aws

관리자 안내서

Amazon WorkSpaces 씬 클라이언트

Amazon WorkSpaces 씬 클라이언트: 관리자 안내서

Table of Contents

Amazon WorkSpaces 씬 클라이언트 관리자 콘솔이란 무엇입니까?

Amazon WorkSpaces 씬 클라이언트 관리자 콘솔을 사용하면 관리자는 WorkSpaces 씬 클라이언트 포털을 통해 WorkSpaces 씬 클라이언트 환경 및 디바이스를 관리할 수 있습니다. 관리자는 이 웹 콘솔에서 환경을 생성하고, 디바이스를 관리하고, 네트워크 내의 WorkSpaces 씬 클라이언트 사용자에 대한 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 조건 및 구성에 나열되어 있습니다.

주제

를 처음 사용하십니까?

WorkSpaces 씬 클라이언트 관리자 콘솔을 처음 사용하는 경우 먼저 다음 섹션을 읽을 것을 권장합니다.

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

아키텍처

각 WorkSpaces 씬 클라이언트는 가상 데스크톱 인터페이스(VDI) 공급자와 연결됩니다. WorkSpaces 씬 클라이언트는 세 가지 VDI 공급자를 지원합니다.

- Amazon WorkSpaces

- AppStream 2.0
- Amazon WorkSpaces Secure Browser

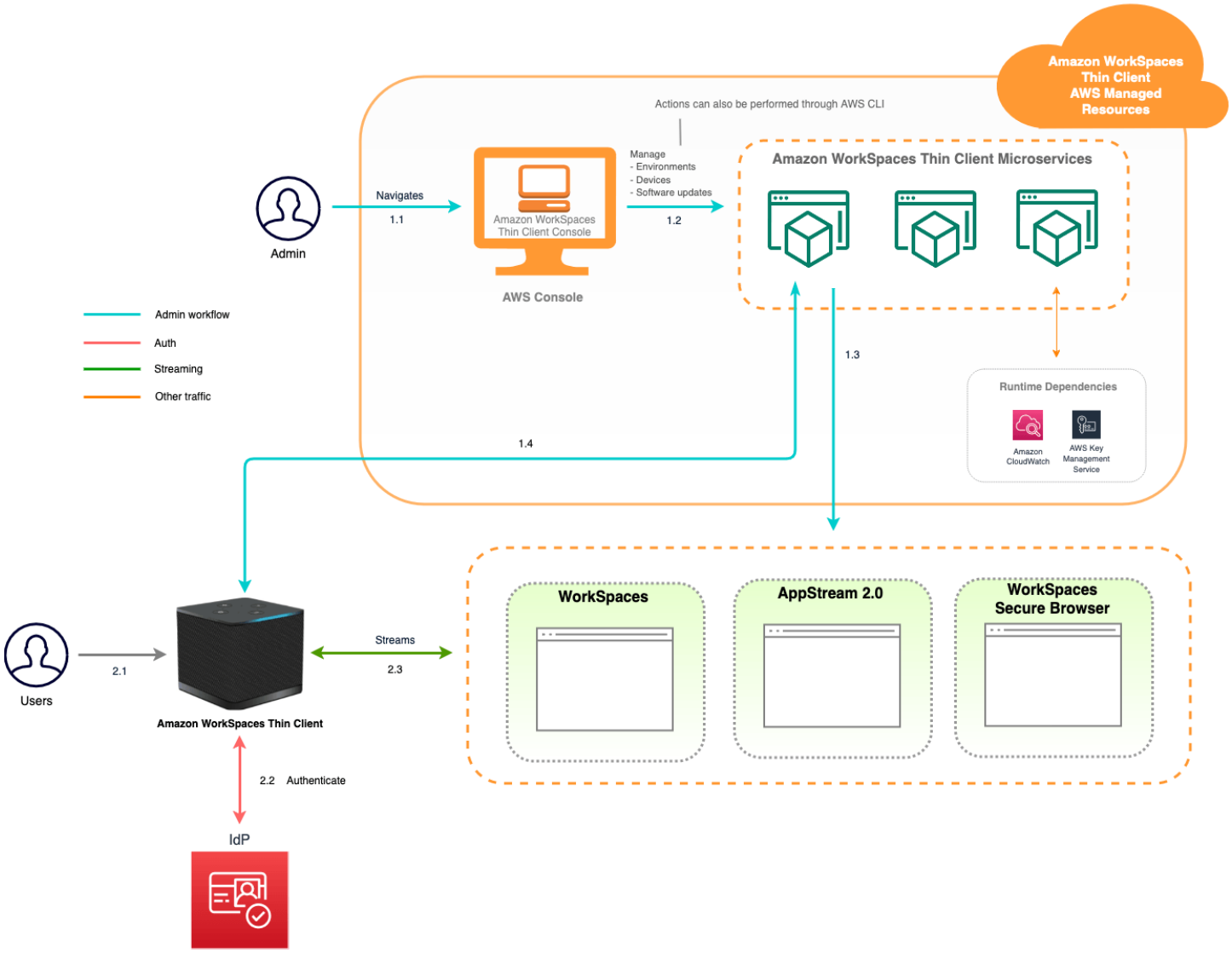
사용된 VDI에 따라 WorkSpaces 씬 클라이언트에 대한 정보는 WorkSpaces용 디렉터리, AppStream 2.0용 스택 및 WorkSpaces Secure Browser용 웹 포털 엔드포인트를 통해 액세스 및 관리됩니다.

Amazon WorkSpaces에 대한 자세한 내용은 WorkSpaces 빠른 설정 시작하기를 참조하세요. 디렉터리는를 통해 관리되며 AWS Directory Service, Simple AD, AD Connector 또는 AWS Managed Microsoft AD라고도 하는 Microsoft Active Directory AWS Directory Service 용 옵션을 제공합니다. 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요.

AppStream 2.0에 대한 자세한 내용은 Amazon AppStream 2.0 시작하기: 샘플 애플리케이션 설정을 참조하세요. AppStream 2.0은 애플리케이션을 호스팅하고 실행하는 데 필요한 AWS 리소스를 관리하고, 자동으로 확장하며, 온디맨드 방식으로 사용자에게 액세스 권한을 제공합니다. AppStream 2.0을 사용하면 기본적으로 설치된 애플리케이션과 구분할 수 없는 유연한 반응형 사용자 환경을 통해 원하는 디바이스에서 필요한 애플리케이션에 액세스할 수 있습니다.

WorkSpaces Secure Browser에 대한 자세한 내용은 Amazon WorkSpaces Secure Browser 시작하기를 참조하세요. Amazon WorkSpaces Secure Browser는 내부 웹 사이트 및 software-as-a-service(SaaS) 애플리케이션에 대한 보안 브라우저 액세스를 용이하게 하도록 설계된 온디맨드 완전 관리형 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 WorkSpaces 씬 클라이언트의 아키텍처를 보여줍니다.


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
Admin workflow
Auth
Streaming
Other traffic
1.4
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

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 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	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따르세요.	AWS Command Line Interface 사용 설명서에서 사용하도록 AWS CLI 를 구성 AWS IAM

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
Center에서 (권장)	이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.		Identity Center하여 프로그래밍 방식 액세스를 구성합니다.
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 비상 액세스를 위한 IAM 사용자 생성에 나와 있는 지침을 따르세요.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리 단계를 수행하여 프로그래밍 방식의 액세스를 구성합니다.

Amazon WorkSpaces 씬 클라이언트용 VDI 시작하기

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

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

> **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

WorkSpaces 씬 클라이언트용 WorkSpaces Personal 구성

WorkSpaces 씬 클라이언트를 Amazon WorkSpaces Personal과 함께 사용하려면 WorkSpaces 디렉터리에 액세스하도록 서비스를 구성해야 합니다. Amazon WorkSpaces Personal 디렉터리는 AWS 콘솔 내 WorkSpaces 씬 클라이언트 환경 생성 페이지의 디렉터리 이름을 기반으로 나열됩니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성해야 합니다. 콘솔 사용을 시작한 후에는 사전 필수 기능을 수정하지 않는 것이 좋습니다.

시작하기 전 준비 사항

WorkSpace를 생성하거나 관리할 AWS 계정이 있는지 확인합니다. 그러나 디바이스 사용자는 WorkSpaces에 연결하고 사용하는 데 AWS 계정이 필요하지 않습니다.

구성을 진행하기 전에 다음 개념을 검토하고 이해합니다.

- WorkSpace를 시작할 때 WorkSpace 번들을 선택합니다. 자세한 내용은 Amazon WorkSpaces 번들 섹션을 참조하세요.
- WorkSpace를 시작할 때 번들에 사용할 프로토콜을 선택합니다. 자세한 내용은 Amazon WorkSpaces Personal용 프로토콜을 참조하세요.
- WorkSpace를 시작할 때 사용자 이름 및 이메일 주소를 포함하여 각 사용자의 프로필 정보를 지정합니다. 사용자는 암호를 생성하여 프로필을 작성합니다. WorkSpaces 및 사용자의 정보는 디렉터리에 저장됩니다. 자세한 내용은 WorkSpaces Personal의 디렉터리 관리를 참조하세요.
- WorkSpaces를 시작할 때 WorkSpaces 씬 클라이언트 웹 액세스를 활성화하고 구성합니다. 자세한 내용은 WorkSpaces 씬 클라이언트 구성을 참조하세요.

1단계: 시스템이 WorkSpaces Personal 필수 기능을 충족하는지 확인

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

Feature	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	• Microsoft Power with Windows 10(Server 2016, 2019 및 2022 기반) • Microsoft Power with Windows 10(Server 2016, 2019, 2022 기반) w Office

Feature	요구 사항
	• Microsoft PowerPro와 Windows 10(Server 2016, 2019 및 2022 기반) • Microsoft PowerPro와 Windows 10(Server 2016, 2019, 2022 기반) w Office • Windows 10을 사용하는 Microsoft 성능(Server 2016, 2019 및 2022 기반) • Microsoft Performance with Windows 10(Server 2016, 2019, 2022 기반) w Office
지원되는 프로토콜	DCV 전용

2단계: 고급 설정을 사용하여 WorkSpace 시작

고급 설정을 사용하여 WorkSpace를 시작하려면

1. https://console.aws.amazon.com/workspaces/v2/home/에서 WorkSpaces 콘솔을 엽니다.
2. 다음 디렉터리 유형 중 하나를 선택하고 다음을 선택합니다.
   - AWS 관리형 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.

