aws

관리자 안내서

아마존 WorkSpaces 씬 클라이언트

아마존 WorkSpaces 씬 클라이언트: 관리자 안내서

Table of Contents

Amazon WorkSpaces 씬 클라이언트 관리자 콘솔이란 무엇입니까?

Amazon WorkSpaces Thin Client 관리자 콘솔을 사용하면 관리자가 WorkSpaces 씬 클라이언트 포털을 통해 씬 클라이언트 환경 및 디바이스를 관리할 수 있습니다. WorkSpaces 관리자는 이 웹 콘솔에서 환경을 만들고, 디바이스를 관리하고, 네트워크 내의 WorkSpaces 씬 클라이언트 사용자를 위한 파라미터를 설정할 수 있습니다.

WorkSpaces 씬 클라이언트에 사용하는 가상 데스크톱 환경은 자체 콘솔 내에서 생성하거나 수정해야 합니다.

> **Important**
>
> WorkSpaces 씬 클라이언트 관리자 콘솔이 제대로 작동하려면 먼저 시스템이 특정 요구 사항을 충족해야 합니다. 이러한 요구 사항은 사전 요구 사항 및 구성에 나열되어 있습니다.

주제

를 처음 사용하십니까?

WorkSpaces Thin Client 관리자 콘솔을 처음 사용하는 경우 먼저 다음 섹션을 읽는 것이 좋습니다.

- WorkSpaces 씬 클라이언트 관리자 콘솔 시작
- WorkSpaces 씬 클라이언트 관리자 콘솔 사용

아키텍처

각 WorkSpaces 씬 클라이언트는 가상 데스크톱 인터페이스 (VDI) 공급자와 연결되어 있습니다. WorkSpaces 씬 클라이언트는 세 개의 VDI 공급자를 지원합니다.

- 아마존 WorkSpaces

- AppStream 2.0
- 아마존 WorkSpaces 시큐어 브라우저

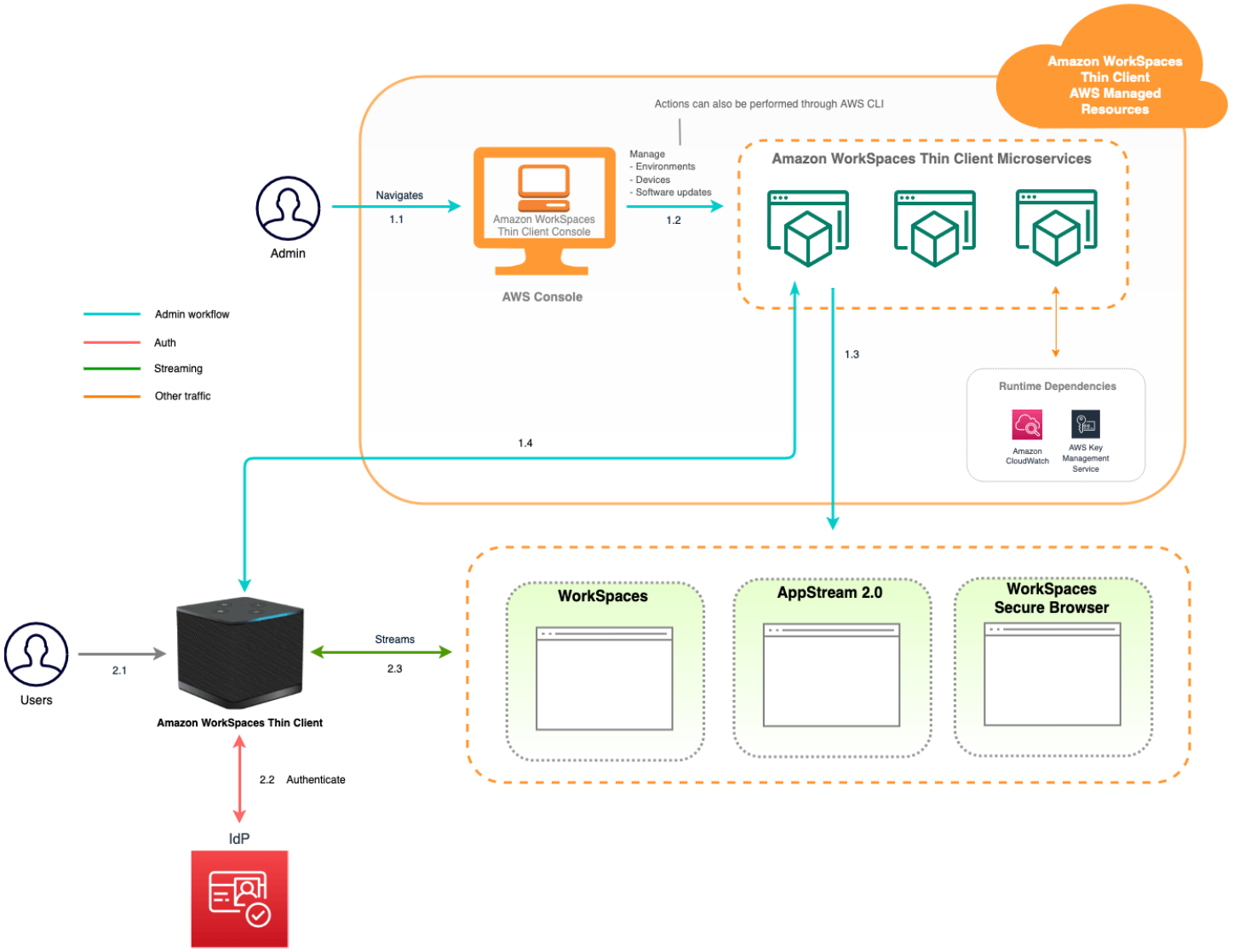
사용된 VDI에 따라 WorkSpaces 씬 클라이언트의 정보는 디렉토리, AppStream 2.0용 스택 및 보안 브라우저용 WorkSpaces 웹 포털 엔드포인트를 통해 액세스되고 관리됩니다. WorkSpaces

WorkSpacesAmazon에 대한 자세한 내용은 WorkSpaces 빠른 설정 시작하기를 참조하십시오. 디렉터리는 Simple AD AWS Directory Service, AD Connector 또는 Microsoft Active Directory의 AWS Directory Service 경우 관리형 Microsoft AD라고도 하는 옵션을 제공하는 를 통해 AWS 관리됩니다. 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요.

AppStream 2.0에 대한 자세한 내용은 Amazon AppStream 2.0 시작하기: 샘플 애플리케이션으로 설정을 참조하십시오. AppStream 2.0은 애플리케이션을 호스팅하고 실행하는 데 필요한 AWS 리소스를 관리하고, 자동으로 확장되며, 필요에 따라 사용자에게 액세스를 제공합니다. AppStream 2.0을 사용하면 기본적으로 설치된 애플리케이션과 구분할 수 없는 유연한 반응형 사용자 환경을 통해 원하는 디바이스에서 필요한 애플리케이션에 액세스할 수 있습니다.

WorkSpaces 보안 브라우저에 대한 자세한 내용은 Amazon WorkSpaces 보안 브라우저 시작하기를 참조하십시오. Amazon WorkSpaces Secure Browser는 내부 웹 사이트 및 (software-as-a-service SaaS) 애플리케이션에 대한 안전한 브라우저 액세스를 지원하도록 설계된 완전관리형 온디맨드 Linux 기반 서비스입니다. 인프라 관리, 특수 클라이언트 소프트웨어 또는 가상 프라이빗 네트워크(VPN) 솔루션에 대한 관리 부담 없이 기존 웹 브라우저에서 서비스에 액세스할 수 있습니다.

다음 다이어그램은 씬 클라이언트의 아키텍처를 보여줍니다. WorkSpaces


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
1.4
Admin workflow
Auth
Streaming
Other traffic
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

Amazon WorkSpaces 씬 클라이언트 관리자 콘솔 설정

주제

AWS에 가입

계정이 AWS 계정없는 경우 다음 단계를 완료하여 새로 만드십시오.

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

IAM 사용자를 생성합니다.

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center에서	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따르세요.	사용 AWS IAM Identity CenterAWS Command Line Interface 설명서에서 사용하도

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
(권장)	이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM 보안 모범 사례를 참조하세요.		록 AWS CLI 구성하여 프로그래밍 액세스를 구성하십시오.
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 첫 IAM 관리 사용자 및 사용자 그룹 만들기에 나온 지침을 따릅니다.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리 단계를 수행하여 프로그래밍 방식의 액세스를 구성합니다.

Amazon WorkSpaces 씬 클라이언트용 VDI 시작하기

Amazon WorkSpaces Thin Client는 AWS 최종 사용자 컴퓨팅 서비스와 함께 작동하여 애플리케이션 및 가상 데스크톱에 대한 안전하고 즉각적인 액세스를 제공하도록 설계된 비용 효율적인 씬 클라이언트 디바이스입니다.

가상 데스크톱 인프라 (VDI) 를 선택하고 WorkSpaces 씬 클라이언트와 함께 작동하도록 구성하십시오.

> **Important**
>
> WorkSpaces 씬 클라이언트 관리자 콘솔이 제대로 작동하려면 먼저 시스템이 특정 요구 사항을 충족해야 합니다. 이러한 요구 사항은 각 가상 데스크톱 공급자의 구성 절차에 나열되어 있습니다.

WorkSpaces 씬 클라이언트에는 가상 데스크톱 공급자에 따라 특정 소프트웨어 구성이 필요합니다.

주제

- Amazon WorkSpaces 씬 클라이언트를 WorkSpaces 위한 구성
- 아마존 WorkSpaces 씬 클라이언트용 AppStream 2.0 구성
- Amazon WorkSpaces 씬 클라이언트용 Amazon WorkSpaces 보안 브라우저 구성

Amazon WorkSpaces 씬 클라이언트를 WorkSpaces 위한 구성

WorkSpacesAmazon에서 WorkSpaces Thin Client를 사용하려면 WorkSpaces 디렉터리에 액세스하도록 서비스를 구성해야 합니다. WorkSpaces Amazon은 AWS 콘솔 내 WorkSpaces Thin Client Create 환경 페이지에 있는 디렉터리 이름을 기준으로 나열됩니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성을 해야 합니다. 콘솔을 사용하기 시작한 후에는 필수 기능을 수정하지 않는 것이 좋습니다.

시작하기 전 준비 사항

계정을 만들거나 관리하려면 AWS 계정이 있어야 합니다. WorkSpace 하지만 기기 사용자는 AWS 계정이 없어도 연결하여 사용할 수 있습니다 WorkSpaces.

구성을 진행하기 전에 다음 개념을 검토하고 이해하십시오.

- 를 WorkSpace 시작할 때 WorkSpace 번들을 선택하십시오. 자세한 내용은 Amazon WorkSpaces 번들을 참조하십시오.
- WorkSpace를 시작할 때 번들에 사용할 프로토콜을 선택하십시오. 자세한 내용은 Amazon용 프로토콜을 참조하십시오 WorkSpaces.
- 를 WorkSpace 시작할 때 사용자 이름 및 이메일 주소를 포함하여 각 사용자의 프로필 정보를 지정하십시오. 사용자는 암호를 생성하여 프로필을 완성합니다. 사용자에 WorkSpaces 대한 정보는 디렉터리에 저장됩니다. 자세한 내용은 디렉터리 관리를 참조하십시오. WorkSpaces
- 를 WorkSpace 시작할 때 WorkSpaces 웹 액세스를 활성화하고 구성하십시오. 자세한 내용은 Amazon WorkSpaces Web Access 활성화 및 구성을 참조하십시오.

1단계: 시스템이 WorkSpaces 필수 기능을 충족하는지 확인

WorkSpaces Thin Client 관리자 콘솔이 WorkSpaces Amazon과 제대로 작동하려면 시스템이 다음과 같은 특정 요구 사항을 충족해야 합니다. 이 표에는 지원되는 모든 기능과 해당 요구 사항이 나와 있습니다.

