으려면 최신 WorkSpaces 클라이언트 버전으로 업그레이드해야 합니다.

특정 버전의 지원에 대한 자세한 내용은 이 표를 참조하세요.

Windows 클라이언트	일반 지원	기술 지침	EOL
2.x	2018	2023년 3월 31일	2023년 8월 31일

Linux 클라이언트	일반 지원	기술 지침	EOL
Ubuntu 18.04용 4.x	2021년 8월 12일	2023년 3월 31일	2023년 8월 31일
Ubuntu 18.04용 3.x	2019년 11월 25일	2023년 3월 31일	2023년 8월 31일

macOS 클라이언트	일반 지원	기술 지침	EOL
2.x	2019	2023년 3월 31일	2023년 8월 31일
1.x	2018	2023년 3월 31일	2023년 8월 31일

iPad 클라이언트	일반 지원	기술 지침	EOL
1.x	2018	2023년 3월 31일	2023년 8월 31일

Android 클라이언트	일반 지원	기술 지침	EOL
2.x	2019	2023년 3월 31일	2023년 8월 31일
1.x	2018	2023년 3월 31일	2023년 8월 31일

웹 액세스	일반 지원		
Google Chrome	현재 버전 및 2개의 최신 메이저 버전		
Firefox	현재 버전 및 2개의 최신 메이저 버전		
Microsoft Edge	현재 버전 및 2개의 최신 메이저 버전		

지원되지 않는 클라이언트

다음 WorkSpaces 클라이언트는 지원되지 않습니다.

운영 체제	클라이언트 버전	일반 지원	기술 지침	EOL	주의
Windows	5.11	2023년 7월 3일	2023년 10월 1일	2023년 10월 1일	품질 문제로 인해 지원되지 않음
Windows	5.10	2023년 6월 19일	2023년 10월 1일	2023년 10월 1일	품질 문제로 인해 지원되지 않음
Windows	5.9	2023년 5월 9일	2023년 10월 1일	2023년 10월 1일	품질 문제로 인해 지원되지 않음

EOL FAQ

EOL에 도달한 WorkSpaces 클라이언트 버전을 사용하고 있습니다. 지원되는 버전으로 업그레이드하려면 어떻게 해야 하나요?

WorkSpaces 클라이언트 다운로드 페이지로 이동하여 완전히 지원되는 WorkSpaces 버전을 다운로드하고 설치합니다.

EOL에 도달한 WorkSpaces 클라이언트 버전을 지원되는 WorkSpaces와 함께 사용할 수 있나요?

EOL에 도달한 클라이언트 버전에는 이전 해상도와 기능이 더 이상 적용되지 않으므로 클라이언트를 최신 버전으로 업그레이드하는 것이 좋습니다. EOL에 도달한 클라이언트 버전을 사용하는 경우 AWS 지원 팀에 자세한 내용을 문의하세요.

EOL에 도달한 WorkSpaces 클라이언트 버전을 사용하고 있습니다. 그래도 문제를 보고할 수 있나요?

먼저 지원되는 버전으로 업그레이드하고 문제를 재현해 봐야 합니다. 지원되는 버전에서도 문제가 지속되면 AWS 지원 팀에 지원 케이스를 여세요.

EOL에 도달한 운영 체제에서 지원되는 WorkSpaces 클라이언트 버전을 사용하고 있습니다. 그래도 문제를 보고할 수 있나요?

EOL에 도달한 운영 체제에 대한 기술 지원 및 소프트웨어 업데이트는 더 이상 제공되지 않으며 AWS에서는 EOL에 도달한 운영 체제를 사용하는 WorkSpaces 클라이언트에 대한 지원을 제공하지 않습니다. 지원되는 운영 체제를 사용하여 WorkSpaces 클라이언트가 지원되는지 확인하세요.

아마존 WorkSpaces 쿼터

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

계정의 기본 할당량은 다음과 같습니다. WorkSpaces AWS Service Quotas 콘솔을 사용하면 기본 할당량과 적용된 할당량을 확인하거나 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다.