비즈니스 연속성

WorkSpaces 씬 클라이언트는 비즈니스 연속성 계획(BCP)의 일부로 비즈니스 연속성을 지원합니다. WorkSpaces 씬 클라이언트 비즈니스 연속성은 WorkSpaces Personal에서만 사용할 수 있습니다. 비즈니스 연속성에 대한 자세한 내용은 Amazon WorkSpaces 관리 안내서의 WorkSpaces Personal의 비즈니스 연속성을 참조하세요. Amazon WorkSpaces

사전 조건

비즈니스 연속성이 WorkSpaces 씬 클라이언트에서 작동하려면 다음 사전 조건을 충족해야 합니다.

- WorkSpaces 리전 간 리디렉션의 경우 - DNS 서비스 및 라우팅 정책이 구성되었습니다. 이를 설정하려면 DNS 서비스 구성 및 DNS 라우팅 정책 설정을 참조하세요.
- WorkSpaces 다중 리전 복원력의 경우 - 대기 WorkSpaces가 생성되었습니다. 이를 생성하려면 대기 WorkSpace 생성을 참조하세요.
- WorkSpaces 씬 클라이언트를 사용하는 리전의 연결 별칭입니다. 리전을 확인하려면 해당 리전을 참조하세요.

WorkSpaces 씬 클라이언트의 비즈니스 연속성 구성

Amazon WorkSpaces 씬 클라이언트에서 WorkSpaces Personal DR을 활성화하려면 SDK를 사용하여 환경에 매핑하도록 연결 별칭을 구성해야 합니다. Amazon WorkSpaces

재해 복구 설정에 대한 샘플 문서 설명:

Example

AWS CLI를 사용하여 스트리밍 데스크톱에 대한 WorkSpaces 연결 별칭을 사용하여 새 환경을 생성하는 예제 명령:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

*wsca-id*를 WorkSpaces Personal 연결 별칭으로 바꿉니다. WorkSpaces 연결 별칭의 ID는 WorkSpaces Management Console 또는 SDK에서 찾을 수 있습니다.

최종 사용자 경험

비즈니스 연속성이 구성되면 지난 15일 이내에 디바이스를 등록하고 활성화해야 합니다. 그런 다음 WorkSpaces 씬 클라이언트 관리 서비스를 사용할 수 없게 되면 사용자는 최대 24시간 동안 세션에 계속 연결할 수 있습니다. 이 조건에서는 디바이스가 소프트웨어 업데이트를 수신하고 자세 정보를 교환하지 않으며 활성화할 수 없습니다. WorkSpaces 씬 클라이언트 콘솔의 해당 디바이스 항목에는 최신 정보가 표시되지 않습니다.

WorkSpaces 씬 클라이언트 디바이스 관리 서비스를 24시간 후에도 사용할 수 없는 경우 다음 오류 메시지가 표시됩니다.

"오류가 발생했습니다. 다시 시도하세요. 문제가 지속되면 IT 관리자에게 문의하십시오. (오류 코드: 3006)."

WorkSpaces 씬 클라이언트에 대한 WorkSpaces 풀 구성

WorkSpaces 씬 클라이언트를 Amazon WorkSpaces Pools와 함께 사용하려면 WorkSpaces Pools 디렉터리에 액세스하도록 SAML 2.0 ID 제공업체(IdP)를 구성해야 합니다. Amazon WorkSpaces Pools 디렉터리는 사용자 그룹에 할당된 비영구 WorkSpaces 풀입니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성해야 합니다.

시작하기 전 준비 사항

WorkSpace를 생성하거나 관리할 AWS 계정이 있는지 확인합니다. 그러나 디바이스 사용자는 WorkSpaces에 연결하고 사용하는 데 AWS 계정이 필요하지 않습니다.

구성을 진행하기 전에 Amazon WorkSpaces 관리 안내서의 WorkSpaces Pools에서 Active Directory 사용을 시작하기 전에에 나열된 개념을 검토하고 이해합니다. Amazon WorkSpaces

WorkSpaces Pools 만들기

사용자 애플리케이션이 시작되어 스트리밍되는 풀을 설정하고 만듭니다.

> **Note**
>
> WorkSpaces Pools를 만들기 전에 디렉터리를 만들어야 합니다. 자세한 내용은 SAML 2.0 구성 및 WorkSpaces Pools 디렉터리 생성을 참조하세요.

풀을 설정하고 만들려면

1. https://console.aws.amazon.com/workspaces/v2/home/에서 WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 WorkSpaces, Pools를 선택합니다.
3. WorkSpaces Pools 생성을 선택합니다.

4. 온보딩(선택 사항)에서 사용 사례에 따라 추천 옵션을 선택하여 사용하려는 WorkSpaces 유형에 대한 추천을 받을 수 있습니다. WorkSpaces Pools를 사용하려는 경우 이 단계를 건너뛸 수 있습니다.
5. WorkSpaces 구성에 다음 세부 정보를 입력합니다.

   - 이름에 풀의 고유 이름 식별자를 입력합니다. 특수 문자는 허용되지 않습니다.
   - 설명에 풀에 대한 설명을 입력합니다(최대 256자).
   - 번들의 경우 WorkSpaces에 사용할 다음 번들 유형 중에서 선택합니다.
     - 기본 WorkSpaces 번들 사용 - 드롭다운에서 번들 중 하나를 선택합니다. 선택한 번들 유형에 대한 자세한 내용은 번들 세부 정보를 선택합니다. 풀에 제공되는 번들을 비교하려면 모든 번들 비교를 선택합니다.
     - 사용자 지정 번들 사용 - 이전에 생성한 번들을 선택합니다. 사용자 지정 번들을 생성하려면 WorkSpaces Personal용 사용자 지정 WorkSpaces 이미지 및 번들 생성을 참조하세요.

     > **Note**
     >
     > 현재 WorkSpaces Pools에서는 BYOL을 사용할 수 없습니다.

   - 최대 세션 기간(분)에서 스트리밍 세션이 활성 상태를 유지할 수 있는 최대 시간을 선택합니다. 이 제한에 도달하기 5분 전까지도 사용자가 스트리밍 인스턴스에 연결되어 있으면 연결이 해제되기 전에 열려 있는 문서를 저장하라는 메시지가 나타납니다. 이 시간이 지나면 인스턴스가 종료되고 새 인스턴스로 교체됩니다. WorkSpaces Pools 콘솔에서 설정할 수 있는 최대 세션 지속 시간은 5760분(96시간)입니다. WorkSpaces Pools API 및 CLI를 사용하여 설정할 수 있는 최대 세션 지속 시간은 432,000초(120시간)입니다.
   - 연결 해제 제한 시간(분)에서 사용자가 연결을 해제한 후 스트리밍 세션이 활성 상태로 유지되는 시간을 선택합니다. 연결 해제 또는 네트워크 중단 후 이 시간 간격 이내에 사용자가 스트리밍 세션에 다시 연결하려고 하면 이전 세션으로 연결됩니다. 그렇지 않으면 새 스트리밍 인스턴스를 사용하여 새 세션에 연결됩니다.
   - 사용자가 Pools 도구 모음에서 세션 종료를 선택하거나 로그아웃하여 세션을 종료할 경우에는 연결 해제 제한 시간이 적용되지 않습니다. 대신 열려 있는 문서를 저장하라는 메시지가 나타난 후 즉시 스트리밍 인스턴스에서 연결이 해제됩니다. 그리고 사용자가 사용하던 인스턴스가 종료됩니다.
   - 사용자가 스트리밍 세션에서 연결을 해제하고 연결 해제 제한 시간(분) 시간 간격이 시작되기 전까지 유휴(비활성) 상태를 유지할 수 있는 시간을 유휴 연결 해제 제한 시간(분)에서 선택합니다. 비활성 상태로 연결이 해제되기 전에 사용자에게 이를 알려줍니다. 연결 해제 제한 시간(분)에 지정된 시간 간격이 경과하기 전에 사용자가 스트리밍 세션으로 다시 연결하면 이전 세션으로

연결됩니다. 그렇지 않으면 새 스트리밍 인스턴스를 사용하여 새 세션에 연결됩니다. 이 값을 0으로 설정하면 비활성화됩니다. 이 값이 비활성화되면 비활성 상태를 이유로 연결이 해제되지 않습니다.

> **Note**
>
> 사용자의 스트리밍 세션에서 키보드 또는 마우스 입력이 중단되면 유휴 상태로 간주됩니다. 도메인에 조인된 풀의 경우 사용자가 Active Directory 도메인 암호 또는 스마트 카드를 사용하여 로그인할 때까지 유휴 연결 해제 제한 시간 카운트다운이 시작되지 않습니다. 파일 업로드와 다운로드, 오디오 인, 오디오 아웃, 픽셀 변경은 사용자 활성 상태로 인정되지 않습니다. 유휴 연결 해제 제한 시간(분)의 시간 간격이 경과된 후에도 사용자가 계속 유휴 상태이면 연결이 해제됩니다.

- 용량 예약 정책(선택 사항)에서 새 용량 예약 추가를 선택합니다. 예상되는 최소 동시 사용자 수를 기준으로 풀의 최소 및 최대 인스턴스 수를 프로비저닝할 시기의 시작 및 종료 날짜와 시간을 지정합니다.
- 수동 규모 조정 정책(선택 사항)에서 풀의 용량을 늘리거나 줄이는 데 사용할 풀의 규모 조정 정책을 지정합니다. 수동 조정 정책을 확장하여 새 조정 정책을 추가합니다.

> **Note**
>
> 풀의 크기는 지정한 최소 및 최대 용량에 의해 제한됩니다.

  - 새 스케일 아웃 정책 추가를 선택하고 지정된 용량 사용률이 지정된 임계값보다 작거나 클 경우 지정된 인스턴스를 추가할 값을 입력합니다.
  - 정책에 새 스케일 인 추가를 선택하고 지정된 용량 사용률이 지정된 임계값보다 작거나 클 경우 지정된 인스턴스를 제거할 값을 입력합니다.
- 태그에서 사용할 키 페어 값을 지정합니다. 키는 "project", "owner" 또는 "environment" 등의 특정 연결 값을 가진 일반 범주일 수 있습니다.

6. 디렉터리 선택 페이지에서 만든 디렉터리를 선택합니다. 디렉터리를 만들려면 디렉터리 생성을 선택합니다. 자세한 내용은 WorkSpaces Pools의 디렉터리 관리를 참조하세요.
7. WorkSpaces Pool 생성을 선택합니다.