기능	요구 사항
웹 액세스	활성화됨
지원되는 운영 체제	• Windows 10 • Windows 10(기존 보유 라이선스 사용) • Windows 11 • Windows 11(기존 보유 라이선스 사용)
지원되는 번들	• 마이크로소프트 파워 (윈도우 10 탑재) (서버 2016, 2019, 2022년 기반) • 마이크로소프트 파워 (윈도우 10 포함) (서버 2016, 2019, 2022년 기반) w 오피스

기능	요구 사항
	• 마이크로소프트 PowerPro , 윈도우 10 탑재 (서버 2016, 2019, 2022년 기반) • 마이크로소프트 PowerPro , 윈도우 10 탑재 (서버 2016, 2019, 2022년 기반) w 오피스 • 윈도우 10을 탑재한 마이크로소프트 퍼포먼스 (서버 2016, 2019, 2022년 기반) • 윈도우 10 기반 마이크로소프트 퍼포먼스 (서버 2016, 2019, 2022년 기반) w 오피스
지원되는 프로토콜	WSP만 해당

2단계: 고급 설정을 사용하여 시작 WorkSpace

고급 설정을 사용하여 다음을 실행하려면 WorkSpace

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

아마존 WorkSpaces 씬 클라이언트용 AppStream 2.0 구성

AppStream 2.0 인스턴스는 스택 이름을 기반으로 나열되며 환경 생성 페이지에서 IdP 로그인 URL을 구성해야 합니다. AppStream 2.0용 SAML 인증은 시작 인증만 지원하므로 관리자는 올바른 로그인 URL을 수동으로 입력해야 합니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성을 해야 합니다. 콘솔을 사용하기 시작한 후에는 필수 기능을 수정하지 않는 것이 좋습니다.

1단계: 시스템이 AppStream 2.0 필수 기능을 충족하는지 확인

WorkSpaces Thin Client 관리자 콘솔이 AppStream 2.0과 제대로 작동하려면 시스템이 다음과 같은 특정 요구 사항을 충족해야 합니다. 이 표에는 지원되는 모든 기능과 요구 사항이 나열되어 있습니다.

기능	요구 사항
ID 제공업체	AppStream 2.0 관리자 안내서의 SAML 설정으로 이동하여 ID 제공자를 생성하십시오. 환경 콘솔을 만들라는 메시지가 표시되면 IDP 로그인 URL을 입력합니다.
운영 체제	Windows
플랫폼 유형	Windows Server(2012 R2, 2016 또는 2019)
스트리밍 프로토콜	TCP 스트리밍 UDP를 사용할 수 없는 경우 TCP에 대한 자동 폴백 메커니즘을 사용할 수 있습니다.
로컬 복사 및 붙여넣기	비활성화 AppStream 2.0 스택 수준에서 구성
로컬 폴더 공유	비활성화 AppStream 2.0 스택 수준에서 구성
로컬 인쇄	비활성화 AppStream 2.0 스택 수준에서 구성

AppStream 2.0의 SAML 인증을 통한 화면 잠금 요구 사항도 지원됩니다. WorkSpaces 씬 클라이언트에서는 사용자 풀 및 프로그래밍 인증 메커니즘이 지원되지 않습니다.

2단계: AppStream 2.0 스택 설정

애플리케이션을 스트리밍하려면 AppStream 2.0에는 스택과 연결된 플릿과 하나 이상의 애플리케이션 이미지가 포함된 환경이 필요합니다. 다음 단계에 따라 플릿과 스택을 설정하고 사용자에게 스택에 대한 액세스 권한을 부여하십시오. 아직 실행하지 않았다면 AppStream 2.0 시작하기: 샘플 애플리케이션으로 설정의 절차를 시도해 보는 것이 좋습니다.

사용할 이미지를 만들려면 자습서: 2.0 콘솔을 사용하여 사용자 지정 AppStream 2.0 이미지 만들기를 참조하십시오. AppStream

플릿을 Active Directory 도메인에 병합하려면 아래 단계를 수행하기 전에 먼저 Active Directory 도메인을 구성해야 합니다. 자세한 내용은 액티브 디렉터리 AppStream 2.0 사용을 참조하십시오.

작업

- 플릿 생성
- 스택 생성
- 사용자에게 액세스 권한 제공
- 리소스 정리

Amazon WorkSpaces 씬 클라이언트용 Amazon WorkSpaces 보안 브라우저 구성

Amazon WorkSpaces Secure Browser는 AWS 콘솔 내 WorkSpaces 씬 클라이언트 생성 환경 페이지의 웹 포털 엔드포인트를 기반으로 합니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성을 해야 합니다. 콘솔을 사용하기 시작한 후에는 필수 기능을 수정하지 않는 것이 좋습니다.

1단계: 시스템이 Amazon WorkSpaces 보안 브라우저 필수 기능을 충족하는지 확인

WorkSpaces 씬 클라이언트 관리자 콘솔이 Amazon WorkSpaces Secure Browser와 제대로 작동하려면 시스템이 다음과 같은 특정 요구 사항을 충족해야 합니다. 이 표에는 지원되는 모든 기능과 요구 사항이 나와 있습니다.

기능	요구 사항
로컬 복사 및 붙여넣기	비활성화
로컬 폴더 공유	비활성화

> **Note**
>
> 싱글 사인온을 위한 WorkSpaces 보안 브라우저 확장 프로그램은 현재 WorkSpaces 씬 클라이언트에서 지원되지 않습니다.

2단계: WorkSpaces 보안 브라우저 포털 설정

WorkSpaces 씬 클라이언트는 특정 구성의 WorkSpaces 보안 브라우저 VPC와 함께 작동합니다.

1. AWS CodeBuild 클라우드포메이션 템플릿을 사용하여 VPC를 생성합니다.
2. ID 공급자를 설정합니다.
3. Amazon WorkSpaces 보안 브라우저 포털을 생성하십시오.
4. 새 Amazon WorkSpaces 보안 브라우저 포털을 테스트해 보십시오.

WorkSpaces 씬 클라이언트 관리자 콘솔 시작

WorkSpaces 씬 클라이언트는 AWS 엔드 유저 컴퓨팅 서비스와 함께 작동하여 애플리케이션 및 가상 데스크톱에 대한 안전하고 즉각적인 액세스를 제공하도록 설계된 비용 효율적인 씬 클라이언트 디바이스입니다.

주제

제공 리전

WorkSpaces 씬 클라이언트는 다음 지역에서 사용할 수 있습니다.

이 지역에서는 WorkSpaces 씬 클라이언트 관리자 콘솔만 사용할 수 있습니다. WorkSpaces 씬 클라이언트 디바이스는 현재 미국, 독일, 프랑스, 이탈리아, 스페인에서만 사용할 수 있습니다.

리전 이름	지역	엔드포인트	콘솔 링크
미국 동부(버지니아 북부)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
미국 서부(오레곤)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
아시아 태평양(뭄바이)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home
유럽(아일랜드)	eu-west-1	thinclient.eu-west	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home

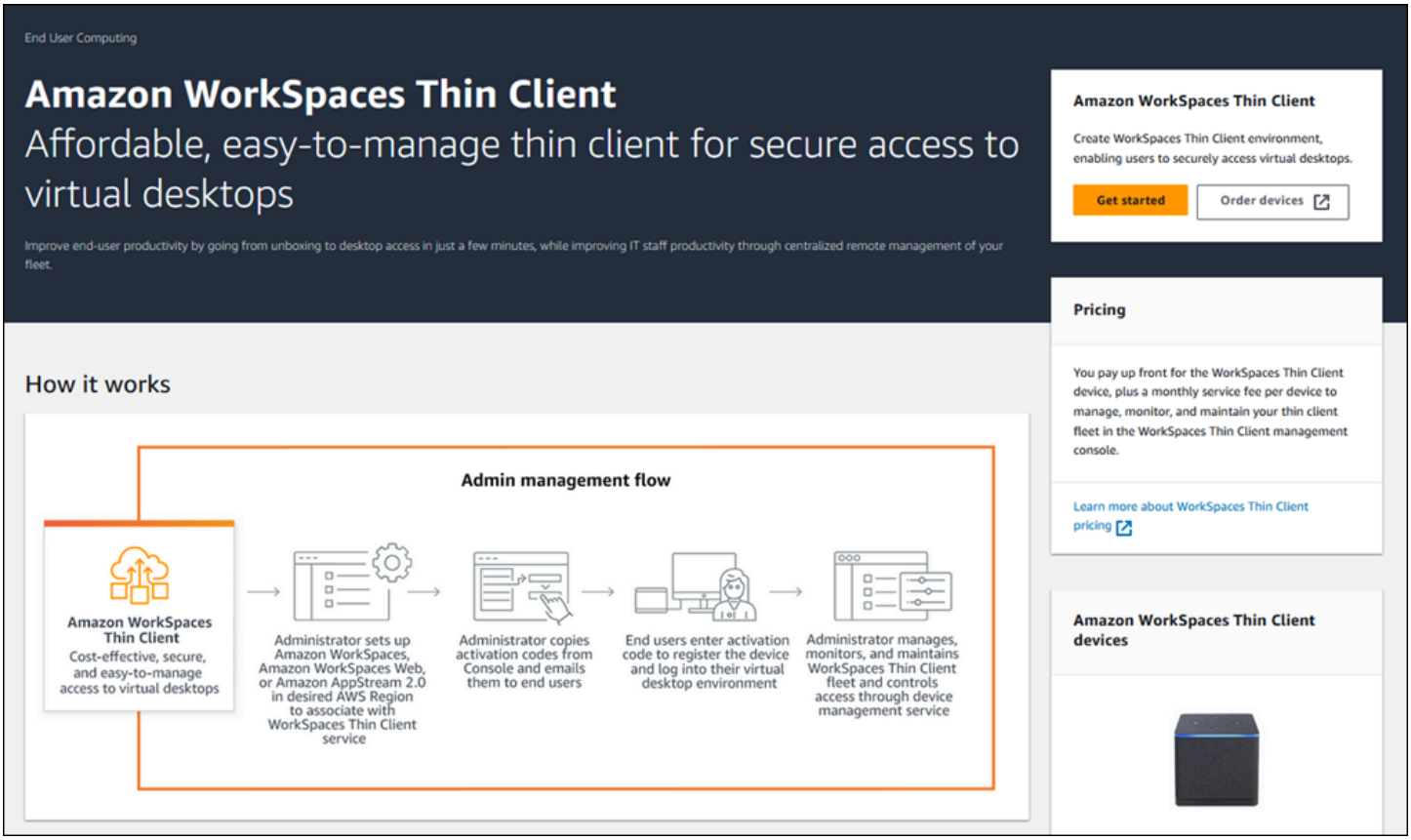
리전 이름	지역	엔드포인트	콘솔 링크
		-1.amazonaws.com	
캐나다(중부)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
유럽(프랑크푸르트)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
유럽(런던)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

WorkSpaces 씬 클라이언트 관리자 콘솔 실행

AWS 계정이 있으면 관리자 콘솔을 시작하고 WorkSpaces 씬 클라이언트 콘솔로 이동할 수 있습니다. 콘솔을 시작하려면 다음과 같이 하십시오.

1. AWS 계정에 로그온합니다.
2. WorkSpaces 씬 클라이언트 콘솔에 액세스합니다.
3. 시작하기를 선택하면 환경으로 이동됩니다.

WorkSpaces 씬 클라이언트 관리자 콘솔 사용



WorkSpaces 씬 클라이언트 관리자 콘솔에 오신 것을 환영합니다!

여기에서 팀을 위해 다양한 WorkSpaces 씬 클라이언트 디바이스와 환경을 관리할 수 있습니다.

WorkSpaces 씬 클라이언트 장치에 대한 자세한 내용은 WorkSpaces 씬 클라이언트 사용 설명서를 참조하십시오.

시작해봅시다.

주제

환경

각 WorkSpaces 씬 클라이언트 장치는 개별 가상 데스크톱 환경을 사용하여 온라인 리소스에 액세스합니다. 사용자는 다음 가상 데스크톱 제공자 중 하나를 사용하여 이 환경에 액세스합니다.

- 아마존 WorkSpaces
- AppStream 2.0
- 아마존 WorkSpaces 시큐어 브라우저

환경 목록

환경 목록 세부 정보

이름 - 이 환경과 연결된 고유 식별자입니다.

가상 데스크톱 서비스 - 이 환경에 사용되는 가상 데스크톱 공급자입니다.

가상 데스크톱 서비스 ID - 가상 데스크톱 서비스 공급자가 이 환경에 할당하는 고유 식별자입니다.

활성화 코드 - 최종 사용자가 가상 데스크톱 환경에 액세스할 때 사용하는 코드입니다.

디바이스 수 - 이 환경에 액세스하는 WorkSpaces 씬 클라이언트 디바이스의 수입니다.

환경 목록 작업

검색 - 관리하는 모든 환경을 검색합니다.

새로 고침 - 환경 목록을 새로 고칩니다.

세부 정보 보기 - 환경 세부 정보를 표시합니다.

조치 - 환경을 편집하거나 삭제할 수 있는 드롭다운 목록을 엽니다.

환경 생성 - 환경 생성 프로세스를 시작합니다.

환경 생성 - 환경 생성 프로세스를 시작합니다.

주제

- 환경 세부 정보
- 환경 생성
- 환경 편집

- 환경 삭제

환경 세부 정보

환경을 선택하면 WorkSpaces 씬 클라이언트 콘솔에 해당 환경에 대한 세부 정보가 표시되어 검토할 수 있습니다. 콘솔에는 이 환경에서 사용하는 가상 데스크톱 공급자에 대한 세부 정보도 표시됩니다.