Service Quotas를 사용할 수 없는 일부 리전에서는 지원 케이스를 제출하여 한도 증가를 요청해야 합니다. 자세한 내용은 Service Quotas 사용 설명서의 Viewing service quotas 및 할당량 증가 요청을 참조하세요.

Resource	기본값	설명	조정 가능
WorkSpaces	1	현재 지역 WorkSpaces 내 이 계정의 최대 수입니다.	예
그래픽 WorkSpaces	0	현재 WorkSpaces 지역에서 이 계정의 최대 그래픽 수입니다. **Note** 2023년 11월 30일 이후에는 Graphics 번들이 더 이상 지원되지 않습니다. Graphics.G4dn 번들로 마이그레이션하는 WorkSpaces 것이 좋습니다. 자세한	예

Resource	기본값	설명	조정 가능
		내용은 마이그레이션 a WorkSpace 섹션을 참조하세요.	
그래픽.G4dn WorkSpaces	0	현재 지역에서 이 계정의 최대 그래픽 수.G4dn. WorkSpaces	예
GraphicsPro WorkSpaces	0	현재 지역 GraphicsPro WorkSpaces 내 이 계정의 최대 수입니다.	예
GraphicsPro.g4dn WorkSpaces	0	현재 WorkSpaces 지역에서 이 계정의 최대 GraphicsPro 개수는.g4dn입니다.	예
스탠바이 WorkSpaces	0	현재 지역 WorkSpaces 내 이 계정의 최대 수입니다.	예
번들	50	현재 리전에 있는 이 계정에 대한 최대 번들 수 이 할당량은 커스텀 번들에만 적용되며 공개 번들에는 적용되지 않습니다.	아니요
연결 에일리어스	20	현재 리전에서 이 계정에 허용된 프록시의 최대 수	아니요

Resource	기본값	설명	조정 가능
디렉터리	50	현재 지역의 이 WorkSpaces 계정에서 Amazon에 사용하기 위해 등록할 수 있는 최대 디렉터리 수입니다.	아니요
이미지	40	현재 리전에 있는 이 계정에 대한 최대 이미지 수	예
IP 액세스 제어 그룹	100	현재 리전에 있는 이 계정에 대한 최대 서브넷 그룹 수	아니요
디렉터리당 IP 액세스 제어 그룹	25	현재 리전에 있는 이 계정의 최대 디렉터리당 최대 IP 액세스 제어 그룹 수	아니요
IP 액세스 제어 그룹당 규칙	10	현재 리전에 있는 이 계정의 최대 IP 액세스 제어 그룹당 최대 규칙 수	아니요

API 제한

허용된 속도는 초당 두 번의 호출입니다. 자세한 내용은 Throttling exceptions을 참조하세요.

WorkSpaces 스트리밍 프로토콜 (WSP) 호스트 에이전트 버전

WorkSpaces 스트리밍 프로토콜 (WSP) 호스트 에이전트는 내부에서 실행되는 호스트 에이전트입니다. WorkSpace 픽셀을 클라이언트 WorkSpace 애플리케이션으로 스트리밍하며 양방향 오디오 및 비디오, 인쇄와 같은 세션 내 기능을 포함합니다. WorkSpaces 스트리밍 프로토콜 (WSP) 에 대한 자세한 내용은 WorkSpacesAmazon용 프로토콜을 참조하십시오.

호스트 에이전트 소프트웨어를 최신 버전으로 업데이트하는 것이 좋습니다. 수동으로 WorkSpaces 재부팅하여 WSP 호스트 에이전트를 업데이트할 수 있습니다. WSP 호스트 에이전트는 정기적인 WorkSpaces 기본 유지 관리 기간 동안에도 자동으로 업데이트됩니다. 유지 관리 기간에 대한 자세한 내용은 유지 WorkSpace 관리를 참조하십시오. 이러한 기능 중 일부는 최신 WorkSpaces 클라이언트 버전을 필요로 합니다. 최신 클라이언트 버전에 대한 자세한 내용은 WorkSpaces 클라이언트를 참조하십시오.