WorkSpaces 씬 클라이언트 액세스 구성

WorkSpaces 씬 클라이언트를 사용하도록 WorkSpaces Pools에 대한 웹 액세스를 구성하려면 AWS 명령 랜드 인터페이스를 사용해야 합니다.

1. AWS Command Line Interface를 설치 또는 업데이트합니다.
2. AWS CLI 설정을 구성합니다.
3. 를 엽니다 AWS CLI.
4. 적절한 정보로 WORKSPACES_DIRECTORY_ID 및를 대체REGION하여 다음을 실행합니다.

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

Amazon WorkSpaces 씬 클라이언트용 AppStream 2.0 구성

AppStream 2.0 인스턴스는 Stack 이름을 기준으로 나열되며, 환경 생성 페이지에 구성된 IdP 로그인 URL이 필요합니다. AppStream 2.0에 대한 SAML 인증은 시작된 인증만 지원하므로 관리자는 올바른 로그인 URL을 수동으로 입력해야 합니다.

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성해야 합니다. 콘솔 사용을 시작한 후에는 사전 필수 기능을 수정하지 않는 것이 좋습니다.

1단계: 시스템이 AppStream 2.0 필수 기능을 충족하는지 확인

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

Feature	요구 사항
ID 제공업체	AppStream 2.0 관리자 안내서의 SAML 설정으로 이동하여 자격 증명 공급자를 생성합니다.

Feature	요구 사항
	Create env console 메시지가 표시되면 IDP 로그인 URL을 입력합니다.
운영 체제	Windows
플랫폼 유형	Windows Server(2012 R2, 2016 또는 2019)
클립보드	비활성화 AppStream 2.0 스택 수준에서 구성됨
파일 전송	비활성화 AppStream 2.0 스택 수준에서 구성됨
로컬 디바이스로 인쇄	비활성화 AppStream 2.0 스택 수준에서 구성됨

AppStream 2.0에서 SAML 인증을 통한 화면 잠금 요구 사항도 지원됩니다. 사용자 풀 및 프로그래밍 인증 메커니즘은 WorkSpaces 씬 클라이언트에서 지원되지 않습니다.

2단계: AppStream 2.0 스택 설정

애플리케이션을 스트리밍하려면 AppStream 2.0에 스택 및 최소 하나의 애플리케이션 이미지와 연결된 플릿을 포함하는 환경이 필요합니다. 다음 단계에 따라 플릿과 스택을 설정하고 사용자에게 스택에 대한 액세스 권한을 부여합니다. 아직 하지 않았다면 AppStream 2.0 시작하기: 샘플 애플리케이션을 사용하여 설정의 절차를 시도해 보는 것이 좋습니다.

사용할 이미지를 만들려면 자습서: AppStream 2.0 콘솔을 사용하여 사용자 지정 AppStream 2.0 이미지 생성을 참조하세요.

플릿을 Active Directory 도메인에 병합하려면 아래 단계를 수행하기 전에 먼저 Active Directory 도메인을 구성해야 합니다. 자세한 내용은 AppStream 2.0과 함께 Active Directory 사용하기를 참조하세요.

업무

- 플릿 생성
- 스택 생성

- 사용자에게 액세스 권한 제공
- 리소스 정리

Amazon WorkSpaces 씬 클라이언트용 Amazon WorkSpaces Secure Browser 구성

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

> **Note**
>
> 콘솔을 처음 사용하기 전에 구성해야 합니다. 콘솔 사용을 시작한 후에는 사전 필수 기능을 수정하지 않는 것이 좋습니다.

1단계: 시스템이 Amazon WorkSpaces Secure Browser 필수 기능을 충족하는지 확인

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

Feature	요구 사항
클립보드	비활성화
파일 전송	비활성화
로컬 디바이스로 인쇄	비활성화

> **Note**
>
> Single Sign-On을 위한 WorkSpaces Secure Browser 확장은 현재 WorkSpaces 씬 클라이언트에서 지원되지 않습니다.

2단계: WorkSpaces Secure Browser 포털 설정

WorkSpaces 씬 클라이언트는 특정 구성에서 WorkSpaces Secure Browser VPC와 함께 작동합니다.

1. AWS CodeBuild Cloudformation 템플릿을 사용하여 VPC를 생성합니다.
2. ID 공급자를 설정합니다.
3. Amazon WorkSpaces Secure Browser 포털을 생성합니다.
4. 새 Amazon WorkSpaces Secure Browser 포털을 테스트합니다.

WorkSpaces 씬 클라이언트 관리자 콘솔 시작

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

주제

적용 대상 리전

WorkSpaces 씬 클라이언트는 다음 리전에서 사용할 수 있습니다.

이러한 리전에서는 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(오리건)	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

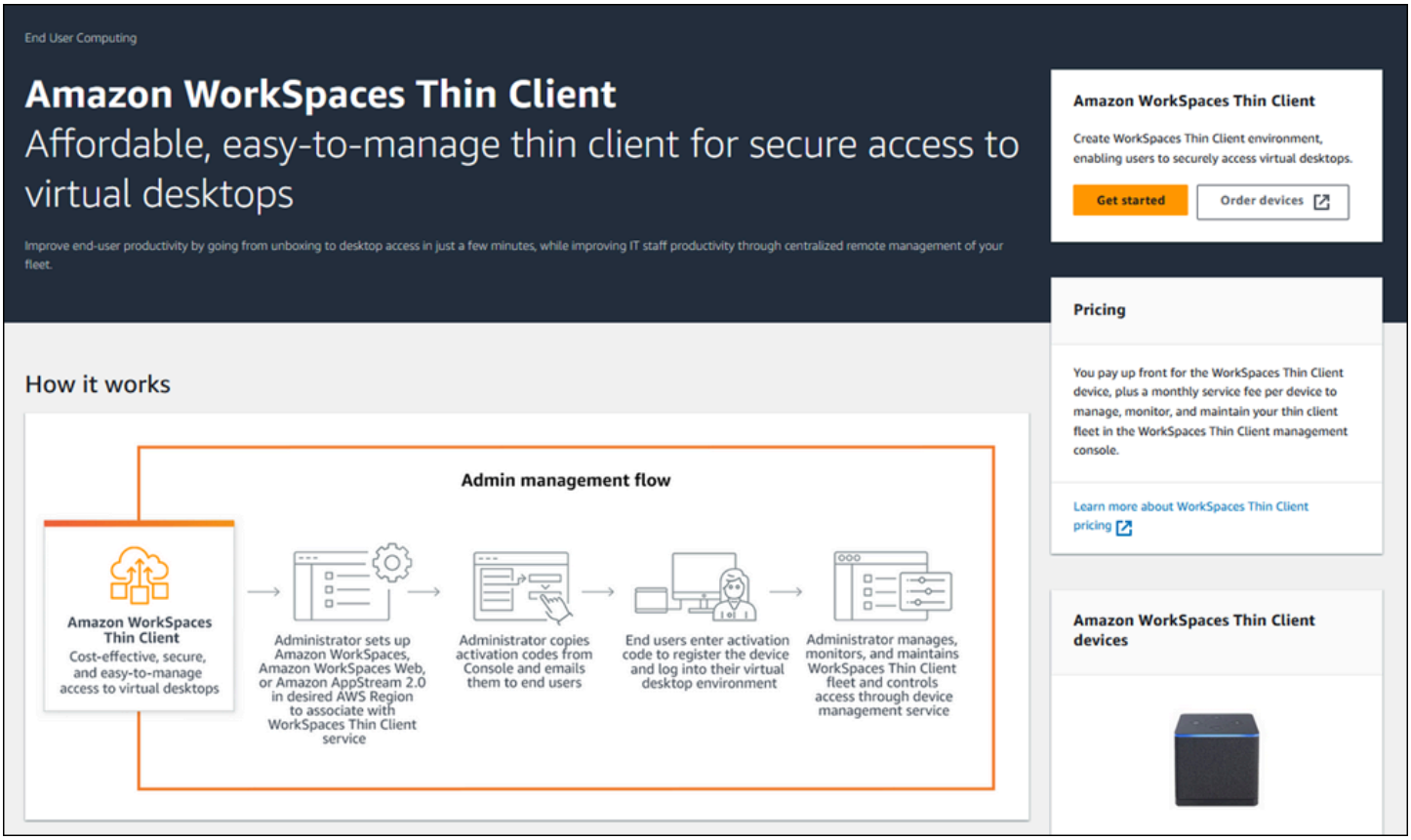
리전 이름	지역	엔드포인트	콘솔 링크
		-1.amazonaws.com	
캐나다(중부)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
유럽(프랑크푸르트)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home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

AWS 계정이 있으면 관리자 콘솔을 시작하고 WorkSpaces 씬 클라이언트 콘솔로 이동할 수 있습니다. 콘솔을 시작하려면 다음을 수행합니다.

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

WorkSpaces 씬 클라이언트 관리자 콘솔 사용



WorkSpaces 씬 클라이언트 관리자 콘솔입니다.

여기에서 팀의 WorkSpaces 씬 클라이언트 디바이스 및 환경을 관리할 수 있습니다.

WorkSpaces 씬 클라이언트 디바이스에 대한 자세한 내용은 WorkSpaces 씬 클라이언트 사용 설명서를 참조하세요.

시작해봅시다.