주제

요약

이름 - 이 환경과 연결된 고유 식별자입니다.

가상 데스크톱 서비스 - 이 환경에 사용되는 가상 데스크톱 공급자입니다.

가상 데스크톱 서비스 ID - 가상 데스크톱 서비스 공급자가 이 환경에 할당하는 고유 식별자입니다.

활성화 코드 - 이 코드는 최종 사용자가 가상 데스크톱 환경에 액세스할 때 사용됩니다.

소프트웨어 항상 보관 up-to-date - 이 설정을 사용하면 소프트웨어를 자동으로 업데이트할 수 있습니다.

유지 관리 기간 시작 시간 - 매주 자동 소프트웨어 업데이트가 시작되는 시간입니다.

유지 관리 기간 종료 시간 - 매주 자동 소프트웨어 업데이트가 완료되는 시간입니다.

유지 관리 기간 요일 - 자동 소프트웨어 업데이트가 발생하는 요일입니다.

관련 디바이스 - 이 환경에 액세스하는 WorkSpaces 씬 클라이언트 디바이스의 수입니다.

생성 시간 - 이 환경을 만든 날짜 및 시간입니다.

가상 데스크톱 환경 세부 정보

Amazon WorkSpaces 디렉터리 세부 정보

디렉터리 ID - 이 환경과 관련된 Amazon WorkSpaces 디렉터리입니다.

디렉터리 이름 - 이 Amazon WorkSpaces 디렉터리와 관련된 고유 식별자입니다.

조직 이름 - Amazon WorkSpaces 디렉터리를 관리하는 조직의 이름입니다.

디렉터리 유형 - Amazon WorkSpaces 디렉터리의 형식입니다.

등록됨 - 이 Amazon WorkSpaces 디렉터리가 등록되었는지 여부.

상태 - 이 Amazon WorkSpaces 디렉터리가 활성 상태인지 여부.

Amazon WorkSpaces 보안 브라우저 포털 세부 정보

이름 - 이 Amazon WorkSpaces 보안 브라우저 포털과 관련된 고유 식별자입니다.

생성 시간 - 이 AppStream 2.0 스택이 생성된 날짜 및 시간입니다.

웹 포털 엔드포인트 - 가상 데스크톱 환경에 액세스하는 데 사용되는 URL입니다.

AppStream 2.0 세부 정보

스택 이름 - 이 AppStream 2.0 스택과 관련된 고유 식별자입니다.

IdP 로그인 URL - AppStream 2.0 스택에 로그인하고 로그아웃하는 데 사용되는 ID 공급자 URL입니다.

생성 시간 - 이 AppStream 2.0 스택이 생성된 날짜 및 시간입니다.

환경 생성

시작하려면 각 디바이스에 AWS 엔드 유저 컴퓨팅 서비스가 필요합니다. WorkSpaces 씬 클라이언트는 다음 서비스를 사용합니다.

- Amazon은 지정된 디렉터리를 WorkSpaces 통해
- AppStream 할당된 스택을 통한 2.0
- 웹 포털 주소를 통한 Amazon WorkSpaces 보안 브라우저

기존 환경에 서비스를 할당하거나 새 환경을 생성해야 합니다.

> **Note**
>
> WorkSpaces 씬 클라이언트는 동일한 지역의 가상 데스크톱만 표시합니다.

주제

- 3단계: 디바이스 사용자에게 활성화 코드 전송

1단계: 환경 세부 정보 입력

1. 환경 세부 정보 필드에 환경의 이름을 입력합니다.
2. 자동 소프트웨어 패치를 설정하려면 항상 소프트웨어 up-to-date 유지 체크박스를 선택합니다.

> **Note**
>
> 자동 소프트웨어 업데이트가 활성화되지 않은 경우 수동으로 업데이트를 푸시하거나 소프트웨어가 만료되어 시스템에서 강제로 업데이트할 때까지 이 환경에 등록된 장치는 소프트웨어 업데이트를 받지 않습니다.
> 또한 장치의 소프트웨어 세트 버전은 시스템에 의해 결정됩니다. 이 버전은 최신 버전이 아닐 수도 있습니다.

3. 사용자 환경의 유지 관리 기간을 예약하려는 경우 선택하십시오.
   - 시스템 전체 유지 관리 기간 적용 - 매주 지정된 시간에 환경 소프트웨어를 자동으로 업데이트합니다.
   - 사용자 지정 유지 관리 기간 적용 - 매주 환경 소프트웨어를 업데이트할 날짜와 시간을 설정합니다.
4. 가상 데스크톱 서비스를 선택합니다.
   - 아마존 WorkSpaces
   - 아마존 WorkSpaces 시큐어 브라우저
   - AppStream 2.0

2단계: 가상 데스크톱 공급자 선택

사용자에게 가상 데스크톱 및 호환 가능한 리소스에 대한 액세스를 제공하는 서비스가 있어야 합니다.

> **Important**
>
> WorkSpaces 씬 클라이언트 관리자 콘솔이 제대로 작동하려면 시스템이 특정 요구 사항을 충족해야 합니다. 이러한 요구 사항은 사전 요구 사항 및 구성에 나열되어 있습니다.
> 콘솔을 설정하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하십시오.

아마존 사용 WorkSpaces

WorkSpaces Amazon은 Windows용 완전 관리형 데스크톱 가상화 서비스로, 지원되는 모든 디바이스에서 리소스에 액세스할 수 있습니다.

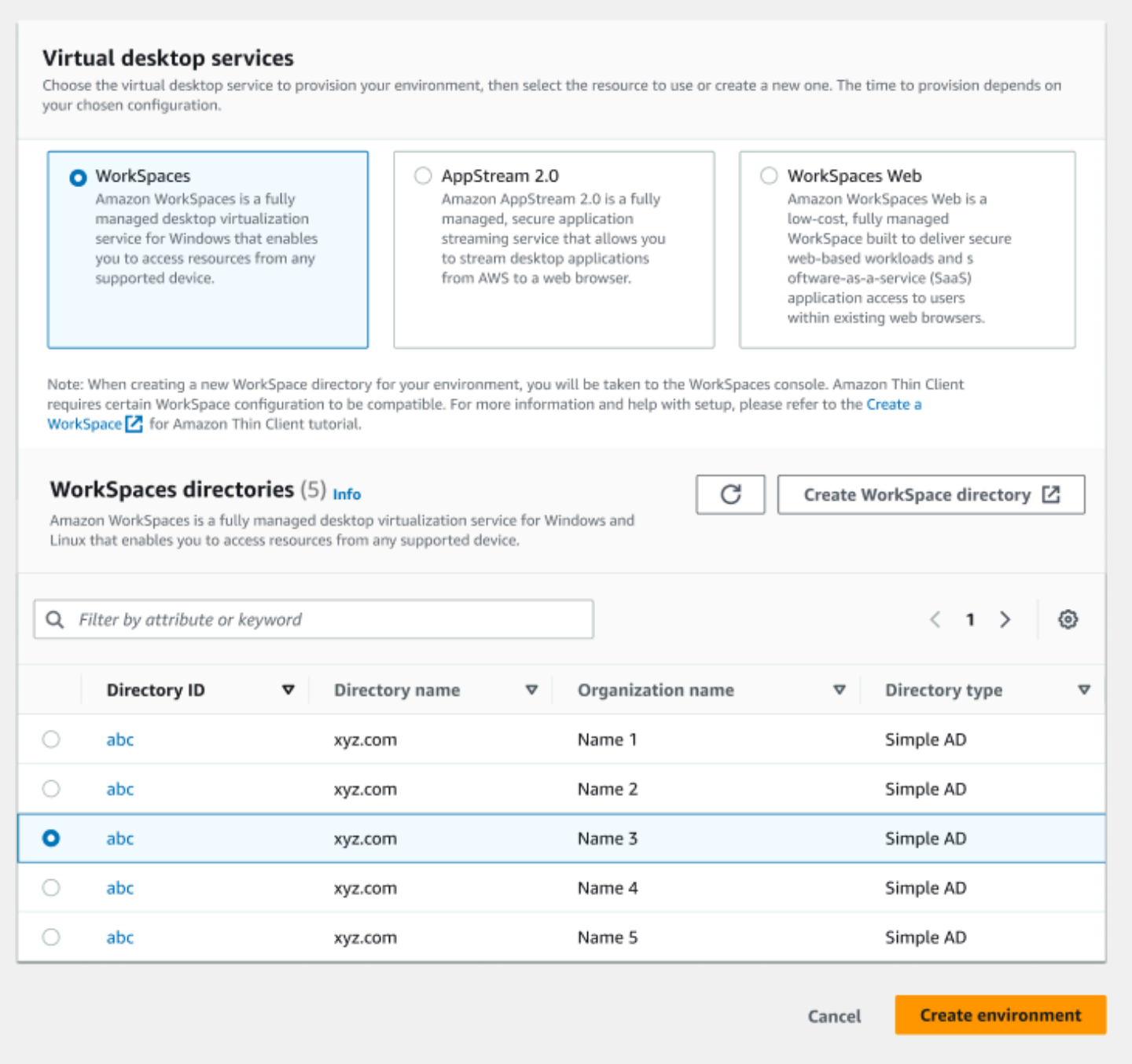
1. WorkSpacesAmazon을 사용하려면 다음 중 하나를 수행하십시오.

   - 그런 다음 환경에 사용하려는 디렉터리를 선택합니다. 드롭다운 목록을 살펴보거나 검색 필드를 사용하여 디렉터리를 검색할 수 있습니다.

     > **Note**
     >
     > 목록에 기존 디렉토리가 없는 경우 WorkSpaces Management Console에서 해당 디렉토리가 WorkSpaces 씬 클라이언트 요구 사항을 충족하는지 확인하십시오.

   - 디렉토리 생성 버튼을 선택하여 WorkSpaces 디렉토리를 생성합니다. 디렉터리 생성에 대한 자세한 내용은 WorkSpaces 디렉터리 관리를 참조하십시오. WorkSpaces

2. 환경 만들기 버튼을 선택합니다.



환경을 만들 때 나중에 세부 정보를 편집할 수 있습니다. 자세한 내용은 환경 편집을 참조하세요.

AppStream 2.0 사용

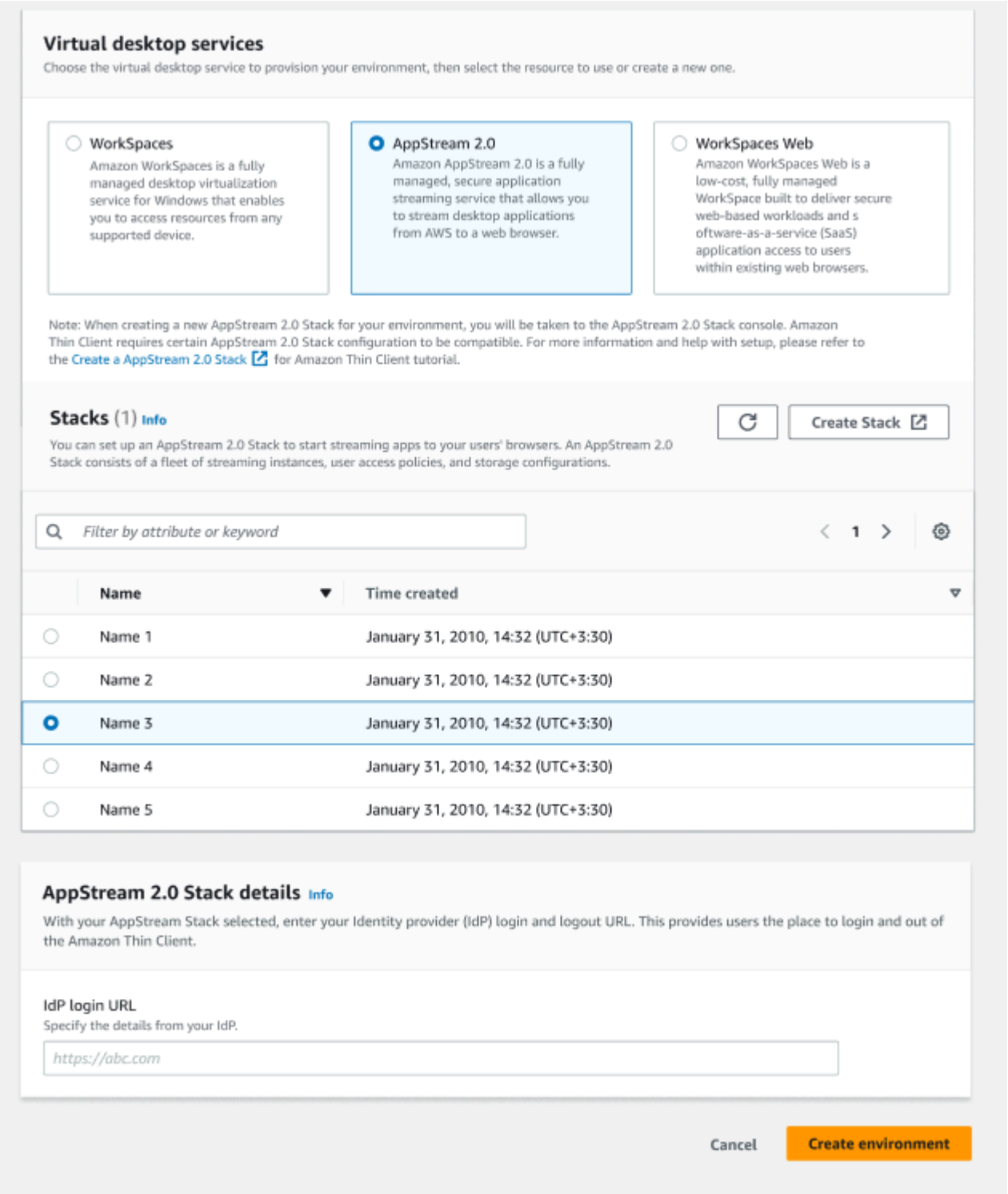
AppStream 2.0은 데스크톱 애플리케이션을 웹 브라우저로 스트리밍하는 데 사용할 수 있는 안전한 완전 관리형 애플리케이션 스트리밍 서비스입니다. AWS