다음 표에서는 WSP 호스트 에이전트의 각 버전의 변경 사항에 대해 설명합니다.

릴리스	날짜	변경
• 윈도우 WorkSpaces - 2.1.0.1554	2024년 5월 15일	• 유휴 연결 해제 타임아웃에 대한 지원이 추가되었습니다. • 유휴 연결 해제 제한 시간을 구성하는 새 그룹 정책 설정을 추가했습니다. • 사용자가 디스플레이 설정을 수정하면 연결이 끊기고 흰색 화면이 표시되는 문제를 WorkSpaces 수정했습니다. • 버그 수정 및 성능 향상.
• 우분투 - 2.1.0.1342 WorkSpaces	2024년 2월 29일	• 기본 웹캠 해상도를 480x360에서 640x480 사이로 변경했습니다. • 버그 수정 및 성능 향상.
• WorkSpaces 윈도우 - 2.0.0.1425	2024년 2월 22일	• 원격 Google Chrome 또는 Microsoft Edge 브라우저에서 실

릴리스	날짜	변경
		행되는 웹 애플리케이션의 세션 내 WebAuthn 리디렉션 요청에 대한 지원이 추가되었습니다. 이 기능은 사용자에게 WebAuthn DCV 리디렉션 확장을 활성화하도록 요청하는 일회성 브라우저 프롬프트를 추가합니다. Windows WorkSpaces 및 네이티브 클라이언트에서만 지원됩니다. WorkSpaces • 로그인할 때 가끔 흰색 또는 정지된 화면이 나타나는 문제를 수정했습니다. • 버그 수정 및 성능 향상.
• 윈도우 WorkSpaces - 2.0.0.1304	2024년 1월 11일	• 로그인 시 발생할 수 있는 스트리밍 중단과 관련된 버그가 수정되었습니다. • 로깅 관련 버그가 수정되었습니다.
• 윈도우 - 2.0.0.1288 WorkSpaces	2023년 11월 16일	• Windows 10+에 CPU 사용량을 줄이고 스트리밍 성능을 향상시키는 간접 디스플레이 드라이버 (IDD) 에 대한 지원이 추가되었습니다. • IDD 드라이버를 사용하거나 사용하지 않도록 설정하는 새 그룹 정책 설정이 추가되었습니다. • 클립보드 이미지 투명성과 관련된 버그가 수정되었습니다. • Windows 스케일 팩터를 유지하는 버그를 수정했습니다. • 버그 수정 및 성능 향상.

릴리스	날짜	변경
• 윈도우 WorkSpaces - 2.0.0.1164	2023년 10월 13일	• 가상 디스플레이 드라이버에 VSync에 대한 지원을 추가했습니다. • VSync를 활성화 또는 비활성화하는 새 그룹 정책 설정을 추가했습니다. • 재연결 및 신뢰성 문제를 개선했습니다. • 버그 수정 및 성능 향상.
• 아마존 리눅스 WorkSpaces - 2.0.0.1086 • WorkSpaces 우분투 - 2.1.0.1086	2023년 8월 18일	• 시간대 리디렉션을 활성화 또는 비활성화하는 새 설정을 추가했습니다. • 로그온 제한 시간을 연장하고 구성 옵션을 추가했습니다. • 중단 후 더 빠르게 재연결할 수 있도록 게이트웨이를 개선했습니다. • 버그 수정 및 성능 향상.
• 아마존 리눅스 WorkSpaces - 2.0.0.907	2023년 6월 30일	• ISV별 통합이 가능하도록 DCV 확장 SDK에 대한 지원을 추가했습니다. • 로그아웃하면 사용자 세션이 종료되도록 연결 해제 동작을 변경했습니다. • 시간대 리디렉션에 대한 지원을 추가했습니다. • 로그온 제한 시간을 연장하고 구성 옵션을 추가했습니다. • 업그레이드 문제를 수정했습니다. • 버그 수정 및 성능 향상.