주제

- 환경
- Devices
- 소프트웨어 업데이트

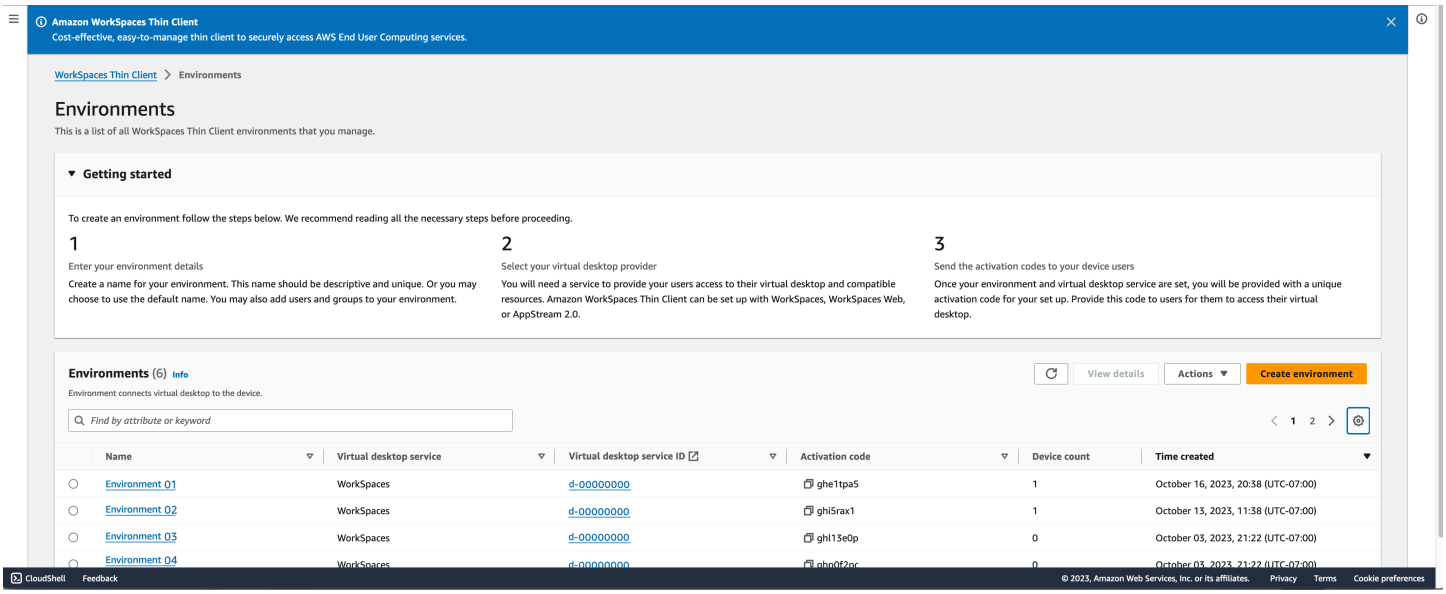
환경

각 WorkSpaces 씬 클라이언트 디바이스는 개별 가상 데스크톱 환경을 사용하여 온라인 리소스에 액세스합니다. 사용자는 다음 가상 데스크톱 공급자 중 하나를 사용하여이 환경에 액세스합니다.

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces Secure Browser

환경 목록

환경에는 검토할 수 있는 여러 파라미터와 수행할 수 있는 몇 가지 작업이 있습니다.



환경 목록 세부 정보

환경에 대한 파라미터가 검토를 위해 나열됩니다. 다음 표에는 요약의 각 요소와 그 작동 방식이 나와 있습니다.

Element	설명
명칭	이 환경과 연결된 고유 식별자입니다.
가상 데스크톱 서비스	이 환경에서 사용하는 가상 데스크톱 공급자입니다.

Element	설명
가상 데스크톱 서비스 ID	가상 데스크톱 서비스 공급자가이 환경에 할당하는 고유 식별자입니다.
활성화 코드	최종 사용자가 가상 데스크톱 환경에 액세스하는 데 사용하는 코드입니다.
디바이스 수	이 환경에 액세스하는 WorkSpaces 씬 클라이언트 디바이스의 수입니다.
생성된 시간	환경이 생성된 날짜 및 시간입니다.

환경 목록 작업

여기에서 수행할 수 있는 여러 작업이 있습니다. 이 중 하나를 선택하여 해당 작업을 수행합니다.

Element	설명
검색	관리하는 모든 환경을 검색합니다.
새로 고침	환경 목록을 새로 고칩니다.
세부 정보 보기	환경 세부 정보를 표시합니다.
작업	환경을 편집하거나 삭제할 수 있는 드롭다운 목록을 엽니다.
환경 생성	환경을 생성하는 프로세스를 시작합니다.

주제

- 환경 세부 정보
- 환경 생성
- 환경 편집
- 환경 삭제

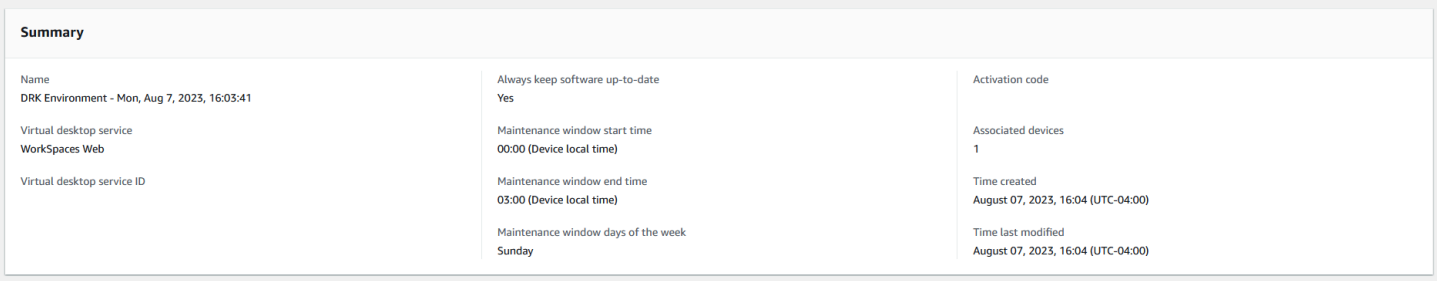
환경 세부 정보

환경을 선택하면 WorkSpaces 씬 클라이언트 콘솔에 검토할 환경에 대한 세부 정보가 표시됩니다. 콘솔에는이 환경에서 사용하는 가상 데스크톱 공급자에 대한 세부 정보도 표시됩니다.

주제

요약

요약 섹션에서는 WorkSpaces 씬 클라이언트 환경의 주요 기능에 대한 개략적인 개요를 제공합니다. 다음 표에는 요약의 각 요소와 그 작동 방식이 나와 있습니다.



Element	설명
명칭	이 환경과 연결된 고유 식별자입니다.
가상 데스크톱 서비스	이 환경에서 사용하는 가상 데스크톱 공급자입니다.
가상 데스크톱 서비스 이름	가상 데스크톱 서비스 공급자가이 환경에 할당하는 고유 식별자입니다.
활성화 코드	이 코드는 최종 사용자가 가상 데스크톱 환경에 액세스하는 데 사용됩니다.
소프트웨어를 항상 up-to-date 유지	이 설정은 자동 소프트웨어 업데이트를 활성화합니다.

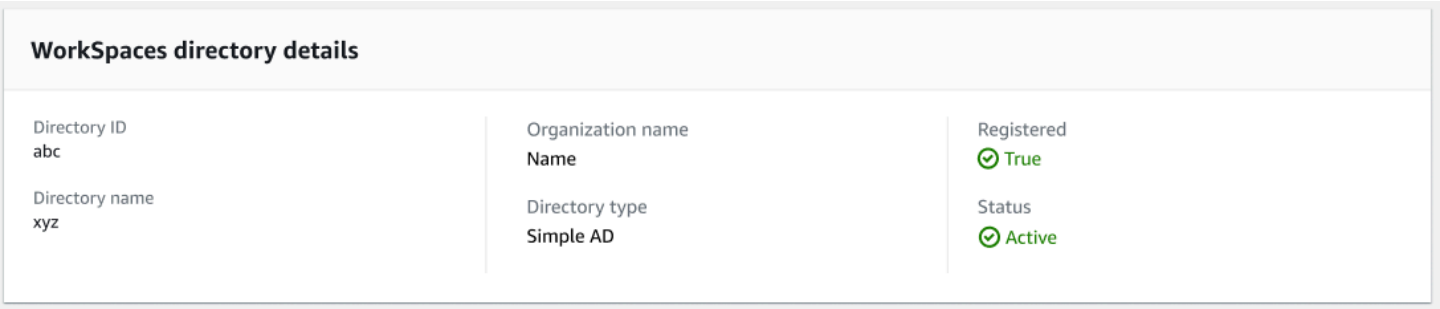
Element	설명
유지 관리 기간 시작 시간	매주 자동 소프트웨어 업데이트가 시작되는 시간입니다.
유지 관리 기간 종료 시간	자동 소프트웨어 업데이트가 완료되는 매주의 시간입니다.
유지 관리 기간 요일	자동 소프트웨어 업데이트가 발생하는 일수입니다.
연결된 디바이스	이 환경에 액세스하는 WorkSpaces 씬 클라이언트 디바이스의 수입니다.
생성 시간	이 환경이 생성된 날짜 및 시간입니다.

가상 데스크톱 환경 세부 정보

WorkSpaces 씬 클라이언트 환경은 가상 데스크톱 인터페이스에서 실행됩니다. 각 인터페이스에는 전용 환경을 제어하는 다양한 파라미터 세트가 있습니다.

Amazon WorkSpaces 디렉터리 세부 정보

Amazon WorkSpaces에서 실행되는 Amazon WorkSpaces씬 클라이언트 환경은 디렉터리를 사용하여 가상 데스크톱을 생성하고 실행합니다. 다음 표에는 세부 정보의 각 요소와 작동 방식이 나열되어 있습니다.

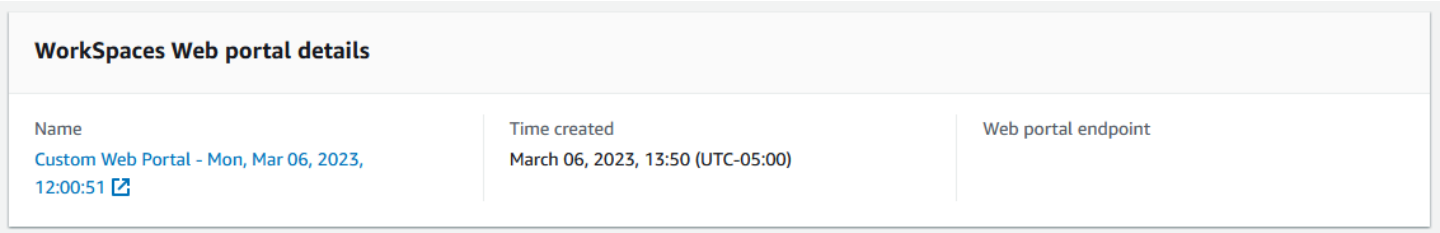


Element	설명
디렉터리 ID	이 환경과 연결된 Amazon WorkSpaces 디렉터리입니다.