> **Warning**
>
> AppStream 2.0 환경을 만들려면 로 `cli_follow_urlparam` 설정해야 합니다`false`. 이를 위해 다음을 수행합니다.
>
> - 기본 프로필의 경우 `aws configure set cli_follow_urlparam false`를 실행합니다.
> - 이름이 `ProfileName`인 프로필의 경우 `aws configure set cli_follow_urlparam false --profile ProfileName`을 실행합니다.

1. AppStream 2.0을 설정하려면 다음 중 하나를 수행하십시오.
   - 그런 다음 환경에 사용하려는 스택을 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 스택을 검색할 수 있습니다.

     > **Note**
     >
     > 목록에 기존 스택이 없는 경우 AppStream 2.0 Management Console에서 해당 스택이 WorkSpaces 씬 클라이언트 요구 사항을 충족하는지 확인하십시오.

   - 스택 생성 버튼을 선택하여 스택을 생성합니다. AppStream 2.0 스택 생성에 대한 자세한 내용은 스택 생성을 참조하십시오.
2. IdP 로그인 URL 필드에 ID 공급자 로그인 및 로그아웃 URL을 입력합니다. 이를 통해 사용자는 WorkSpaces 씬 클라이언트에 로그인하고 로그아웃할 수 있습니다.
3. 환경 생성 버튼을 선택합니다.



환경을 만든 후에도 세부 정보를 나중에 편집할 수 있습니다. 자세한 내용은 환경 편집을 참조하세요.

Amazon WorkSpaces 보안 브라우저 사용

Amazon WorkSpaces Secure Browser는 기존 웹 브라우저 내의 사용자에게 안전한 웹 기반 워크로드 및 SaaS (Software as a Service) 애플리케이션 액세스를 제공하도록 구축된 저렴한 완전 관리형 WorkSpaces 콘솔입니다.

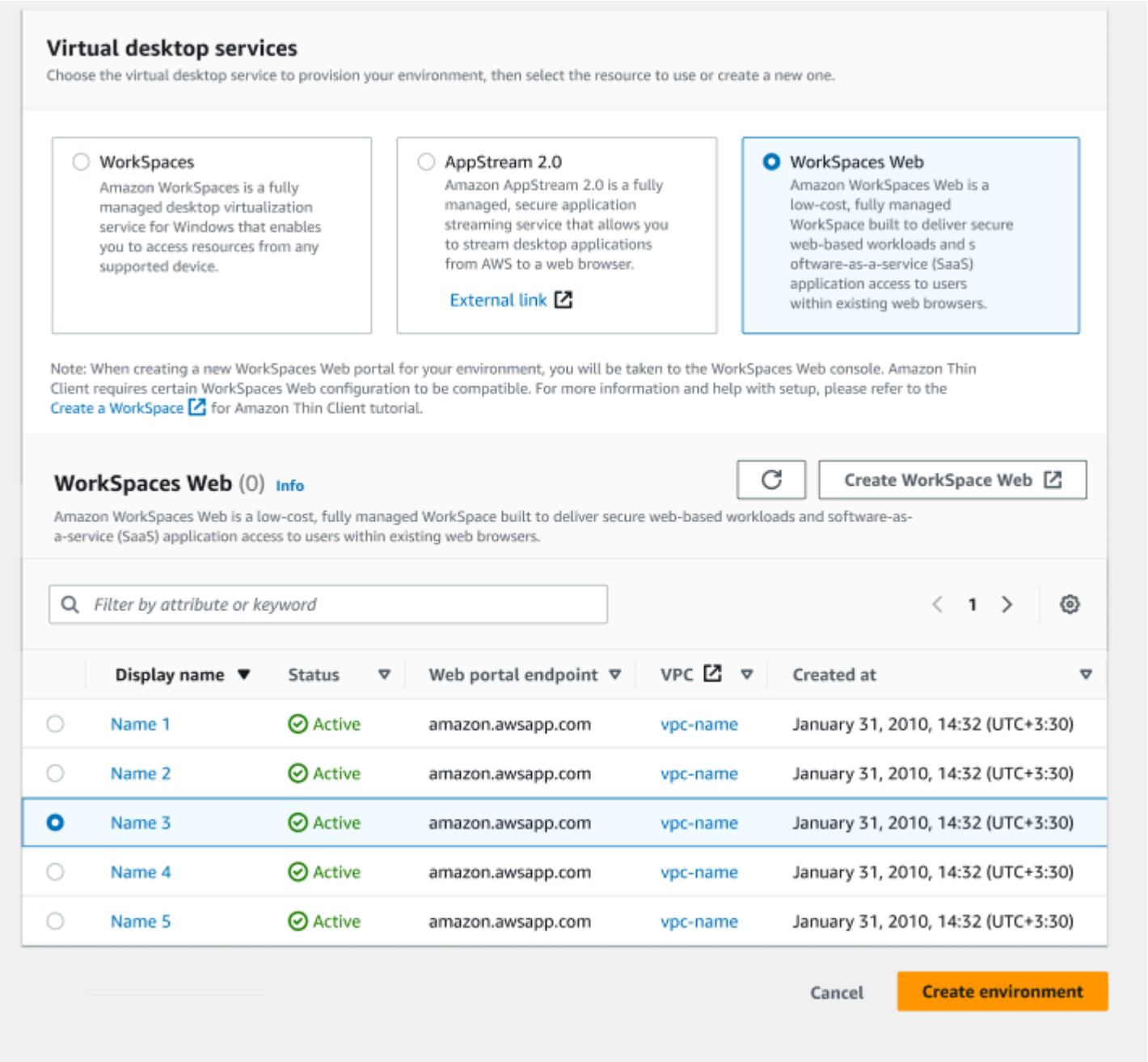
1. Amazon WorkSpaces 보안 브라우저를 설정하려면 다음 중 하나를 수행하십시오.

   - 환경에 사용할 웹 포털을 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 웹 포털을 검색할 수 있습니다.

     > **Note**
     >
     > 목록에 기존 웹 포털이 없는 경우 WorkSpaces Secure Browser Management Console에서 해당 포털이 WorkSpaces 씬 클라이언트 요구 사항을 충족하는지 확인하십시오.

   - WorkSpaces 보안 브라우저 생성 버튼을 선택하여 웹 포털을 생성합니다. WorkSpaces 보안 브라우저 웹 포털 생성에 대한 자세한 내용은 Amazon WorkSpaces 보안 브라우저 설정을 참조하십시오.

2. 환경 생성 버튼을 선택합니다.



환경을 만든 후에도 세부 정보를 나중에 편집할 수 있습니다. 자세한 내용은 환경 편집을 참조하세요.

3단계: 디바이스 사용자에게 활성화 코드 전송

환경 및 가상 데스크톱 서비스를 설정하고 나면 AWS Management Console에서 설정을 위한 고유한 활성화 코드를 받게 됩니다.

모든 WorkSpaces Thin Client 장치 사용자에게 이 활성화 코드를 제공하면 사용자가 이 활성화 코드를 사용하여 가상 데스크톱에 액세스할 수 있습니다.

디바이스 사용자가 Amazon WorkSpaces Thin Client를 설정하는 데 도움이 되는 방법에 대한 추가 정보는 WorkSpaces 씬 클라이언트 사용 설명서를 참조하십시오.

환경 편집

WorkSpaces Thin Client 관리 콘솔은 개별 사용자의 가상 데스크톱 환경을 관리합니다. 이 콘솔에서 가상 데스크톱 환경을 편집하거나 삭제할 수 있습니다.

1. 편집할 환경을 선택합니다.

   > **Note**
   >
   > 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 환경을 검색할 수 있습니다.

2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 편집을 선택합니다. 환경 편집 창으로 이동합니다.
4. 다음 중 원하는 항목을 편집합니다.
   - 환경 이름 필드에서 환경의 이름을 변경합니다.
   - 자동 소프트웨어 패치 업데이트의 소프트웨어 업데이트 세부 정보 확인란을 변경합니다.
   - 환경의 유지 관리 기간을 예약하려는 시기를 변경합니다.
5. 환경 편집 버튼을 선택합니다.

환경 삭제

> **Note**
>
> 등록된 디바이스가 있는 환경은 삭제할 수 없습니다. 먼저 환경의 모든 디바이스를 등록 취소한 후 삭제해야 합니다.

1. 삭제할 환경을 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 환경을 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 삭제를 선택합니다. 환경 삭제 확인 창이 나타납니다.
4. 확인 필드에 '삭제'를 입력합니다.

5. 삭제 버튼을 선택합니다.

디바이스

각 WorkSpaces Thin Client 최종 사용자는 가상 데스크톱 환경 및 온라인 리소스에 연결하는 전용 장치를 가지고 있습니다. 이러한 장치는 AWS 사이트의 WorkSpaces Thin Client 관리자 콘솔을 통해 관리됩니다.

이 콘솔에서 팀을 위한 디바이스를 주문할 수 있습니다.

디바이스 목록

디바이스 목록 세부 정보

디바이스 ID - 개별 디바이스에 할당된 식별 번호입니다.

디바이스 이름 - (선택 사항) 디바이스에 부여하는 고유한 이름입니다.

활동 상태 - 장치의 현재 상태입니다. 두 가지 상태 상태가 있습니다.

- 활성 - 지난 7일 동안 네트워크에 한 번 이상 연결되었습니다.
- 비활성 - 지난 7일 동안 네트워크에 연결되지 않았습니다.

등록 상태 - 장치가 설정되었고, 이 AWS 계정과 연결되어 있으며, 특정 환경에 속해 있는지 확인합니다. 상태는 다음 중 하나일 수 있습니다.

- 등록됨 - 기본 상태입니다.
- 등록 취소 - 장치가 재설정 및 등록 취소 프로세스 중입니다.

> **Note**
>
> 등록 취소 상태인 경우 장치를 삭제할 수 있습니다.

- 등록 취소됨 - 디바이스가 성공적으로 등록 취소되었습니다.

> **Note**
>
> 등록 취소 또는 등록 취소 상태인 경우에만 장치를 삭제할 수 있습니다.

- 보관됨 - 디바이스가 보관되었습니다.

환경 ID - 이 디바이스가 연결된 환경의 식별자입니다.

소프트웨어 규정 준수 - 디바이스 소프트웨어의 규정 준수 상태입니다. 두 가지 상태 상태가 있습니다.

- 규정 준수
- 규정 미준수

디바이스 목록 작업

검색 - 관리하는 모든 디바이스를 검색합니다.

새로 고침 - 디바이스 목록을 새로 고칩니다.

세부 정보 보기 - 디바이스 세부 정보를 표시합니다.

작업 - 다음 작업을 수행할 수 있는 드롭다운 목록을 엽니다.

- 디바이스 이름 편집
- 등록 취소
- 아카이브
- 삭제
- 디바이스 세부 정보 내보내기

디바이스 주문 - 디바이스 주문 프로세스를 시작합니다.

주제

- 디바이스 세부 정보
- 디바이스 이름 편집
- 디바이스 재설정 및 등록 취소
- 디바이스 보관
- 디바이스 삭제
- 디바이스 세부 정보 내보내기

디바이스 세부 정보

요약

장치 일련 번호 - 개별 장치에 할당된 식별 번호입니다.