릴리스	날짜	변경
• 윈도우 WorkSpaces - 2.0.0.829	2023년 6월 8일	• 로그아웃하면 사용자 세션이 종료되도록 연결 해제 동작을 변경했습니다. • A/V 동기화 및 일본어 키보드와 관련된 버그를 수정했습니다. • WSP 설치 프로그램 안정성을 개선했습니다.
• WorkSpaces 우분투 - 2.1.0.829	2023년 5월 16일	• 로그아웃하면 사용자 세션이 종료되도록 연결 해제 동작을 변경했습니다. • ISV별 통합이 가능하도록 DCV 확장 SDK에 대한 지원을 추가했습니다. • 시간대 리디렉션에 대한 지원을 추가했습니다. • 업그레이드 문제를 수정했습니다.
• 윈도우 WorkSpaces - 2.0.0.799	2023년 5월 8일	• 몇 가지 이미지 품질 및 성능 최적화를 통해 UDP 기반 QUIC 전송을 개선했습니다. • ISV별 통합이 가능하도록 DCV 확장 SDK에 대한 지원을 추가했습니다. • 확장 SDK를 활성화 또는 비활성화하는 새 그룹 정책 설정을 추가했습니다. • 한국어, 일본어, 독일어 키보드 레이아웃을 개선했습니다. • 세션 정지 문제, 하드웨어 가속화, 프린터 리디렉션, 로그 세부 사항 표시, target-fps 그룹 정책 설정과 관련된 버그를 수정했습니다.

Note

- 호스트 에이전트 버전을 확인하는 방법에 대한 자세한 내용은 최신 버전의 WSP에서 지원되는 클라이언트 및 호스트 운영 시스템은 무엇입니까?를 참조하세요.
- Host Agent 버전을 업데이트하는 방법에 대한 자세한 내용은 WorkSpaceWSP가 이미 있는 경우 어떻게 업데이트하나요? 를 참조하십시오. .
- WSP macOS 클라이언트 버전 릴리스 노트는 사용 설명서의 WorkSpaces macOS 클라이언트 애플리케이션 섹션에 있는 릴리스 노트를 참조하십시오. WorkSpaces
- WSP Windows 클라이언트 버전 릴리스 노트는 사용 설명서의 WorkSpaces Windows 클라이언트 애플리케이션 섹션에 있는 릴리스 노트를 참조하십시오. WorkSpaces

WSP에서 SDK 확장을 지원함

Amazon WorkSpaces 스트리밍 프로토콜(WSP)은 NICE DCV 기술로 구축되어 다양한 워크로드 및 사용 사례에서 WorkSpaces 인스턴스에 대한 고성능 원격 액세스를 지원합니다. NICE DCV 확장 SDK를 사용하여 개발자는 최종 사용자의 WSP WorkSpaces 환경을 다음과 같이 사용자 지정할 수 있습니다.

- 사용자 지정 하드웨어 지원을 촉진합니다.
- 원격 세션에서 서드 파티 애플리케이션의 유용성을 향상합니다. 예를 들어 VoIP 애플리케이션을 위한 로컬 오디오 종료를 추가하거나 회의 애플리케이션을 위한 로컬 비디오 재생을 추가합니다.
- 스크린 리더와 같은 접근성 소프트웨어에 원격 세션 및 원격으로 실행되는 애플리케이션에 대한 정보를 제공합니다.
- 보안 소프트웨어가 로컬 엔드포인트의 보안 상태를 분석하여 조건부 액세스 정책을 허용할 수 있도록 합니다.
- 설정된 원격 세션을 통해 임의의 데이터 전송을 수행합니다.