Element	설명
디렉터리 이름	이 Amazon WorkSpaces 디렉터리와 연결된 고유 식별자입니다.
조직 이름	Amazon WorkSpaces 디렉터리를 제어하는 조직의 이름입니다.
디렉터리 유형	Amazon WorkSpaces 디렉터리의 형식입니다.
등록	이 Amazon WorkSpaces 디렉터리의 등록 여부입니다.
상태 표시기	이 Amazon WorkSpaces 디렉터리가 활성 상태인지 여부입니다.

Amazon WorkSpaces Secure Browser 포털 세부 정보

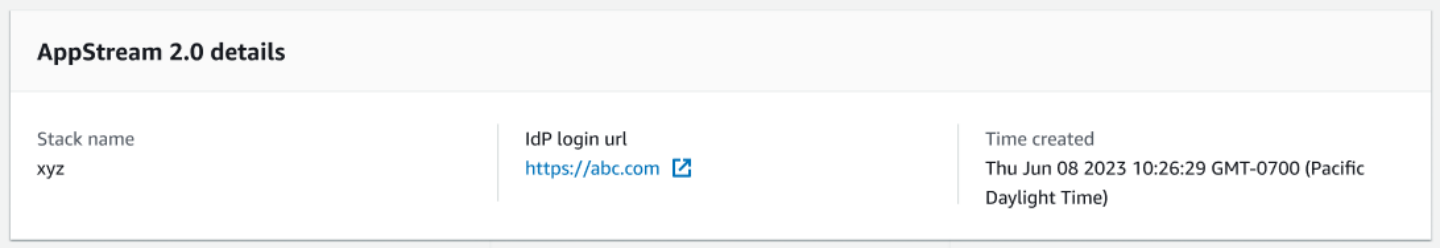
WorkSpaces 씬 클라이언트 환경은 Amazon WorkSpaces Secure Browser에서 실행되며 웹 포털을 사용하여 가상 데스크톱을 생성하고 실행합니다. 다음 표에는 세부 정보의 각 요소와 작동 방식이 나열되어 있습니다.



Element	설명
명칭	이 WorkSpaces Secure Browser 포털과 연결된 고유 식별자입니다.
생성 시간	이 WorkSpaces Secure Browser 포털이 생성된 날짜와 시간입니다.
웹 포털 엔드포인트	가상 데스크톱 환경에 액세스하는 데 사용되는 URL입니다.

AppStream 2.0 세부 정보

WorkSpaces 씬 클라이언트 환경은 AppStream 2.0 정보 스택에서 실행되어 가상 데스크톱을 생성하고 실행합니다. 다음 표에는 세부 정보의 각 요소와 작동 방식이 나열되어 있습니다.



Element	설명
스택 이름	이 AppStream 2.0 스택과 연결된 고유 식별자입니다.
IdP 로그인 URL	AppStream 2.0 스택에 로그인 및 로그아웃하는 데 사용되는 자격 증명 공급자 URL입니다.
생성 시간	이 AppStream 2.0 스택이 생성된 날짜와 시간입니다.

환경 생성

시작하려면 각 디바이스에 AWS 최종 사용자 컴퓨팅 서비스가 필요합니다. WorkSpaces 씬 클라이언트는 다음 서비스를 사용합니다.

- 할당된 디렉터리를 통한 Amazon WorkSpaces
- 할당된 스택을 통한 AppStream 2.0
- 웹 포털 주소를 통한 Amazon WorkSpaces Secure Browser

기존 환경에 서비스를 할당하거나 새 서비스를 생성해야 합니다.

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

주제

1단계: 환경 세부 정보 입력

1. 환경 세부 정보 필드에 환경의 이름을 입력합니다.
2. 자동 소프트웨어 패치를 설정하려면 소프트웨어를 항상 최신 상태로 유지 확인란을 선택합니다.

> **Note**
>
> 자동 소프트웨어 업데이트가 활성화되지 않은 경우 업데이트를 수동으로 푸시하거나 소프트웨어가 만료되고 시스템이 업데이트를 강제로 실행할 때까지이 환경에 등록된 디바이스는 소프트웨어 업데이트를 받지 않습니다.
> 또한 디바이스 소프트웨어 세트 버전은 시스템에 의해 결정됩니다. 이 버전은 최신 버전이 아닐 수 있습니다.

3. 환경에 대한 유지 관리 기간을 예약할 시기를 선택합니다.
   - 시스템 전체 유지 관리 기간 적용 - 매주 정해진 시간에 환경 소프트웨어를 자동으로 업데이트합니다.
   - 사용자 지정 유지 관리 기간 적용 - 매주 환경 소프트웨어를 업데이트할 날짜와 시간을 설정합니다.
4. 가상 데스크톱 서비스를 선택합니다.
   - Amazon WorkSpaces
   - Amazon WorkSpaces Secure Browser
   - AppStream 2.0

2단계: 가상 데스크톱 공급자 선택

사용자에게 가상 데스크톱 및 호환되는 리소스에 대한 액세스 권한을 제공하는 서비스가 있어야 합니다.

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

Amazon WorkSpaces 사용

Amazon WorkSpaces는 Windows용 완전관리형 데스크톱 가상화 서비스로, 지원되는 모든 디바이스에서 리소스에 액세스할 수 있도록 합니다.

1. Amazon WorkSpaces를 사용하려면 다음 중 하나를 수행합니다.
   - 그런 다음 환경에 사용하려는 디렉터리를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 디렉터리를 검색할 수 있습니다.
   - WorkSpaces 디렉터리 생성 버튼을 선택하여 디렉터리를 생성합니다. WorkSpaces 디렉터리 생성에 대한 자세한 내용은 WorkSpaces 디렉터리 관리를 참조하세요.
2. 환경 생성 버튼을 선택합니다.

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

AppStream 2.0 사용

AppStream 2.0은에서 웹 브라우저로 데스크톱 애플리케이션을 스트리밍 AWS 하는 데 사용할 수 있는 완전 관리형 보안 애플리케이션 스트리밍 서비스입니다.

> **Important**
>
> AppStream 2.0 환경을 생성하려면 `cli_follow_urlparam`을 `false`로 설정해야 합니다. 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 수행합니다.

- 그런 다음 환경에 사용하려는 스택을 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 스택을 검색할 수 있습니다.
- 스택 생성 버튼을 선택하여 스택을 생성합니다. AppStream 2.0 스택 생성에 대한 자세한 내용은 스택 생성을 참조하세요.

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

Amazon WorkSpaces Secure Browser 사용

Amazon WorkSpaces Secure Browser는 기존 웹 브라우저 내의 사용자에게 안전한 웹 기반 워크로드 및 서비스형 소프트웨어(SaaS) 애플리케이션 액세스를 제공하도록 구축된 저비용 완전관리형 WorkSpaces 콘솔입니다.

1. Amazon WorkSpaces Secure Browser를 설정하려면 다음 중 하나를 수행합니다.
   - 환경에 사용할 웹 포털을 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 웹 포털을 검색할 수 있습니다.
   - WorkSpaces Secure Browser 생성 버튼을 선택하여 웹 포털을 생성합니다. WorkSpaces Secure Browser 웹 포털 생성에 대한 자세한 내용은 Amazon WorkSpaces Secure Browser 설정을 참조하세요.
2. 환경 생성 버튼을 선택합니다.

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

3단계: 디바이스 사용자에게 활성화 코드 전송

환경 및 가상 데스크톱 서비스를 설정하면 AWS 관리 콘솔에서 설정에 대한 고유한 활성화 코드를 받게 됩니다.

WorkSpaces 씬 클라이언트 디바이스 사용자에게이 활성화 코드를 제공하면 해당 활성화 코드를 사용하여 가상 데스크톱에 액세스할 수 있습니다.

디바이스 사용자가 Amazon WorkSpaces 씬 클라이언트를 설정하는 데 도움이 되는 방법에 대한 자세한 내용은 WorkSpaces 씬 클라이언트 사용 설명서를 참조하세요. Amazon WorkSpaces

환경 편집

WorkSpaces 씬 클라이언트 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 업데이트를 위한 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.

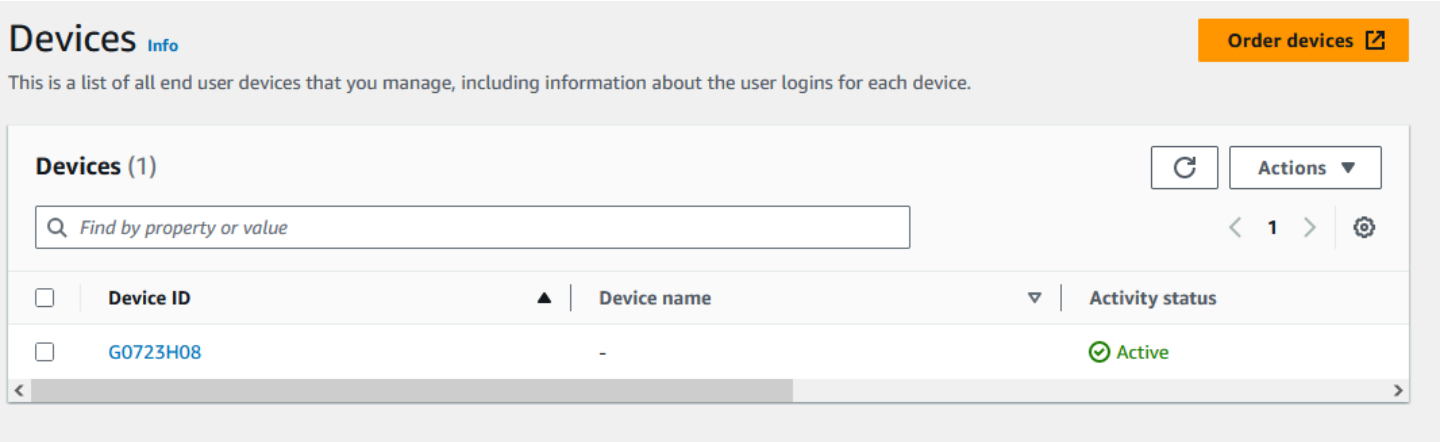
Devices

각 WorkSpaces 씬 클라이언트 최종 사용자에게는 가상 데스크톱 환경 및 온라인 리소스에 연결하는 전용 디바이스가 있습니다. 이 디바이스는 AWS 사이트의 WorkSpaces 씬 클라이언트 관리자 콘솔을 통해 관리됩니다.

이 콘솔에서 팀을 위한 디바이스를 주문할 수 있습니다.