ARN - Amazon 리소스 이름 (ARN) 형식의 디바이스 고유 식별자입니다.

디바이스 이름 - 디바이스에 부여하는 이름. 이름을 만들지 않은 경우 이름을 지정할 수 있습니다. 그렇지 않으면 기본 이름이 지정됩니다.

장치 유형 - 계정에 연결된 최종 사용자 장치의 유형입니다.

작동 상태 - 이 디바이스의 현재 상태입니다. 두 가지 상태 상태는 다음과 같습니다.

- 활성
- 비활성

환경 ID - 장치가 사용하는 환경의 식별 번호입니다.

등록 상태 - 장치가 설정되었고, 이 AWS 계정과 연결되어 있으며, 특정 환경에 속해 있음을 확인합니다. 다음 네 가지 상태 중 하나일 수 있습니다.

- 등록됨 - 기본 상태입니다.
- 등록 취소 - 장치가 재설정 및 등록 취소 프로세스 중입니다.
- 등록 취소됨 - 디바이스가 성공적으로 등록 취소되었습니다.

> **Note**
>
> 장치가 등록 취소됨 또는 보관됨 상태인 경우에만 장치를 삭제할 수 있습니다.

- 보관됨 - 관리자가 이 장치를 현재 서비스 중이 아닌 것으로 표시했습니다.

등록 날짜 - 디바이스가 활성화된 날짜입니다.

마지막으로 로그인한 시간 - 가장 최근에 로그인한 날짜와 시간입니다.

마지막 상태 점검 날짜 - 가장 최근에 장치를 체크인한 날짜 및 시간.

현재 소프트웨어 버전 - 이 디바이스가 현재 사용하고 있는 소프트웨어 버전입니다.

소프트웨어 업데이트 예약 - 디바이스에 예약된 소프트웨어 버전입니다.

소프트웨어 규정 준수 - 소프트웨어 세트가 유효한지 확인합니다. 두 가지 상태 상태가 있습니다.

- 규정 준수
- 규정 미준수

사용자 로그

마지막 장치 액세스 - 이 장치를 마지막으로 사용한 날짜 및 시간입니다.

디바이스 이름 편집

1. 편집할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 장치를 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 장치 이름 편집을 선택합니다. 장치 이름 편집 창이 나타납니다.
4. 디바이스 이름 확인 필드에 새 디바이스 이름을 입력합니다.
5. 저장 버튼을 선택합니다.

디바이스 재설정 및 등록 취소

1. 등록 취소할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 장치를 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 등록 취소를 선택합니다. 등록 취소 창이 나타납니다.
4. 확인 필드에 '등록 취소'를 입력합니다.
5. 등록 취소 버튼을 선택합니다.

> **Note**
>
> 강제로 등록을 취소하면 사용자가 로그아웃되며 세션 도중에 WorkSpaces 씬 클라이언트 디바이스를 재부팅해야 합니다.

디바이스 보관

1. 보관할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 디바이스를 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 아카이브를 선택합니다. 아카이브 창이 나타납니다.
4. 확인 필드에 '재설정 및 보관'을 입력합니다.
5. 재설정 및 보관 버튼을 선택합니다.

> **Note**
>
> 디바이스를 보관하면 사용자가 강제로 로그아웃되며 세션 도중에 WorkSpaces 씬 클라이언트 디바이스를 재부팅해야 합니다.

디바이스 삭제

1. 삭제할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 장치를 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 삭제를 선택합니다. 삭제 창이 나타납니다.
4. 확인 필드에 '삭제'를 입력합니다.
5. 삭제 버튼을 선택합니다.

> **Note**
>
> 디바이스가 성공적으로 삭제되면 사용자는 WorkSpaces 씬 클라이언트 디바이스를 Amazon에 반환해야 합니다.

디바이스 세부 정보 내보내기

1. 세부 정보를 내보내려는 디바이스를 선택합니다. 드롭다운 목록을 살펴보거나 검색 필드를 사용하여 디바이스를 검색할 수 있습니다.

2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 장치 세부 정보 내보내기를 선택합니다. 선택한 장치의 세부 정보가 스프레드시트 형식으로 다운로드됩니다.

소프트웨어 업데이트

WorkSpaces 씬 클라이언트에는 새로운 기능을 도입하고 보안 패치를 적용하는 소프트웨어 업데이트가 필요한 경우가 있습니다. 이러한 업데이트는 버전이 지정된 소프트웨어 세트로 표시됩니다.

소프트웨어 세트에는 WorkSpaces 씬 클라이언트 장치의 소프트웨어 애플리케이션 또는 운영 체제에 대한 업데이트가 포함될 수 있습니다. 이 콘솔에서 소프트웨어를 즉시 업데이트하도록 선택하거나 해당 환경의 유지 관리 기간 동안 자동 업데이트를 예약할 수 있습니다.

릴리스된 소프트웨어 세트 목록은 WorkSpaces 씬 클라이언트 환경 소프트웨어 세트를 참조하십시오.

주제

- 환경 소프트웨어 업데이트
- 디바이스 소프트웨어 업데이트
- WorkSpaces 씬 클라이언트 소프트웨어 릴리스

환경 소프트웨어 업데이트

WorkSpaces 씬 클라이언트는 사용자에게 가상 데스크톱에 대한 액세스를 제공하는 AWS 최종 사용자 컴퓨팅 서비스입니다. 이러한 가상 데스크톱은 새 소프트웨어 세트로 정기적으로 업데이트됩니다. 환경 소프트웨어를 업데이트하려면 다음과 같이 하십시오.

1. 사용 가능한 소프트웨어 업데이트의 목록에서 소프트웨어 세트를 선택합니다. 소프트웨어 세트 목록은 WorkSpaces 씬 클라이언트 환경 소프트웨어 세트를 참조하십시오.
2. 설치 버튼을 선택합니다.
3. 페이지 상단에서 환경을 선택합니다.
4. 환경 섹션의 목록에서 업데이트할 환경을 선택합니다.
5. 업데이트 예약에서 다음 중 하나를 선택하여 환경을 업데이트할 시기를 선택합니다.
    - 지금 소프트웨어 업데이트 - 등록된 모든 디바이스에서 환경 소프트웨어 업데이트를 시작합니다.

> **Note**
>
> 지금 소프트웨어를 업데이트하면 활성 사용자 세션이 모두 중단될 수 있습니다.

- 각 환경 유지 관리 기간 동안 소프트웨어 업데이트 - 해당 환경의 예약된 유지 관리 기간 동안 환경 소프트웨어를 업데이트합니다.

6. 확인란을 선택하여 업데이트를 승인합니다. 이 상자를 선택해야 소프트웨어가 업데이트됩니다.
7. 설치 버튼을 선택합니다.

디바이스 소프트웨어 업데이트

WorkSpaces 씬 클라이언트는 사용자를 전용 가상 데스크톱에 연결하는 씬 클라이언트 디바이스를 제공하는 AWS 최종 사용자 컴퓨팅 서비스입니다. 이러한 장치는 새 소프트웨어로 정기적으로 업데이트됩니다. 장치 소프트웨어를 업데이트하려면 다음과 같이 하십시오.

1. 사용 가능한 소프트웨어 업데이트의 목록에서 소프트웨어 세트를 선택합니다.
2. 설치 버튼을 선택합니다.
3. 페이지 상단에서 디바이스를 선택합니다.
4. 장치 섹션의 목록에서 업데이트할 장치를 하나 또는 여러 개 선택합니다. 소프트웨어 세트 목록은 WorkSpaces 씬 클라이언트 환경 소프트웨어 세트를 참조하십시오.
5. 업데이트 예약 옵션에서 다음 중 하나를 선택하여 환경을 업데이트할 시기를 선택합니다.

   - 지금 소프트웨어 업데이트 - 디바이스 소프트웨어를 즉시 업데이트합니다.

   > **Note**
   >
   > 지금 소프트웨어를 업데이트하면 활성 사용자 세션이 모두 중단될 수 있습니다.

   - 각 장치 유지 관리 기간 동안 소프트웨어 업데이트 - 장치의 예약된 유지 관리 기간 동안 환경 소프트웨어를 업데이트합니다.

6. 확인란을 선택하여 업데이트를 승인합니다. 이 상자를 선택해야 소프트웨어가 업데이트됩니다.
7. 설치 버튼을 선택합니다.

WorkSpaces 씬 클라이언트 소프트웨어 릴리스

WorkSpaces 씬 클라이언트는 사용자에게 디바이스의 가상 데스크톱에 대한 액세스를 제공하는 AWS 최종 사용자 컴퓨팅 서비스입니다. 이러한 장치는 새 소프트웨어 세트로 정기적으로 업데이트됩니다. 다음 표에는 출시된 모든 소프트웨어 세트가 설명되어 있습니다. 관리자는 AWS 관리 콘솔을 사용하여 사용 가능한 소프트웨어 세트를 볼 수 있습니다.

소프트웨어 세트	릴리스 날짜	변경
2.5.0	06-13-2024	• 세션을 시작하기 전에 절전 모드에서 깨어났을 때 장치가 키보드 및 마우스 설정 화면을 잠시 표시하던 문제를 수정했습니다. • 장치 도구 모음의 홈 버튼 이름이 로그인으로 변경되었습니다. • 세션의 오디오/비디오 통화 성능이 개선되었습니다.
2.4.3	05-29-2024	• 크로미엄의 CVE-2024-5274 중요 보안 문제에 대한 제로데이 수정
2.4.2	05-17-2024	• 크로미엄의 CVE-2024-4947 중요 보안 문제에 대한 제로데이 수정
2.4.1	05-15-2024	• 크로미엄의 CVE-2024-4671 및 CVE-2024-4761 중요 보안 문제에 대한 제로데이 픽스가 적용되었습니다. • WorkSpaces 로그인 페이지의 AWS 및 Privacy 링크를 마우스 오른쪽 버튼으로 클릭하여 브라우저를 독립 실

소프트웨어 세트	릴리스 날짜	변경
		행형 모드로 열 수 있던 문제를 수정했습니다.
2.4.0	05-09-2024	• 'accounts.google.com'을 차단하고 구글 워크스페이스를 2.0 세션의 IDP로 사용할 수 없는 문제를 수정했습니다. AppStream • 장치 설정 도구 모음은 화면의 아무 영역에서나 클릭 한 번으로 자동으로 축소됩니다.
2.3.0	04-05-2024	• 장치 설정이 축소된 도구 모음에 표시되므로 보이는 화면을 더 잘 활용할 수 있습니다. • 이제 최종 사용자는 디바이스가 비활성 상태로 전환될 때까지 대기하도록 시간을 구성할 수 있습니다. • 두 번째 디스플레이에 “about:blank” URL이 표시되는 문제를 수정했습니다. • 확장 디스플레이를 닫았을 때 흰색 화면이 나타나는 문제를 수정했습니다. • 이제 최종 사용자가 설정한 볼륨 레벨이 기기를 다시 시작해도 계속 유지됩니다.

소프트웨어 세트	릴리스 날짜	변경
2.2.1	02-16-2024	• 로그인 프로세스 중에 사용자가 SAML 2.0 인증으로 WorkSpaces 구성된 상태로 로그인할 수 없는 문제가 수정되었습니다.
2.2.0	02-08-2024	• 영어 (영국), 프랑스어, 독일어, 이탈리아어, 스페인어 로케일을 사용하는 ISO 키보드에 대한 지원이 추가되었습니다.
2.1.2	01-26-2024	• 크로미엄의 CVE-2024-0519 중요 보안 문제에 대한 제로데이 수정 • 잠금 기능과 관련된 최종 사용자 지연 시간 개선. • 내부 기기 연결 엔드포인트는 'thinclient*' 도메인으로 전환됩니다.
2.1.1	12-21-2023년	• 크로미엄의 CVE-2023-7024 중요 보안 문제에 대한 제로데이 수정
2.1.0	12-20-2023년	• 장치 설정에 홈 버튼을 추가하고 메타 키 지원을 활성화합니다. 이렇게 하면 최종 사용자가 Meta+L을 눌러 잠금 화면을 호출할 수 있습니다.
2.0.1	12-06-2023년	• 크로미엄의 CVE-2024-6345 중요 보안 문제에 대한 제로데이 수정
2.0.0	11-15-2023년	• 최초 릴리스

WorkSpaces 씬 클라이언트 리소스에서 태그 사용

각 리소스에 고유한 메타데이터를 태그로 할당하여 WorkSpaces 씬 클라이언트의 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 사용하여 AWS 리소스를 관리하고 결제 데이터를 비롯한 데이터를 정리할 수 있는 간단하면서도 강력한 방법으로 사용할 수 있습니다.