NICE DCV 확장 SDK를 시작하려면 NICE DCV 확장 SDK 설명서를 참조하세요. NICE DCV 확장 SDK GitHub 리포지토리에서 SDK를 찾을 수 있습니다. 또한 NICE DCV 확장 SDK 샘플 GitHub 리포지토리에서 SDK의 통합 예시를 찾을 수 있습니다.

다음은 WorkSpaces에서 지원됩니다.

- 스트리밍 프로토콜 - WorkSpaces 스트리밍 프로토콜(WSP)
- WorkSpaces Windows 클라이언트 – Windows: 5.9.0.4110 이상

> **Note**
>
> WorkSpaces Android, iOS 클라이언트, 웹 액세스는 NICE DCV 확장 SDK를 지원하지 않습니다.

- WorkSpaces 지원 - Windows, Linux 및 Ubuntu 서버

WorkSpaces에 대한 문서 기록

다음 표에서는 2018년 1월 1일 이후 WorkSpaces 서비스와 Amazon WorkSpaces 관리 안내서의 주요 변경 사항을 설명합니다. 사용자로부터 받은 의견을 수렴하기 위해 설명서가 자주 업데이트됩니다.

이러한 업데이트에 대한 알림을 받으려면 WorkSpaces RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
AmazonWorkSpacesAdmin 관리형 정책 업데이트	WorkSpaces에서 Amazon WorkspacesAdmin 관리형 정책에 WorkSpaces:Restore Workspace 작업을 추가하여 관리자에게 WorkSpaces를 복원할 수 있는 액세스 권한을 부여했습니다.	2023년 7월 17일
WSP에서 SDK 확장을 지원함	NICE DCV 확장 SDK를 사용하여 개발자는 최종 사용자의 WSP WorkSpaces 환경을 사용자 지정할 수 있습니다.	2023년 5월 25일
WorkSpaces 스트리밍 프로토콜(WSP) 호스트 에이전트 버전	WorkSpaces 스트리밍 프로토콜(WSP)의 버전 정보입니다.	2023년 5월 8일
AWS GovCloud(미국 동부)에 Amazon WorkSpaces 출시	Amazon WorkSpaces를 AWS GovCloud(미국 동부)에서 사용할 수 있습니다.	2023년 5월 3일
Amazon WorkSpaces 웹캠 지원	Amazon WorkSpaces는 이제 WorkSpaces 스트리밍 프로토콜(WSP)을 사용하여 로컬 웹캠 비디오 입력을 Windows WorkSpaces 데스크톱으로 원활하게 리디렉션함으로써 실시	2021년 4월 5일

	간 오디오-비디오(AV)를 지원합니다.	
WorkSpaces macOS 클라이언트 애플리케이션에서 Amazon WorkSpaces 스마트 카드 지원	이제 일반 액세스 카드(CAC) 및 개인 신원 확인(PIV) 스마트 카드를 Amazon WorkSpaces macOS 클라이언트 애플리케이션에서 사용할 수 있습니다. WorkSpaces에서 WorkSpaces 스트리밍 프로토콜(WSP)을 사용하여 스마트 카드가 지원됩니다.	2021년 4월 5일
Amazon WorkSpaces 번들 관리 API	이제 Amazon WorkSpaces 번들 관리 API를 사용할 수 있습니다. 이러한 API 작업은 WorkSpaces 번들에 대한 생성, 삭제 및 이미지 연결 작업을 지원합니다.	2021년 3월 15일
아시아 태평양(뭄바이)에 Amazon WorkSpaces 출시	Amazon WorkSpaces를 아시아 태평양(뭄바이) 리전에서 사용할 수 있습니다.	2021년 3월 8일
WorkSpaces 스트리밍 프로토콜(WSP)	WorkSpaces 스트리밍 프로토콜(WSP)은 이제 Graphics 및 GraphicsPro를 제외한 모든 번들 유형에서 라이선스 포함(Windows Server 2016) 및 기존 보유 라이선스(BYOL)를 사용하는 Windows 10 기반 WorkSpaces에서 모두 사용할 수 있습니다. WSP는 AWS GovCloud(미국 서부) 리전에 있는 Linux WorkSpaces에서도 사용할 수 있습니다.	2020년 12월 1일