디바이스 목록

네트워크의 모든 디바이스에 대해 검토할 수 있는 여러 파라미터와 수행할 수 있는 몇 가지 작업이 있습니다.



디바이스 목록 세부 정보

디바이스의 파라미터가 검토를 위해 나열됩니다. 다음 표에는 요약의 각 요소와 그 작동 방식이 나와 있습니다.

Element	설명
디바이스 ID	개별 디바이스에 할당된 식별 번호입니다.
디바이스 이름	(선택 사항) 디바이스에 부여하는 고유한 이름입니다.
활동 상태	디바이스의 현재 상태입니다. 다음과 같은 두 가지 상태가 있습니다.

Element	설명
	• 활성 - 지난 7일 동안 한 번 이상 네트워크에 연결되었습니다. • 비활성 - 지난 7일 동안 네트워크에 연결되지 않았습니다.
등록 상태	디바이스가 설정되었고,이 AWS 계정과 연결되어 있으며, 특정 환경의 일부인지 확인합니다. 다음 상태 중 하나일 수 있습니다. • 등록됨 - 기본 상태입니다. • 등록 취소 - 디바이스가 재설정 및 등록 취소 프로세스에 있습니다. Note 디바이스가 등록 취소 상태인 경우 삭제할 수 있습니다. • Deregsitered - 디바이스가 성공적으로 등록 취소되었습니다. Note 디바이스가 등록 취소 중 또는 등록 취소됨 상태인 경우에만 디바이스를 삭제할 수 있습니다. • 아카이브됨 - 디바이스가 아카이브되었습니다.
환경 ID	이 디바이스가 연결된 환경의 식별자입니다.

Element	설명
소프트웨어 규정 준수	디바이스 소프트웨어의 규정 준수 상태입니다. 다음과 같은 두 가지 상태가 있습니다. • 규정 준수 • 규정 미준수

디바이스 목록 작업

여기에서 수행할 수 있는 여러 작업이 있습니다. 이 중 하나를 선택하여 해당 작업을 수행합니다.

Element	설명
검색	관리하는 모든 디바이스를 검색합니다.
새로 고침	디바이스 목록을 새로 고칩니다.
세부 정보 보기	디바이스 세부 정보를 표시합니다.
작업	다음을 수행할 수 있는 드롭다운 목록을 엽니다. • 디바이스 이름 편집 • 등록 취소 • Archive(보관) • 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

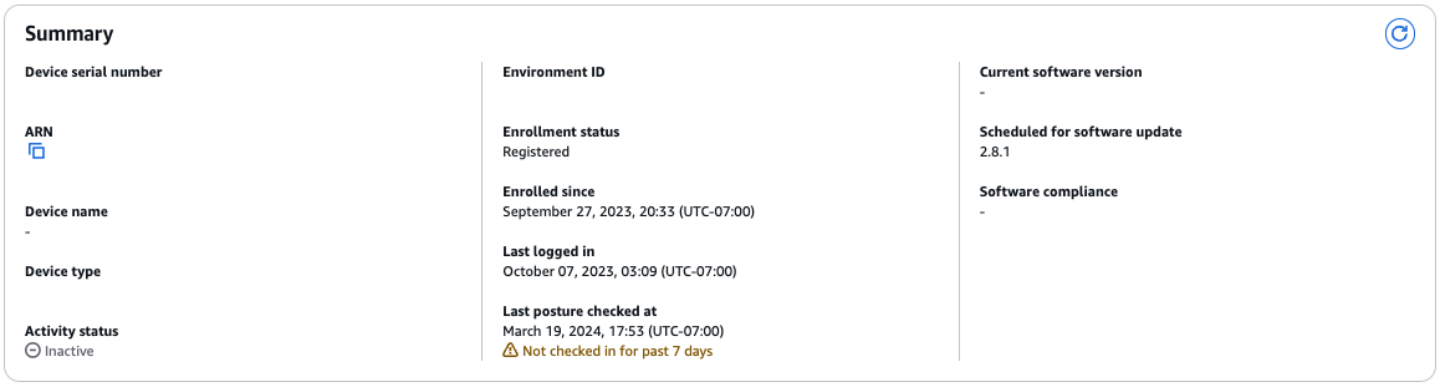
디바이스를 선택하면 WorkSpaces 씬 클라이언트 콘솔에 검토할 디바이스의 세부 정보가 표시됩니다. 콘솔에는 디바이스의 네트워크 유형 및 연결된 주변 장치에 대한 세부 정보도 표시됩니다.

주제

- 요약
- 디바이스 설정
- 사용자 활동

요약

요약 섹션에서는 WorkSpaces 씬 클라이언트 디바이스의 주요 기능에 대한 개략적인 개요를 제공합니다. 다음 표에는 요약의 각 요소와 그 작동 방식이 나와 있습니다.

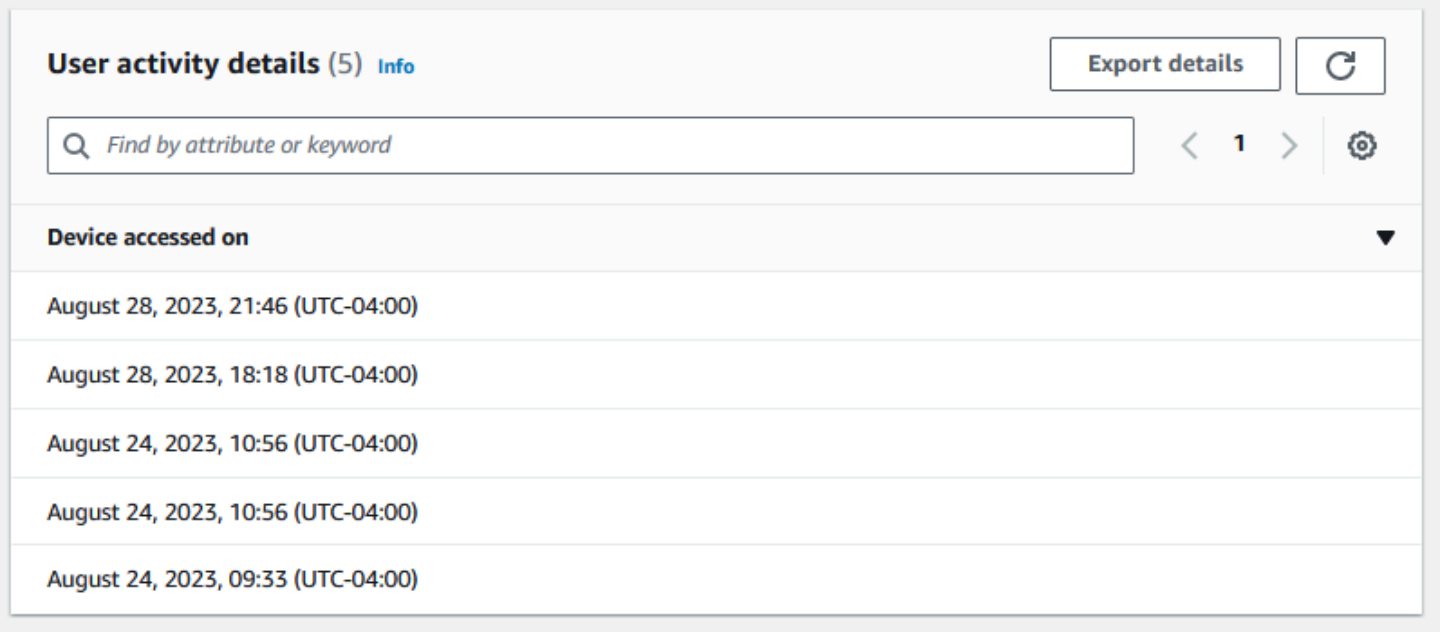


Element	설명
디바이스 일련 번호	개별 디바이스에 할당된 식별 번호입니다.
ARN	Amazon 리소스 이름(ARN) 형식의 디바이스에 대한 고유 식별자입니다.

Element	설명
디바이스 이름	디바이스에 부여하는 이름입니다. 이름을 생성하지 않은 경우 이름을 지정할 수 있습니다. 그렇지 않으면 기본 이름이 지정됩니다.
디바이스 유형	계정에 연결된 최종 사용자 디바이스의 유형입니다.
활동 상태	이 디바이스의 현재 상태입니다. 두 가지 상태는 다음과 같습니다. • 활성 • 비활성
환경 ID	디바이스가 사용하는 환경의 식별 번호입니다.
등록 상태	디바이스가 설정되었고,이 AWS 계정과 연결되어 있으며, 특정 환경의 일부인지 확인합니다. 다음 네 가지 상태 중 하나일 수 있습니다. • 등록됨 - 기본 상태입니다. • 등록 취소 - 디바이스가 재설정 및 등록 취소 프로세스에 있습니다. • 등록 취소됨 - 디바이스가 성공적으로 등록 취소되었습니다. **Note** 디바이스가 등록 취소됨 또는 보관됨 상태인 경우에만 디바이스를 삭제할 수 있습니다. • 아카이브됨 - 관리자가이 디바이스를 현재 서비스 중이 아닌 것으로 표시했습니다.
이후 등록됨	디바이스가 활성화된 날짜입니다.

Element	설명
마지막 로그인	가장 최근 로그인 날짜 및 시간입니다.
에서 마지막으로 확인된 자세	가장 최근의 디바이스 체크인 날짜 및 시간입니다.
현재 소프트웨어 버전	이 디바이스에서 현재 사용 중인 소프트웨어 버전입니다.
소프트웨어 업데이트 예정	디바이스에서 예약된 소프트웨어 버전입니다.
소프트웨어 규정 준수	소프트웨어 세트가 유효한지 확인합니다. 다음과 같은 두 가지 상태가 있습니다. • 규정 준수 • 규정 미준수

사용자 로그



Element	설명
마지막 디바이스 액세스	이 디바이스가 마지막으로 사용된 날짜와 시간입니다.