기존 리소스에 태그를 추가하면 해당 태그는 다음 달 첫날까지 비용 할당 보고서에 표시되지 않습니다. 예를 들어 7월 15일에 기존 WorkSpaces Thin Client 디바이스에 태그를 추가하면 8월 1일이 되어서야 비용 할당 보고서에 태그가 표시됩니다. 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

> **Note**
>
> Cost Explorer에서 WorkSpaces 씬 클라이언트 리소스 태그를 보려면 사용 설명서의 사용자 정의 비용 할당 태그 활성화에 나와 있는 지침에 따라 WorkSpaces 씬 클라이언트 리소스에 적용한 태그를 활성화해야 합니다.AWS Billing
> 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 씬 클라이언트 리소스에 해당 기간 동안 요금이 발생해야 합니다. Cost Explorer에는 태그가 활성화된 시점의 비용 데이터만 표시됩니다. 현재로서는 과거 데이터가 제공되지 않습니다.

태그를 지정할 수 있는 리소스:

- 태그를 생성할 때 WorkSpaces 씬 클라이언트 환경과 같은 리소스에 태그를 추가할 수 있습니다.
- WorkSpaces 씬 클라이언트 환경, 디바이스, 소프트웨어 세트 등 유형의 기존 리소스에 태그를 추가할 수 있습니다.

태그 제한

- 리소스당 최대 태그 수 - 50개
- 최대 키 길이—유니코드 128자
- 최대 값 길이—유니코드 문자 256자

- 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:`접두사는 사용하도록 예약되어 있으므로 태그 이름이나 값에 사용하지 마십시오. AWS 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다.

콘솔을 사용하여 기존 환경의 태그를 업데이트하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 환경을 선택하여 세부 정보 페이지를 엽니다.
3. 편집을 선택합니다.
4. 태그 섹션에서 다음 중 하나 이상을 수행하십시오.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
   - 태그를 업데이트하려면 Value 값을 편집하십시오.
   - 태그를 삭제하려면 태그 옆에 있는 제거를 선택합니다.
5. 태그 업데이트를 마치면 [Save] 를 선택합니다.

콘솔을 사용하여 기존 장치의 태그를 업데이트하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 디바이스를 선택하여 해당 세부 정보 페이지를 엽니다.
3. [Tags]를 선택합니다.
4. 태그 관리를 선택합니다.
5. 다음 중 한 개 이상을 수행할 수 있습니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
   - 태그를 업데이트하려면 Value 값을 편집하십시오.
   - 태그를 삭제하려면 태그 옆에 있는 제거를 선택합니다.
6. 태그 업데이트를 마치면 [Save] 를 선택합니다.

콘솔을 사용하여 소프트웨어 업데이트의 태그를 업데이트하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 소프트웨어 업데이트를 선택하여 해당 세부 정보 페이지를 엽니다.

3. 태그 섹션에서 태그 관리를 선택합니다.
4. 다음 중 한 개 이상을 수행할 수 있습니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
   - 태그를 업데이트하려면 Value 값을 편집하십시오.
   - 태그를 삭제하려면 태그 옆에 있는 제거를 선택합니다.
5. 태그 업데이트를 마치면 [Save] 를 선택합니다.

Amazon WorkSpaces 씬 클라이언트의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다.

보안은 기업과 기업 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. Amazon WorkSpaces Thin Client에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 WorkSpaces 씬 클라이언트를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 WorkSpaces 씬 클라이언트를 구성하는 방법을 보여줍니다. 또한 WorkSpaces 씬 클라이언트 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 배울 수 있습니다.

주제

Amazon WorkSpaces 씬 클라이언트의 데이터 보호

AWS 공동 책임 모델 Amazon WorkSpaces Thin Client의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 은 (는) 모두를 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API 또는 SDK를 AWS 서비스 사용하여 WorkSpaces 씬 클라이언트 또는 다른 클라이언트로 작업하는 경우가 포함됩니다. AWS CLI AWS 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 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

Amazon WorkSpaces Thin Client는 WorkSpaces 씬 클라이언트 디바이스의 사용자 사용 및 가상 데스크톱 서비스와의 상호 작용에 대한 정보를 수집하고 제공합니다. 가용 메모리, 네트워크 진단, 네트워크 정보, 디바이스 연결, SAML 자격 증명, 디바이스 식별 정보, 충돌 보고서 등을 예로 들 수 있습니다. 이 정보는 서비스를 제공하는 데 사용되며 서비스에 대한 사용자 경험을 개선하는 데 사용될 수 있습니다. 또한 서비스를 제공하기 위한 목적으로만 정보가 사용자가 서비스를 사용하는 AWS 지역 외부로 전송될 수 있습니다. 당사는 AWS 개인정보 취급방침에 따라 이 정보를 처리합니다.

주제

- 인터넷 업무 트래픽 프라이버시

데이터 암호화

WorkSpaces Thin Client는 사용자 설정, 장치 식별자, ID 제공자 정보, 스트리밍 데스크톱 식별자와 같은 환경 및 장치 사용자 지정 데이터를 수집합니다. WorkSpaces 씬 클라이언트는 세션 타임스탬프도 수집합니다. 수집된 데이터는 아마존 DynamoDB 및 아마존 S3에 저장됩니다. WorkSpaces 씬 클라이언트는 암호화에 AWS KMS (키 관리 서비스) 를 사용합니다.

콘텐츠를 보호하려면 다음 지침을 따릅니다.

- 최소 권한 액세스를 구현하고 WorkSpaces 씬 클라이언트 작업에 사용할 특정 역할을 생성합니다.
- 고객 관리 키를 end-to-end 제공하여 데이터를 보호하면 WorkSpaces Thin Client가 사용자가 제공한 키로 저장된 데이터를 암호화할 수 있습니다.
- 환경 활성화 코드와 사용자 보안 인증 정보를 공유하지 않도록 주의해야 합니다.
  - 관리자는 WorkSpaces 씬 클라이언트 콘솔에 로그인해야 하며, 사용자는 WorkSpaces 씬 클라이언트 설정을 위한 활성화 코드를 제공해야 하며 스트리밍 데스크톱에 로그인하려면 자격 증명을 사용해야 합니다.
  - 물리적으로 액세스할 수 있는 사람은 누구나 WorkSpaces 씬 클라이언트를 설정할 수 있지만 로그인을 위한 유효한 활성화 코드와 사용자 자격 증명이 없으면 세션을 시작할 수 없습니다.
- 사용자는 화면 잠금, 재부팅 또는 장치 도구 모음을 사용하여 장치 종료를 선택하여 세션을 명시적으로 종료할 수 있습니다. 이렇게 하면 디바이스 세션이 삭제되고 세션 보안 인증 정보가 지워집니다.

WorkSpaces Thin Client는 KMS로 모든 민감한 데이터를 암호화하여 기본적으로 콘텐츠와 메타데이터를 보호합니다. AWS 기존 설정을 적용하는 데 오류가 발생할 경우, 사용자는 새 세션에 액세스할 수 없고 디바이스는 소프트웨어 업데이트를 적용할 수 없습니다.

Amazon WorkSpaces 씬 클라이언트의 저장 데이터 암호화

Amazon WorkSpaces Thin Client는 기본적으로 암호화를 제공하여 저장된 민감한 고객 데이터를 AWS 자체 암호화 키를 사용하여 보호합니다.

- AWS 소유 키 — Amazon WorkSpaces Thin Client는 기본적으로 이러한 키를 사용하여 개인 식별 데이터를 자동으로 암호화합니다. AWS 소유 키를 확인, 관리 또는 사용하거나 사용 여부를 감사할 수 없습니다. 하지만 데이터를 암호화하는 키를 보호하기 위해 어떤 작업을 수행하거나 어떤 프로그램을 변경할 필요가 없습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서에서 AWS 소유 키를 참조하세요.

저장 데이터를 기본적으로 암호화하면 민감한 데이터 보호와 관련된 운영 오버헤드와 복잡성을 줄이는 데 도움이 됩니다. 동시에 엄격한 암호화 규정 준수 및 규제 요구 사항을 충족하는 안전한 애플리케이션을 구축할 수 있습니다.

이 암호화 계층을 비활성화하거나 다른 암호화 유형을 선택할 수는 없지만 씬 클라이언트 환경을 생성할 때 고객 관리형 키를 선택하여 기존 AWS 소유 암호화 키에 두 번째 암호화 계층을 추가할 수 있습니다.

- 고객 관리형 키 — Amazon WorkSpaces Thin Client는 사용자가 생성하고 소유하고 관리하는 대칭형 고객 관리 키를 사용하여 기존 AWS 소유 암호화에 두 번째 암호화 계층을 추가할 수 있도록 지원합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.
  - 키 정책 수립 및 유지
  - IAM 정책 및 권한 수립 및 유지
  - 키 정책 활성화 및 비활성화
  - 키 암호화 자료 교체
  - 태그 추가
  - 키 별칭 생성
  - 삭제를 위한 스케줄 키

자세한 내용은 AWS Key Management Service 개발자 안내서에서 고객 관리형 키를 참조하세요.

다음 표에는 Amazon WorkSpaces Thin Client가 개인 식별 데이터를 암호화하는 방법이 요약되어 있습니다.

데이터 유형	AWS 소유 키 암호화	고객 관리형 키 암호화 (선택 사항)
환경 이름 WorkSpaces 씬 클라이언트 환경 이름	활성화됨	활성화됨
디바이스 이름 WorkSpaces 씬 클라이언트 디바이스 이름	활성화됨	활성화됨

> **Note**
>
> Amazon WorkSpaces Thin Client는 AWS 자체 키를 사용하여 저장 시 암호화를 자동으로 활성화하여 개인 식별 데이터를 무료로 보호합니다.
> 하지만 고객 관리 키 사용에는 AWS KMS 요금이 적용됩니다. 요금에 대한 자세한 내용은 AWS 키 관리 서비스 요금을 참조하세요.

Amazon WorkSpaces 씬 클라이언트가 AWS KMS에서 보조금을 사용하는 방법

Amazon WorkSpaces Thin Client를 사용하려면 고객 관리 키를 사용하려면 허가가 필요합니다.

고객 관리 키로 암호화된 WorkSpaces 씬 클라이언트 환경을 생성하면 Amazon WorkSpaces Thin Client가 AWS KMS에 CreateGrant 요청을 전송하여 사용자 대신 승인을 생성합니다. AWS KMS의 부여는 Amazon WorkSpaces Thin Client에게 고객 계정의 KMS 키에 대한 액세스 권한을 부여하는 데 사용됩니다.

고객 관리 키를 사용하여 씬 클라이언트 암호화 환경에 새 WorkSpaces 씬 클라이언트 디바이스를 등록하고 해당 디바이스의 이름이 변경되면 Amazon WorkSpaces Thin Client는 AWS KMS에 CreateGrant 요청을 전송하여 사용자를 대신하여 승인을 생성합니다. AWS KMS의 부여는 Amazon WorkSpaces Thin Client에게 고객 계정의 KMS 키에 대한 액세스 권한을 부여하는 데 사용됩니다.

Amazon WorkSpaces Thin Client는 다음과 같은 내부 작업에 고객 관리 키를 사용하려면 권한 부여가 필요합니다.

- AWS KMS에 암호 해독 요청을 보내 암호화된 데이터를 해독하십시오.

언제든지 권한 부여에 대한 액세스를 취소하거나 고객 관리 키에 대한 서비스의 액세스 권한을 제거할 수 있습니다. 이렇게 하면 Amazon WorkSpaces Thin Client는 고객 관리 키로 암호화된 데이터에 액세스할 수 없게 되며, 이는 해당 데이터에 종속된 작업에 영향을 미칩니다. 예를 들어, Amazon WorkSpaces Thin Client가 액세스할 수 없는 환경 세부 정보를 가져오려고 하면 작업에서 `AccessDeniedException` 오류가 반환됩니다. 또한 WorkSpaces 씬 클라이언트 디바이스는 WorkSpaces 씬 클라이언트 환경을 사용할 수 없습니다.

고객 관리형 키 생성

AWS 관리 콘솔 또는 AWS KMS API 작업을 사용하여 대칭 고객 관리 키를 생성할 수 있습니다.

대칭형 고객 관리형 키를 생성하려면

AWS Key Management Service Developer 개발자 안내서에서 대칭형 고객 관리형 키 생성에 대한 단계를 따릅니다.

키 정책

키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서에서 고객 관리형 키 액세스 관리를 참조하세요.