스마트 카드	Amazon WorkSpaces는 이제 AWS GovCloud (미국 서부) 리전의 Windows 및 Linux WorkSpaces에서 세션 전(로그인) 및 세션 내 스마트 카드 인증을 지원합니다.	2020년 12월 1일
사용자 지정 이미지 공유	이제 AWS 계정 간에 사용자 지정 WorkSpaces 이미지를 공유할 수 있습니다. 이미지를 공유한 후 수신자 계정은 이미지를 복사하여 새 WorkSpaces를 시작하기 위한 번들을 생성하는 데 사용할 수 있습니다.	2020년 10월 1일
리전 간 리디렉션	이제 도메인 이름 시스템(DNS) 라우팅 정책과 함께 작동하여 기본 WorkSpaces를 사용할 수 없는 경우 사용자를 대체 WorkSpaces로 리디렉션하는 기능인 리전 간 리디렉션을 사용할 수 있습니다.	2020년 9월 10일
BYOL WorkSpaces에서 Microsoft Office 2016 또는 2019 구독	이제 기존 보유 Windows 라이선스(BYOL) WorkSpaces에서 AWS가 제공하는 Microsoft Office Professional 2016 또는 2019를 구독할 수 있습니다.	2020년 9월 3일
중국(닝샤)에서 BYOL 자동화	기존 보유 라이선스 사용(BYOL) 자동화를 사용하여 중국(닝샤)의 WorkSpaces에 Windows 10 데스크톱 라이선스를 사용하는 프로세스를 간소화할 수 있습니다.	2020년 4월 2일

이미지 검사기	이미지 검사기 도구를 사용하면 Windows WorkSpace가 이미지 생성 요구 사항을 충족하는지 확인할 수 있습니다. 이미지 검사기는 이미지를 생성하는 데 사용하려는 WorkSpace에서 일련의 테스트를 수행하고 발견된 문제를 해결하는 방법에 대한 지침을 제공합니다.	2020년 3월 30일
WorkSpaces 마이그레이션	Amazon WorkSpaces 마이그레이션 기능을 사용하면 사용자 볼륨의 데이터를 유지하면서 한 번들에서 다른 번들로 WorkSpace를 마이그레이션할 수 있습니다. 이 기능을 사용하여 Windows 7 데스크톱 환경에서 Windows 10 데스크톱 환경으로 WorkSpaces를 마이그레이션할 수 있고, 한 퍼블릭 또는 사용자 지정 번들에서 다른 퍼블릭 또는 사용자 지정 번들로 WorkSpaces를 마이그레이션할 수도 있습니다.	2020년 1월 9일
Amazon WorkSpaces API에 대한 PrivateLink 통합	인터넷을 통해 연결하는 대신 Virtual Private Cloud(VPC)의 인터페이스 엔드포인트를 통해 Amazon WorkSpaces API 엔드포인트에 직접 연결할 수 있습니다. VPC 인터페이스 엔드포인트를 사용하는 경우 VPC와 Amazon WorkSpaces API 엔드포인트 간의 통신은 모두 AWS 네트워크에서 안전하게 수행됩니다.	2019년 11월 25일