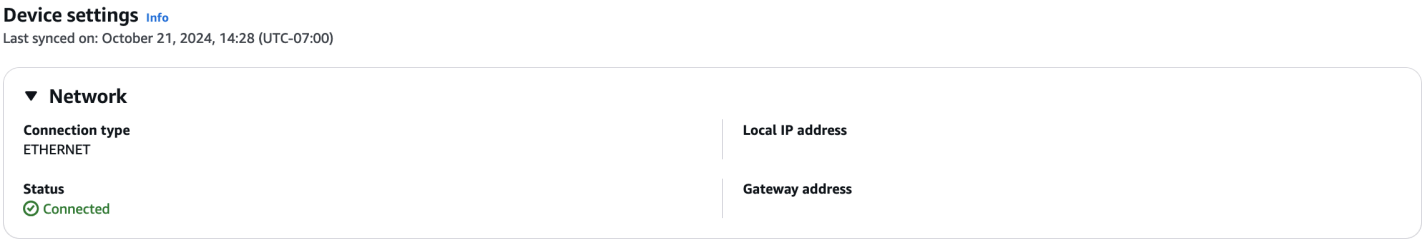
디바이스 설정

디바이스의 파라미터가 검토를 위해 나열됩니다. 다음 표에는 각 요소와 그 작동 방식이 나열되어 있습니다.

> **Note**
>
> 디바이스 설정 정보는 디바이스가 온라인 상태일 때만 업데이트됩니다. 디바이스가 오프라인 상태인 경우 일부 정보가 최신 상태가 아닐 수 있습니다.

제목 및 네트워크

WorkSpaces 씬 클라이언트 디바이스 세부 정보는 디바이스의 네트워크 연결에 대한 개요를 제공합니다. 다음 표에는 각 요소와 그 작동 방식이 나열되어 있습니다.

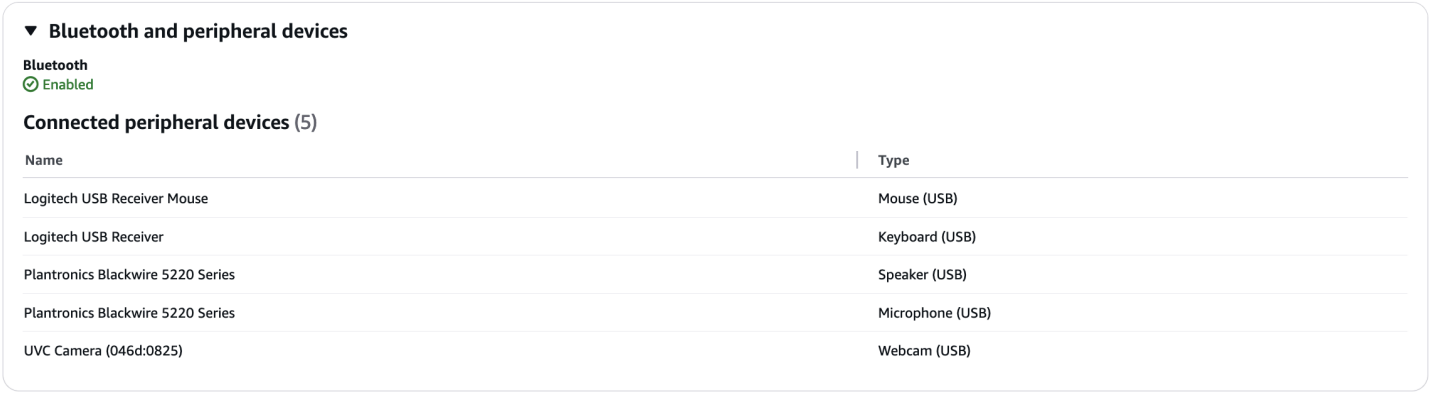


Element	설명
에 마지막으로 동기화됨	최신 디바이스 설정이 콘솔과 동기화된 날짜와 시간입니다.
연결 유형	디바이스에서 사용하는 네트워크 연결 유형입니다. 연결 유형은 이더넷 또는 Wifi일 수 있습니다.
상태 표시기	네트워크의 상태입니다. 디바이스가 현재 연결되어 있거나 지난 20분 이내에 연결된 경우 상태

Element	설명
	가 '연결됨'으로 표시됩니다. 네트워크 연결이 20분 이상 끊어지면 상태가 변경되어 디바이스가 인터넷에 마지막으로 연결된 이후 경과된 시간이 표시됩니다. 예: “20분 전에 마지막으로 연결됨”.
로컬 IP 주소	연결된 네트워크의 로컬 IP 주소입니다.
게이트웨이 주소	연결된 네트워크의 게이트웨이 주소입니다.

Bluetooth 및 주변 장치

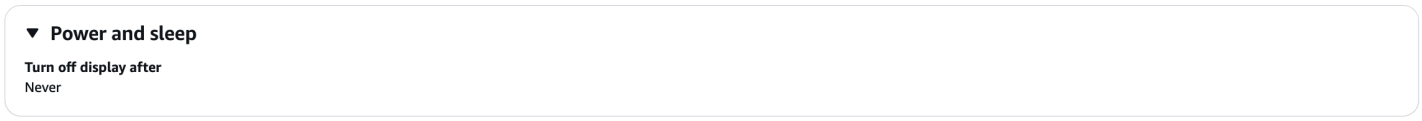
WorkSpaces 씬 클라이언트 디바이스 세부 정보는 디바이스에 연결된 주변 장치의 목록을 제공합니다. 다음 표에는 각 요소와 그 작동 방식이 나와 있습니다.



Element	설명
Bluetooth	디바이스의 Bluetooth 상태입니다. 두 가지 상태는 다음과 같습니다. • 활성화됨 • 비활성
연결된 주변 디바이스	Logitech 마우스와 같은 연결된 주변 장치의 이름과 마우스(USB)와 같은 연결된 주변 장치의 유형 목록입니다.

전원 및 절전 모드

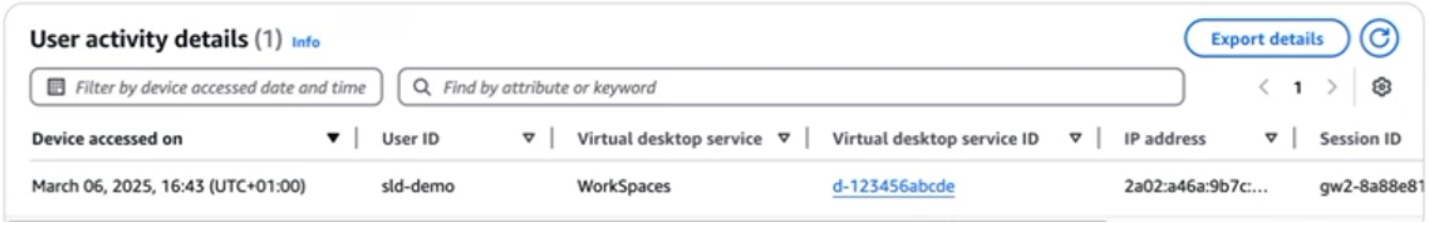
각 WorkSpaces 씬 클라이언트 디바이스에는 절전 모드가 있습니다. 다음 표에는이 모드의 상태가 나열되어 있습니다.



Element	설명
이후 디스플레이 끄기	디바이스가 디스플레이를 끄는 비활성 시간입니다.

사용자 활동

이 탭에는 특정 디바이스의 설정 및 사용 정보에 대한 로그가 표시됩니다. 다음 표에는이 로그의 각 요소가 나열되어 있습니다.



Element	설명
에서 액세스한 디바이스	디바이스가 활성화된 날짜 및 시간입니다.
사용자 ID	디바이스에 액세스하는 사용자의 식별 번호입니다.
가상 데스크톱 서비스	디바이스가 사용하는 가상 데스크톱 서비스입니다.
가상 데스크톱 서비스 ID	사용자와 연결된 가상 데스크톱 서비스 ID 번호입니다.
IP 주소	디바이스에 액세스하는 IP의 식별 번호입니다.

Element	설명
이벤트 유형	디바이스 사용 방법에 대한 세부 정보입니다.

> **Note**
>
> WorkSpaces Personal을 제외하고 VDIs 로그인 시작 이벤트만 표시합니다.

테이블 위의 검색 창을 사용하여 테이블에서 특정 정보를 찾을 수 있습니다. 날짜 및 시간을 기준으로 테이블 결과를 필터링할 수도 있습니다.

세부 정보 내보내기 버튼을 선택하여 테이블을 csv 파일로 내보낼 수 있습니다.

디바이스 이름 편집

1. 편집할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 디바이스를 검색할 수 있습니다.
2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 디바이스 이름 편집을 선택합니다. 디바이스 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 디바이스를 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**
>
> 등록을 강제로 취소하면 사용자가 로그아웃되며 세션 중에 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 강제로 보관하면 사용자가 로그아웃되고 세션 중에 WorkSpaces 씬 클라이언트 디바이스를 재부팅해야 합니다.

디바이스 삭제

1. 삭제할 디바이스를 선택합니다. 드롭다운 목록을 탐색하거나 검색 필드를 사용하여 디바이스를 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.

디바이스 세부 정보 내보내기

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

2. 작업 버튼을 선택합니다.
3. 드롭다운 목록에서 디바이스 세부 정보 내보내기를 선택합니다. 스프레드시트 형식으로 선택한 디바이스 다운로드에 대한 세부 정보입니다.

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 디바이스의 소프트웨어 애플리케이션 또는 운영 체제에 대한 업데이트가 포함될 수 있습니다. 이 콘솔에서 소프트웨어를 즉시 업데이트하도록 선택하거나 환경의 유지 관리 기간 동안 자동 업데이트를 예약할 수 있습니다.

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

주제

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

환경 소프트웨어 업데이트

WorkSpaces 씬 클라이언트는 사용자에게 가상 데스크톱에 대한 액세스 권한을 제공하는 AWS 최종 사용자 컴퓨팅 서비스입니다. 이러한 가상 데스크톱은 주기적으로 새 소프트웨어 세트로 업데이트됩니다. 환경 소프트웨어를 업데이트하려면 다음을 수행합니다.

1. 사용 가능한 소프트웨어 업데이트의 목록에서 소프트웨어 세트를 선택합니다. 소프트웨어 세트 목록은 WorkSpaces 씬 클라이언트 환경 소프트웨어 세트를 참조하세요.
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**
>
> 이제 소프트웨어를 업데이트하면 활성 사용자 세션이 중단될 수 있습니다.

- 각 환경 유지 관리 기간 동안 소프트웨어 업데이트 - 환경에 대해 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 디바이스는 새 소프트웨어로 주기적으로 업데이트됩니다. 디바이스 소프트웨어를 업데이트하려면 다음을 수행합니다.