Amazon WorkSpaces Thin Client 리소스에서 고객 관리형 키를 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- `kms:DescribeKey`— Amazon WorkSpaces Thin Client에서 키를 검증할 수 있도록 고객이 관리하는 키 세부 정보를 제공합니다.
- `kms:GenerateDataKey` - 고객 관리형 키를 사용하여 데이터를 암호화하도록 허용합니다.
- `kms:Decrypt` - 고객 관리형 키를 사용하여 데이터를 복호화하도록 허용합니다.
- `kms:CreateGrant` - 고객 관리형 키에 권한 부여를 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여하여 Amazon WorkSpaces Thin Client에 필요한 권한 부여 작업에 대한 액세스를 허용합니다. 권한 부여 사용에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

  이를 통해 Amazon WorkSpaces Thin Client는 다음을 수행할 수 있습니다.

  - `Decrypt`를 직접 호출하여 암호화된 데이터를 복호화합니다.

다음은 Amazon WorkSpaces Thin Client에 추가할 수 있는 정책 설명 예제입니다.

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

정책의 권한 지정에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

키 액세스 문제 해결에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.

WorkSpaces 씬 클라이언트의 고객 관리 키 지정

고객 관리 키를 다음 리소스에 대한 2차 계층 암호화로 지정할 수 있습니다.

- WorkSpaces 씬 클라이언트 환경

환경을 생성할 때 Amazon WorkSpaces Thin Client가 식별 가능한 개인 데이터를 암호화하는 데 사용하는 a를 제공하여 데이터 키를 지정할 수 있습니다. `kmsKeyArn`

- `kmsKeyArn`— AWS KMS 고객 관리 키의 키 식별자. 키 ARN을 제공합니다.

고객 관리 키로 암호화된 WorkSpaces 씬 클라이언트 환경에 새 WorkSpaces 씬 클라이언트 디바이스를 추가하면 WorkSpaces 씬 클라이언트 디바이스는 씬 클라이언트 환경의 고객 관리 키 설정을 상속합니다. WorkSpaces

암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함하는 선택적 키-값 쌍 집합입니다.

AWS KMS는 암호화 컨텍스트를 인증된 추가 데이터로 사용하여 인증된 암호화를 지원합니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함시키면 AWS KMS는 암호화 컨텍스트를 암호화된 데이터에 바인딩합니다. 데이터를 해독하려면 요청에 동일한 암호화 컨텍스트를 포함시키십시오.

Amazon WorkSpaces 씬 클라이언트 암호화 컨텍스트

Amazon WorkSpaces Thin Client는 모든 AWS KMS 암호화 작업에서 동일한 암호화 컨텍스트를 사용합니다. 여기서 키는 ARN (Amazon 리소스 이름) 이고 값은 Amazon 리소스 이름 (ARN) 입니다. `aws:thinclient:arn`

다음은 환경 암호화 컨텍스트입니다.

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

다음은 장치 암호화 컨텍스트입니다.

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

모니터링을 위한 암호화 컨텍스트 사용

대칭형 고객 관리 키를 사용하여 WorkSpaces 씬 클라이언트 환경 및 디바이스 데이터를 암호화하는 경우 감사 레코드 및 로그의 암호화 컨텍스트를 사용하여 고객 관리 키가 사용되는 방식을 식별할 수도 있습니다. 암호화 컨텍스트는 AWS CloudTrail 또는 Amazon Logs에서 생성된 CloudWatch 로그에도 나타납니다.

암호화 컨텍스트를 사용하여 고객 관리형 키에 대한 액세스 제어

그러나 키 정책 및 IAM 정책에서 암호화 컨텍스트를 조건으로 사용하여 대칭형 고객 관리형 키에 대한 액세스를 제어할 수도 있습니다. 또한 권한 부여에서 암호화 컨텍스트 제약 조건을 사용할 수 있습니다.

Amazon WorkSpaces Thin Client는 권한 부여의 암호화 컨텍스트 제약을 사용하여 계정 또는 지역의 고객 관리 키에 대한 액세스를 제어합니다. 권한 부여 제약 조건에 따라 권한 부여가 허용하는 작업은 지정된 암호화 컨텍스트를 사용해야 합니다.

다음은 특정 암호화 컨텍스트에서 고객 관리형 키에 대한 액세스 권한을 부여하는 키 정책 설명의 예시입니다. 이 정책 설명의 조건에 따라 `kms:Decrypt` 호출에는 암호화 컨텍스트를 지정하는 암호화 컨텍스트 제약 조건이 있어야 합니다.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Amazon WorkSpaces 씬 클라이언트의 암호화 키 모니터링

AWS KMS 고객 관리형 키를 Amazon WorkSpaces 씬 클라이언트 리소스와 함께 사용하는 AWS CloudTrail 경우 Amazon CloudWatch Logs를 사용하여 Amazon WorkSpaces 씬 클라이언트가 AWS KMS로 보내는 요청을 추적할 수 있습니다.

다음은 고객 관리 키로 암호화된 데이터에 액세스하기 위해 Amazon WorkSpaces Thin Client에서 호출하는 `DescribeKey` `CreateGrant` `GenerateDataKeyDecrypt`,,,, `Decrypt` (사용`Grant`) KMS 작업을 모니터링하기 위한 AWS CloudTrail 이벤트입니다.

다음 예제에서 WorkSpaces 씬 클라이언트 환경을 확인할 `encryptionContext` 수 있습니다. WorkSpaces 씬 클라이언트 디바이스에 대해서도 유사한 CloudTrail 이벤트가 기록됩니다.

DescribeKey

Amazon WorkSpaces Thin Client는 이 `DescribeKey` 작업을 사용하여 AWS KMS 고객 관리 키를 확인합니다.

다음 예제 이벤트는 `DescribeKey` 작업을 기록합니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
```

```
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateGrant

Amazon WorkSpaces Thin Client는 이 `CreateGrant` 작업을 사용하여 KMS Grant를 생성하며, 이를 통해 디바이스에서 데이터에 액세스할 때 데이터를 복호화할 수 있습니다.

다음 예제 이벤트는 `CreateGrant` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
```

```
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


GenerateDataKey

Amazon WorkSpaces Thin Client는 이 `GenerateDataKey` 작업을 사용하여 데이터를 암호화합니다.

다음 예제 이벤트는 GenerateDataKey 작업을 기록합니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
```

```
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces Thin Client는 `Decrypt` 작업을 사용하여 데이터를 복호화합니다.

다음 예제 이벤트는 `Decrypt` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
```

```
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Decrypt (using Grant)

WorkSpaces 씬 클라이언트 디바이스가 환경 또는 디바이스 정보에 액세스하면 `Decrypt` 작업이 사용되며 KMS 키를 통해 작업이 허용됩니다. `Grant`

다음 예제 이벤트는 a를 통해 승인된 `Decrypt` 작업을 기록합니다. `Grant`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

자세히 알아보기

다음 리소스에서 저장 데이터 암호화에 대한 추가 정보를 확인할 수 있습니다:

- AWS Key Management Service 기본 개념에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요.
- AWS Key Management Service의 보안 모범 사례에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

전송 중 암호화

WorkSpaces 씬 클라이언트는 HTTPS 및 TLS 1.2를 통해 전송 중인 데이터를 암호화합니다. 콘솔을 사용하거나 직접 API 호출을 사용하여 WorkSpaces 씬 클라이언트에 요청을 보낼 수 있습니다. 전송되는 요청 데이터는 HTTPS 또는 TLS 연결을 통해 전송하여 암호화됩니다. 요청 데이터는 AWS 콘솔, AWS 명령줄 인터페이스 또는 AWS SDK에서 씬 클라이언트로 전송할 수 있습니다. WorkSpaces 여기에는 디바이스의 모든 소프트웨어 업데이트도 포함됩니다.

전송 중 암호화 및 보안 연결(HTTPS, TLS)은 기본적으로 구성됩니다.

키 관리

자체 고객 관리형 AWS KMS 키를 제공하여 고객 정보를 암호화할 수 있습니다. 키를 제공하지 않으면 WorkSpaces 씬 클라이언트는 AWS 소유 키를 사용합니다. AWS SDK를 사용하여 키를 설정할 수 있습니다.

인터넷 업무 트래픽 프라이버시

관리자는 시작 시간 및 보류 중인 소프트웨어 업데이트 정보를 포함한 WorkSpaces Thin Client 세션 이벤트를 볼 수 있습니다. 이러한 로그는 암호화되어 WorkSpaces Thin Client 콘솔에서 고객에게 안전하게 전달됩니다. 개별 스트리밍 데스크톱 세션에 대한 사용자 정보 및 추가 세부 정보는 데스크톱 서비스에 기록됩니다. 자세한 내용은 모니터링, AppStream 2.0 모니터링 및 보고 또는 WorkSpaces 웹 용사용자 액세스 로깅을 참조하십시오. WorkSpaces

Amazon WorkSpaces 씬 클라이언트의 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 WorkSpaces Thin Client 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

고객

씬 클라이언트에서 WorkSpaces 수행하는 작업에 따라 AWS Identity and Access Management (IAM) 사용 방식이 다릅니다.

서비스 사용자 - WorkSpaces 씬 클라이언트 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 WorkSpaces 씬 클라이언트 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. WorkSpaces 씬 클라이언트의 기능에 액세스할 수 없는 경우 을 참조하십시오Amazon WorkSpaces 씬 클라이언트 ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 WorkSpaces 씬 클라이언트 리소스를 담당하는 경우 씬 클라이언트에 WorkSpaces 대한 전체 액세스 권한이 있을 것입니다. 서비스 사용자가 액세스해야 하는 WorkSpaces 씬 클라이언트 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사에서 WorkSpaces 씬 클라이언트와 함께 IAM을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오Amazon WorkSpaces 씬 클라이언트와 IAM의 작동 방식.

IAM 관리자 - IAM 관리자라면 씬 클라이언트에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다 WorkSpaces . IAM에서 사용할 수 있는 WorkSpaces 씬 클라이언트 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페

더레이션 ID의 예입니다. 연동 자격 증명으로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용자 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

연동 보안 인증

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용자 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 보안 인증입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증 정보만 제공합니다. 자세한 정보는 IAM 사용자 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기 섹션을 참조하세요. IAM 자격 증명 센터를 사용하는 경우 권한 집합을 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트 섹션을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입

니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용자 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증 정보를 얻을 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용자 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자

또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책의 권한이 요청 허용 또는 거부 여부를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용자 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

보안 인증 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 보안 인증에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용자 설명서의 IAM 정책 생성을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용자 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 특성입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 특성을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 자격 증명 기반 정책의 교집합과 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용자 설명서의 세션 정책을 참조하세요.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

Amazon WorkSpaces 씬 클라이언트와 IAM의 작동 방식

IAM을 사용하여 씬 클라이언트에 대한 액세스를 관리하기 전에 WorkSpaces 씬 클라이언트에서 사용할 수 있는 WorkSpaces IAM 기능에 대해 알아보십시오.

Amazon WorkSpaces 씬 클라이언트와 함께 사용할 수 있는 IAM 기능

IAM 특성	WorkSpaces 씬 클라이언트 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

WorkSpaces 씬 클라이언트 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

씬 클라이언트에 대한 ID 기반 정책 WorkSpaces

ID 기반 정책 지원	예

자격 증명기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수

행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 태스크와 리소스 뿐만 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용자 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

씬 클라이언트의 ID 기반 정책 예제 WorkSpaces

WorkSpaces 씬 클라이언트 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

씬 클라이언트 내의 리소스 기반 정책 WorkSpaces

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념합니다. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용자 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

WorkSpaces 씬 클라이언트에 대한 정책 조치

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

WorkSpaces 씬 클라이언트 작업 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Thin Client에서 정의한 작업을 참조하십시오.

WorkSpaces 씬 클라이언트의 정책 조치는 조치 앞에 다음 접두사를 사용합니다.

```
workspaces-thin-client
```

명령문 하나에 여러 작업을 지정하려면 다음 예와 같이 쉼표로 구분합니다.

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

WorkSpaces 씬 클라이언트 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

씬 클라이언트의 WorkSpaces 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 보고서에는 `Resource` 또는 `NotResource` 요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

WorkSpaces 씬 클라이언트 리소스 유형 및 ARN 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Thin Client에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 Amazon WorkSpaces Thin Client에서 정의한 작업을 참조하십시오.

WorkSpaces 씬 클라이언트 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

씬 클라이언트의 정책 조건 키 WorkSpaces

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 적음 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명령문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

WorkSpaces 씬 클라이언트 조건 키 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Thin Client의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon WorkSpaces Thin Client에서 정의한 작업을 참조하십시오.

WorkSpaces 씬 클라이언트 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

씬 클라이언트의 ACL WorkSpaces

ACL 지원	아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC (씬 클라이언트 포함) WorkSpaces

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우 값은 부분입니다.

ABAC에 대한 자세한 정보는 IAM 사용자 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용자 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

WorkSpaces 씬 클라이언트에서 임시 자격 증명 사용

임시 보안 인증 정보 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 기능이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증 정보를 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용자 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 정보 섹션을 참조하세요.