Amazon WorkSpaces에 대한 Linux 클라이언트	이제 Linux 클라이언트를 사용하여 WorkSpaces에 액세스할 수 있습니다.	2019년 11월 25일
중국(닝샤)에 Amazon WorkSpaces 출시	Amazon WorkSpaces를 이제 중국(닝샤) 리전에서 사용할 수 있습니다	2019년 11월 13일
WorkSpaces를 알려진 마지막 정상 상태로 복원	복원 기능을 사용하여 WorkSpace를 알려진 마지막 정상 상태로 롤백할 수 있습니다.	2019년 9월 18일
FIPS 엔드포인트 암호화	연방정부의 위험 및 인증 관리 프로그램(FedRAMP) 또는 미국 국방부(DoD) 클라우드 컴퓨팅 보안 요구 사항 가이드(SRG)를 준수하려면 Amazon WorkSpaces를 구성하여 디렉터리 수준에서 Federal Information Processing Standards(FIPS) 엔드포인트 암호화를 사용할 수 있습니다.	2019년 9월 12일
WorkSpace 이미지 복사	동일한 리전 또는 다른 리전 간에 이미지를 복사할 수 있습니다.	2019년 6월 27일
사용자를 위한 셀프 서비스 WorkSpace 관리 기능	사용자가 환경을 더 잘 제어할 수 있도록 사용자를 위한 셀프 서비스 WorkSpace 관리 기능을 활성화할 수 있습니다.	2018년 11월 19일

BYOL 자동화	기존 보유 라이선스 사용(BYOL) 자동화를 사용하여 WorkSpaces에 Windows 7 및 Windows 10 데스크톱 라이선스를 사용하는 프로세스를 간소화할 수 있습니다.	2018년 11월 16일
PowerPro 및 GraphicsPro 번들	PowerPro 및 GraphicsPro 번들을 이제 WorkSpaces에 사용할 수 있습니다.	2018년 10월 18일
성공한 WorkSpace 로그인 모니터링	Amazon CloudWatch Events의 이벤트를 사용하여 성공한 WorkSpace 로그인을 모니터링하고 대응할 수 있습니다.	2018년 9월 17일
Windows 10 WorkSpaces용 Web Access	이제 사용자는 웹 액세스 클라이언트를 사용하여 Windows 10 데스크톱 환경을 실행하는 WorkSpace에 액세스할 수 있습니다.	2018년 8월 24일
URI 로그인	URI(Uniform Resource Identifier)를 사용하여 사용자에게 WorkSpace에 대한 액세스 권한을 제공할 수 있습니다.	2018년 7월 31일
Amazon Linux WorkSpaces	사용자를 위해 Amazon Linux WorkSpaces를 프로비저닝할 수 있습니다.	2018년 26월 6일
IP 액세스 제어 그룹	사용자가 WorkSpaces에 액세스할 수 있는 IP 주소를 제어할 수 있습니다.	2018년 4월 30일

인플레이스 업그레이드	Windows 10 BYOL WorkSpaces를 최신 버전의 Windows 10으로 업그레이드할 수 있습니다.	2018년 3월 9일

이전 업데이트

다음 표에서는 2018년 1월 1일 이전 Amazon WorkSpaces 서비스 및 해당 설명서에 대한 주요 추가 사항을 설명합니다.

변경 사항	설명	날짜
유연한 컴퓨팅 옵션	Value, Standard, Performance 및 Power 번들 중에서 WorkSpaces를 전환할 수 있습니다	2017년 12월 22일
구성 가능한 스토리지	WorkSpaces를 시작한 후 나중에 WorkSpaces의 사용자 및 루트 볼륨 크기를 구성하여 이를 늘릴 수 있습니다.	2017년 12월 22일
디바이스 액세스 제어	WorkSpaces에 액세스할 수 있는 디바이스 유형을 지정할 수 있습니다. 또한 WorkSpaces에 대한 액세스를 신뢰할 수 있는 디바이스(관리형 디바이스라고도 함)로 제한할 수 있습니다.	2017년 19월 6일
포리스트 간 신뢰	AWS Managed Microsoft AD와 온프레미스 Microsoft Active Directory 도메인 간에 신뢰 관계를 설정한 다음 온프레미스 도메인의 사용자에게 WorkSpaces를 프로비저닝할 수 있습니다.	2017년 2월 9일
Windows Server 2016 번들	WorkSpaces에서 제공하는 번들에는 Windows Server 2016에 의해 구동되는 Windows 10 데스크톱 경험이 포함됩니다.	2016년 11월 29일
웹 액세스	WorkSpaces Web Access를 사용하여 웹 브라우저에서 Windows WorkSpaces에 액세스할 수 있습니다.	2016년 11월 18일

변경 사항	설명	날짜
시간 요금제 WorkSpaces	사용자에게 시간 단위로 청구하도록 WorkSpaces를 구성할 수 있습니다.	2016년 8월 18일
Windows 10 BYOL	Windows 10 데스크톱 라이선스를 WorkSpaces로 가져올 수 있습니다(BYOL).	2016년 7월 21일
태깅 지원	태그를 사용하여 WorkSpaces를 관리 및 추적할 수 있습니다.	2016년 17월 5일
저장된 등록 내역	새 등록 코드를 입력할 때마다 WorkSpaces 클라이언트에 저장됩니다. 따라서 다른 디렉터리 또는 리전에 속한 WorkSpaces 간에 쉽게 전환할 수 있습니다.	2016년 1월 28일
Windows 7 BYOL, Chromebook 클라이언트, WorkSpace 암호화	Windows 7 데스크톱 라이선스를 WorkSpaces로 가져오고(BYOL), Chromebook 클라이언트를 사용하고, WorkSpace 암호화를 사용할 수 있습니다.	2015년 10월 1일
CloudWatch 모니터링	CloudWatch 모니터링에 대한 정보를 추가했습니다.	2015년 4월 28일
자동 세션 재연결	WorkSpaces 데스크톱 클라이언트 애플리케이션에 자동 세션 재연결 기능에 대한 정보를 추가했습니다.	2015년 3월 31일
퍼블릭 IP 주소	WorkSpaces에 퍼블릭 IP 주소를 자동으로 할당할 수 있습니다.	2015년 1월 23일
아시아 태평양(싱가포르)에 WorkSpaces 출시	아시아 태평양(싱가포르) 리전에서 WorkSpaces를 사용할 수 있습니다.	2015년 1월 15일
Value 번들 추가, Standard 번들 업데이트, Office 2013 추가	Value 번들을 사용할 수 있고, Standard 번들 하드웨어가 업그레이드되었고, Microsoft Office 2013을 Plus 패키지에 사용할 수 있습니다.	2014년 11월 6일

변경 사항	설명	날짜
이미지 및 번들 지원	사용자 지정한 WorkSpace에서 이미지를 생성하고 이 이미지에서 사용자 지정 WorkSpace 번들을 생성할 수 있습니다.	2014년 10월 28일
PCoIP 제로 클라이언트 지원	WorkSpaces PCoIP 제로 클라이언트 디바이스에 액세스할 수 있습니다.	2014년 10월 15일
아시아 태평양(도쿄)에 WorkSpaces 출시	아시아 태평양(도쿄) 리전에서 WorkSpaces를 사용할 수 있습니다.	2014년 8월 26일
로컬 프린터 지원	WorkSpaces에 로컬 프린터 지원을 활성화할 수 있습니다.	2014년 8월 26일
멀티 펙터 인증	연결된 디렉터리에서 멀티 팩터 인증을 사용할 수 있습니다.	2014년 8월 11일
기본 OU 지원 및 대상 도메인 지원	WorkSpace 시스템 계정이 배치되는 기본 조직 단위(OU)와 WorkSpace 시스템 계정이 생성되는 별도의 도메인을 선택할 수 있습니다.	2014년 7월 7일
보안 그룹 추가	WorkSpace에 보안 그룹을 추가할 수 있습니다.	2014년 7월 7일
아시아 태평양(시드니)에 WorkSpaces 출시	아시아 태평양(시드니) 리전에서 WorkSpaces를 사용할 수 있습니다.	2014년 5월 15일
유럽(아일랜드)에 WorkSpaces 출시	유럽(아일랜드) 리전에서 WorkSpaces를 사용할 수 있습니다.	2014년 5월 5일
공개 베타 버전	WorkSpaces를 공개 베타 버전으로 사용할 수 있습니다.	2014년 3월 25일

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