씬 클라이언트에 대한 WorkSpaces 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

WorkSpaces 씬 클라이언트의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 WorkSpaces 씬 클라이언트 기능이 중단될 수 있습니다. WorkSpaces 씬 클라이언트가 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

씬 클라이언트의 서비스 연결 역할 WorkSpaces

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 섹션을 참조하세요. Service-linked role(서비스 연결 역할) 열에서 Yes이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Amazon WorkSpaces 씬 클라이언트의 ID 기반 정책 예제

기본적으로 사용자와 역할은 WorkSpaces 씬 클라이언트 리소스를 생성하거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용자 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형의 ARN 형식을 비롯하여 WorkSpaces 씬 클라이언트에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조의 Amazon WorkSpaces Thin Client용 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례

- 씬 클라이언트 콘솔 사용 WorkSpaces
- WorkSpaces 씬 클라이언트에 읽기 전용 액세스 권한을 부여하십시오.
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- WorkSpaces 씬 클라이언트에 대한 전체 액세스 권한 부여

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 WorkSpaces 씬 클라이언트 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하십시오. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 관한AWS 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용자 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- Use conditions in IAM policies to further restrict access(IAM 정책의 조건을 사용하여 액세스 추가 제한) – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용자 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용자 설명서의 IAM Access Analyzer policy validation(IAM Access Analyzer 정책 검증)을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용자 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용자 설명서의 IAM의 보안 모범 사례를 참조하세요.

씬 클라이언트 콘솔 사용 WorkSpaces

Amazon WorkSpaces Thin Client 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 자신의 WorkSpaces 씬 클라이언트 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

WorkSpaces 씬 클라이언트에 읽기 전용 액세스 권한을 부여하십시오.

이 예제는 IAM 사용자가 WorkSpaces 씬 클라이언트 구성을 볼 수는 있지만 변경할 수는 없도록 하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 AWS CLI 또는 AWS API를 사용하여 콘솔 또는 프로그램에서 이 작업을 완료할 수 있는 권한이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces 씬 클라이언트에 대한 전체 액세스 권한 부여

이 예제는 WorkSpaces 씬 클라이언트 IAM 사용자에게 전체 액세스 권한을 부여하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 AWS CLI 또는 AWS API를 사용하여 콘솔 또는 프로그램에서 모든 WorkSpaces 씬 클라이언트 작업을 완료할 수 있는 권한이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
```

```
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Amazon WorkSpaces 씬 클라이언트 ID 및 액세스 문제 해결

다음 정보를 사용하면 WorkSpaces 씬 클라이언트 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 WorkSpaces 씬 클라이언트에서 작업을 수행할 권한이 없습니다.
- 액세스 키를 보아야 합니다.
- 저는 관리자이며 다른 사람들이 WorkSpaces Thin Client에 액세스할 수 있도록 허용하고 싶습니다.
- 외부 사용자가 내 WorkSpaces 씬 클라이언트 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

저는 WorkSpaces 씬 클라이언트에서 작업을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-thin-client-device`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `workspaces-thin-client:`*`ListDevices`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

이 경우 Mateo는 관리자에게 작업을 사용하여 *`my-thin-client-device`* 리소스에 액세스할 수 있도록 정책을 업데이트해 달라고 요청합니다`workspaces-thin-client:`*`ListDevices`*.

액세스 키를 보아야 합니다.

IAM 사용자 액세스 키를 생성한 후에는 언제든지 액세스 키 ID를 볼 수 있습니다. 하지만 보안 액세스 키는 다시 볼 수 없습니다. 보안 액세스 키를 잃어버린 경우 새로운 액세스 키 페어를 생성해야 합니다.

액세스 키는 액세스 키 ID(예: AKIAIOSFODNN7EXAMPLE)와 보안 액세스 키(예: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)의 두 가지 부분으로 구성됩니다. 사용자 이름 및 암호와 같이 액세스 키 ID와 보안 액세스 키를 함께 사용하여 요청을 인증해야 합니다. 사용자 이름과 암호를 관리하는 것처럼 안전하게 액세스 키를 관리합니다.

> **Important**
>
> 정식 사용자 ID를 찾는 데 도움이 되더라도 액세스 키를 타사에 제공하지 마시기 바랍니다. 이렇게 하면 다른 사람에게 내 계정에 대한 영구적인 액세스 권한을 부여할 수 있습니다. AWS 계정

액세스 키 페어를 생성할 때는 액세스 키 ID와 보안 액세스 키를 안전한 위치에 저장하라는 메시지가 나타납니다. 보안 액세스 키는 생성할 때만 사용할 수 있습니다. 하지만 보안 액세스 키를 잃어버린 경우 새로운 액세스 키를 IAM 사용자에게 추가해야 합니다. 최대 두 개의 액세스 키를 가질 수 있습니다. 이미 두 개가 있는 경우 새로 생성하려면 먼저 키 페어 하나를 삭제해야 합니다. 지침을 보려면 IAM 사용 설명서의 액세스 키 관리 단원을 참조하십시오.

저는 관리자이며 다른 사람들이 WorkSpaces Thin Client에 액세스할 수 있도록 허용하고 싶습니다.

다른 사람이 WorkSpaces Thin Client에 액세스할 수 있도록 하려면 액세스가 필요한 개인 또는 애플리케이션에 대한 IAM 엔티티 (사용자 또는 역할) 를 생성해야 합니다. 다른 사용자들은 해당 엔터티에 대한 보안 인증을 사용해 AWS에 액세스합니다. 그런 다음 WorkSpaces Thin Client에서 올바른 권한을 부여하는 정책을 엔티티에 연결해야 합니다.

바로 시작하려면 IAM 사용 설명서의 첫 번째 IAM 위임 사용자 및 그룹 생성을 참조하십시오.

자세한 설명은 WorkSpaces 씬 클라이언트에 대한 전체 액세스 권한 부여 섹션을 참조하세요.

외부 사용자가 내 WorkSpaces 씬 클라이언트 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- WorkSpaces 씬 클라이언트가 이러한 기능을 지원하는지 여부를 알아보려면 을 참조하십시오Amazon WorkSpaces 씬 클라이언트와 IAM의 작동 방식.
- 소유한 리소스에 대한 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오. AWS 계정
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 자격 증명 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용자 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용자 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조합니다.

Amazon WorkSpaces 씬 클라이언트의 레질리언스

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS 글로벌 인프라 외에도 WorkSpaces Thin Client는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다.

Amazon WorkSpaces 씬 클라이언트의 취약성 분석 및 관리

구성 및 IT 제어는 사용자와 사용자 간의 AWS 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

아마존 WorkSpaces 씬 클라이언트는 아마존, WorkSpaces 아마존 AppStream 2.0, 웹과 WorkSpaces 상호 통합됩니다. 각 서비스의 업데이트 관리에 대한 자세한 내용은 다음 링크를 참조하십시오.

- 아마존 AppStream 2.0의 업데이트 관리
- Amazon의 업데이트 관리 WorkSpaces
- Amazon WorkSpaces Web의 구성 및 취약성 분석

Amazon WorkSpaces 씬 클라이언트 모니터링

모니터링은 Amazon WorkSpaces Thin Client 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS WorkSpaces Thin Client를 감시하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 전화를 건 사용자와 계정 AWS, 호출이 이루어진 소스 IP 주소, 호출이 발생한 시간을 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

를 사용하여 Amazon WorkSpaces 씬 클라이언트 API 호출 로깅 AWS CloudTrail

Amazon WorkSpaces Thin Client는 씬 클라이언트에서 사용자, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다. AWS CloudTrail WorkSpaces CloudTrail WorkSpaces 씬 클라이언트에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 WorkSpaces 씬 클라이언트 콘솔에서의 호출과 WorkSpaces 씬 클라이언트 API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 WorkSpaces 씬 클라이언트에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷에 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 WorkSpaces Thin Client에 대한 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

WorkSpaces 씬 클라이언트 정보: CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. WorkSpaces Thin Client에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

WorkSpaces Thin Client의 이벤트를 AWS 계정포함하여 내 이벤트의 진행 중인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티

션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 WorkSpaces 씬 클라이언트 작업은 Amazon WorkSpaces 씬 클라이언트 API 참조에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어, `CreateEnvironment`, `ListDevices`, 및 `GetSoftwareSet` 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

WorkSpaces 씬 클라이언트 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `GetDevice` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
```

```
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

를 사용하여 Amazon WorkSpaces 씬 클라이언트 리소스 생성 AWS CloudFormation

Amazon WorkSpaces Thin Client는 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 와 AWS CloudFormation통합되어 있습니다. 이렇게 하면 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있습니다. 원하는 모든 AWS 리소스 (예: 환경) 를 설명하는 템플릿을 생성하고 해당 리소스를 AWS CloudFormation 프로비저닝 및 구성합니다.

를 사용하면 AWS CloudFormation템플릿을 재사용하여 WorkSpaces 씬 클라이언트 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 지역과 지역에 동일한 리소스를 반복적으로 프로비저닝하십시오.

WorkSpaces 씬 클라이언트 및 AWS CloudFormation 템플릿

WorkSpaces 씬 클라이언트 및 관련 서비스를 위한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML 형식의 형식이 지정된 텍스트 파일입니다. 이러한 템플릿은 스택에 프로비저닝하려는 리소스를 설명합니다. AWS CloudFormation JSON 또는 YAML 형식에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 템플릿을 시작하는 데 도움을 받을 수 있습니다. AWS CloudFormation 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

WorkSpaces 씬 클라이언트는 에서 환경 생성을 지원합니다. AWS CloudFormation환경용 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon WorkSpaces Thin Client 리소스 유형 참조를 참조하십시오.

에 대해 자세히 알아보십시오. AWS CloudFormation

자세히 AWS CloudFormation알아보려면 다음 리소스를 참조하십시오.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

인터페이스 엔드포인트 (AWS PrivateLink) 를 사용하여 Amazon WorkSpaces Thin Client에 액세스

를 AWS PrivateLink 사용하여 VPC와 Amazon WorkSpaces 씬 클라이언트 간에 프라이빗 연결을 생성할 수 있습니다. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결을 사용하지 않고 WorkSpaces 씬 클라이언트에 VPC로 액세스할 수 있습니다. AWS Direct Connect VPC의 인스턴스는 WorkSpaces 씬 클라이언트에 액세스하는 데 퍼블릭 IP 주소가 필요하지 않습니다.

에서 구동되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. AWS PrivateLink 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 씬 클라이언트로 향하는 트래픽의 진입점 역할을 하는 요청자 관리 네트워크 인터페이스입니다. WorkSpaces

자세한 내용은AWS PrivateLink 가이드의 AWS PrivateLink를 통해 AWS 서비스 에 액세스를 참조하세요.

씬 클라이언트 고려 사항 WorkSpaces

WorkSpaces 씬 클라이언트의 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 고려 사항을 검토하십시오.

WorkSpaces 씬 클라이언트는 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출을 지원합니다.

WorkSpaces 씬 클라이언트용 인터페이스 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()AWS CLI를 사용하여 WorkSpaces 씬 클라이언트용 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하십시오.

다음 서비스 이름을 사용하여 WorkSpaces 씬 클라이언트용 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.thinclient.api
```

인터페이스 엔드포인트에 프라이빗 DNS를 활성화하면 기본 지역 DNS 이름을 사용하여 WorkSpaces 씬 클라이언트에 API 요청을 할 수 있습니다. 예를 들어 `api.thinclient.us-east-1.amazonaws.com`입니다.

인터페이스 엔드포인트의 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 통해 WorkSpaces 씬 클라이언트에 대한 전체 액세스를 제공합니다. VPC에서 WorkSpaces Thin Client에 부여된 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결하십시오.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체(AWS 계정, IAM 사용자, IAM 역할)
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은AWS PrivateLink 가이드의 엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조하세요.

예: WorkSpaces 씬 클라이언트 작업에 대한 VPC 엔드포인트 정책

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책을 인터페이스 엔드포인트에 연결하면 모든 리소스의 모든 보안 주체에 대해 나열된 WorkSpaces 씬 클라이언트 작업에 대한 액세스 권한이 부여됩니다.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

WorkSpaces 씬 클라이언트 관리자 안내서의 문서 기록

다음 표에는 WorkSpaces 씬 클라이언트 관리자 안내서의 릴리스에 대한 설명서 기록이 설명되어 있습니다.

변경 사항	설명	날짜
• Amazon WorkSpaces 씬 클라이언트를 WorkSpaces 위한 구성 • 아마존 WorkSpaces 씬 클라이언트용 AppStream 2.0 구성	• 운영 체제 목록을 업데이트 했습니다. • ID 제공자 절차를 업데이트 했습니다.	2024년 2월 12일
최초 릴리스	최초 릴리스	2023년 11월 26일

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