1. 사용 가능한 소프트웨어 업데이트의 목록에서 소프트웨어 세트를 선택합니다.
2. 설치 버튼을 선택합니다.
3. 페이지 상단에서 디바이스를 선택합니다.
4. 디바이스 섹션의 목록에서 업데이트할 디바이스를 선택합니다. 소프트웨어 세트 목록은 WorkSpaces 씬 클라이언트 환경 소프트웨어 세트를 참조하세요.
5. 업데이트 예약 옵션에서 다음 중 하나를 선택하여 환경을 업데이트할 시기를 선택합니다.

   - 지금 소프트웨어 업데이트 - 디바이스 소프트웨어를 즉시 업데이트합니다.

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

   - 각 디바이스 유지 관리 기간 동안 소프트웨어 업데이트 - 디바이스의 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 액세스 권한을 제공하는 AWS 최종 사용자 컴퓨팅 서비스입니다. 이러한 디바이스는 새 소프트웨어 세트로 주기적으로 업데이트됩니다. 다음 표에서는 릴리스된 모든 소프트웨어 세트를 설명합니다. 관리자는 AWS 관리 콘솔을 사용하여 사용 가능한 소프트웨어 세트를 볼 수 있습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.16.1	7-3-2025	• Chromium의 CVE-2025-6554 중요 보안 문제에 대해 수정되었습니다.
2.16.0	6-27-2025	• 네트워크 지연 시간에 대한 알림이 추가되었습니다. • 세션 중에 두 번째 모니터가 어두워지는 것을 복구할 수 있는 기능이 추가되었습니다. • 디바이스가 절전 모드에서 돌아온 후 모니터가 흰색 화면을 표시하거나 자동 확장되지 않는 문제를 수정했습니다.
2.15.0	6-19-2025	• 라틴 아메리카 스페인어 및 국제 영어 키보드에 대한 지원이 추가되었습니다. • 디바이스가 장시간 키보드 또는 마우스 활동을 감지하지 못하면 최종 사용자에게 알림이 표시됩니다.
2.14.1	6-09-2025	• Chromium의 CVE-2025-5419 중요 보안 문제를 수정했습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.13.0	3-31-2025	• 최종 사용자는 제품 만족도 피드백 설문 조사를 알림으로 볼 수 있습니다. • FIDO2 인증 흐름에 대한 시험판 기능 지원을 추가합니다. FIDO2 세션 전 세부 정보를 참조하세요. • 세션에서 오디오/비디오가 재생 중이면 디바이스가 절전 모드로 전환되지 않습니다. • 모니터가 연결되고 연결이 끊어지면 최종 사용자에게 알림이 표시됩니다. • 디바이스는 서비스 개선을 위해 운영 체제에서 진단 정보를 수집합니다. • 소프트웨어 설치 날짜 설정에서 잘못된 날짜가 표시되는 문제를 해결합니다.
2.14.0	4-29-2025	• 사용성 개선 및 버그 수정.

소프트웨어 세트	릴리스 날짜	변경 사항
2.13.0	3-31-2025	• 최종 사용자는 제품 만족도 피드백 설문 조사를 알림으로 볼 수 있습니다. • FIDO2 인증 흐름에 대한 시험판 기능 지원을 추가합니다. FIDO2 세션 전 세부 정보를 참조하세요. • 세션에서 오디오/비디오가 재생 중이면 디바이스가 절전 모드로 전환되지 않습니다. • 모니터가 연결되고 연결이 끊어지면 최종 사용자에게 알림이 표시됩니다. • 디바이스는 서비스 개선을 위해 운영 체제에서 진단 정보를 수집합니다. • 소프트웨어 설치 날짜 설정에서 잘못된 날짜가 표시되는 문제를 해결합니다.
2.12.0	1-30-2025	• 마우스의 뒤로 버튼을 누를 때 최종 사용자가 세션에서 로그아웃되는 문제를 해결합니다.
2.11.2	1-24-2025	• 모니터 간 마우스 이동을 호출하는 동안 오디오가 깨지는 문제를 해결합니다.
2.11.1	12-27-2024	• 듀얼 모니터 자동 확장 문제를 해결합니다. • VoiceView 레이블이 약간 개선되었습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.11.0	12-19-2024	• WorkSpaces 씬 클라이언트는 이제 VoiceView 및 Magnifier를 지원합니다.
2.10.0	11-22-2024	• 최종 사용자는 키보드 바로 가기를 사용하여 디바이스 도구 모음을 축소할 수 있습니다.
2.9.0	10-28-2024	• 이제 관리자는 AWS 콘솔의 특정 디바이스의 디바이스 세부 정보 페이지에서 최종 사용자의 디바이스 설정을 볼 수 있습니다. • WorkSpaces 씬 클라이언트는 이제 단일 화면에 대해 2K 해상도 모니터를 지원합니다. • 최종 사용자는 WorkSpaces 씬 클라이언트 디바이스에서 네트워크 진단과 관련된 알림을 볼 수 있습니다. • 이제 최종 사용자는 기본 설정에 따라 왼쪽 또는 오른쪽에 디바이스 도구 모음을 배치하도록 선택할 수 있습니다. • 디바이스가 대기 또는 유휴 시간 동안 소프트웨어 업데이트를 설치하지 않는 문제를 수정했습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.8.1	09-26-2024	• 디바이스가 절전 모드로 전환된 후 두 번째 모니터를 켤 수 없는 중요한 문제를 수정했습니다.
2.8.0	09-06-2024	• 씬 클라이언트는 4K 해상도의 모니터를 지원합니다. • WorkSpaces 씬 클라이언트 디바이스 관리 서비스를 일시적으로 사용할 수 없는 경우에도 사용자는 VDI 세션에 연결할 수 있습니다. • AWS 콘솔의 사용자 활동 세부 정보 섹션에 중복 항목이 표시되는 문제를 수정했습니다. • 최종 사용자는 WorkSpaces 씬 클라이언트에서 WorkSpaces를 스트리밍하는 동안 PrintScreen 옵션을 사용할 수 있습니다. WorkSpaces
2.7.1	08-27-2024	• Chromium의 CVE-2024-7971 및 CVE-2024-7965 중요 보안 문제에 대한 제로데이 수정.

소프트웨어 세트	릴리스 날짜	변경 사항
2.7.0	07-29-2024	• 두 번째 모니터의 성능이 개선되었습니다. • 도구 모음 언어가 디바이스 언어 변경에 영향을 미치지 않는 문제를 수정했습니다. • 이제 디바이스는 서비스 개선을 위한 진단 정보를 수집합니다.
2.6.0	07-09-2024	• 사용자는 수신 소프트웨어 업데이트를 연기하여 중단 없이 작업을 완료할 수 있습니다. • 디바이스 설정을 통해 사용자는 저장된 WiFi 네트워크를 잊을 수 있습니다. • 세션의 오디오/비디오 호출 성능이 개선되었습니다. • VDI 세션에 대한 일부 사용자 설정은 디바이스 재부팅 후에도 유지됩니다.
2.5.0	06-13-2024	• 디바이스가 세션을 시작하기 전에 절전 모드에서 잠시 깨어날 때 키보드 및 마우스 설정 화면을 표시하는 문제를 수정했습니다. • 디바이스 도구 모음의 홈 버튼 이름이 로그인으로 변경되었습니다. • 세션의 오디오/비디오 호출 성능이 개선되었습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.4.3	05-29-2024	• Chromium의 CVE-2024-5274 중요 보안 문제에 대한 제로데이 수정.
2.4.2	05-17-2024	• Chromium의 CVE-2024-4947 중요 보안 문제에 대한 제로데이 수정.
2.4.1	05-15-2024	• Chromium의 CVE-2024-4671 및 CVE-2024-4761 중요 보안 문제에 대한 제로데이 수정. • WorkSpaces 로그인 페이지에서 AWS 및 프라이버시 링크를 마우스 오른쪽 버튼으로 클릭하여 브라우저를 독립 실행형 모드로 열 수 있었던 문제를 수정했습니다.
2.4.0	05-09-2024	• "accounts.google.com"을 차단하고 Google Workspace를 AppStream 2.0 세션의 IDP로 사용하지 못하는 문제를 수정했습니다. • 디바이스 설정 도구 모음은 화면의 아무 영역이나 클릭하면 자동으로 축소됩니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.3.0	04-05-2024	• 디바이스 설정이 축소된 도구 모음에 표시되므로 보이는 화면을 더 잘 활용할 수 있습니다. • 이제 최종 사용자는 디바이스가 비활성 상태에서 절전 모드로 전환되기 전에 대기하도록 기간을 구성할 수 있습니다. • 두 번째 디스플레이에 "about:blank" URL이 표시되는 문제를 수정했습니다. • 확장 디스플레이가 닫힐 때 흰색 화면이 나타나는 문제를 수정했습니다. • 최종 사용자가 설정한 볼륨 수준은 이제 디바이스 재시작 후에도 유지됩니다.
2.2.1	02-16-2024	• 사용자가 SAML 2.0 인증으로 구성된 WorkSpaces에 로그인하지 못하게 하는 로그인 프로세스 중에 발생하는 문제를 수정했습니다.
2.2.0	02-08-2024	• 영어(영국), 프랑스어, 독일어, 이탈리아어, 스페인어 로캘이 있는 ISO 키보드에 대한 지원이 추가되었습니다.

소프트웨어 세트	릴리스 날짜	변경 사항
2.1.2	01-26-2024	• Chromium의 CVE-2024-0519 중요 보안 문제에 대한 제로데이 수정. • 잠금 기능과 관련된 최종 사용자 지연 시간 개선. • 내부 디바이스 경계 엔드포인트는 'thinclient*' 도메인으로 전환됩니다.
2.1.1	12-21-2023	• Chromium의 CVE-2023-7024 중요 보안 문제에 대한 제로데이 수정.
2.1.0	12-20-2023	• 디바이스 설정에 홈 버튼을 추가하고 메타 키에 대한 지원을 활성화합니다. 이렇게 하면 최종 사용자가 Meta+L을 눌러 잠금 화면을 호출할 수 있습니다.
2.0.1	12-06-2023	• Chromium의 CVE-2024-6345 중요 보안 문제에 대한 제로데이 수정.
2.0.0	11-15-2023	• 초기 릴리스

WorkSpaces 씬 클라이언트 리소스에 대한 태그 사용

자체 메타데이터를 각 리소스에 태그로 지정하여 WorkSpaces 씬 클라이언트 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 간단하지만 강력한 방법으로 사용하여 AWS 리소스를 관리하고 결제 데이터를 포함한 데이터를 구성할 수 있습니다.

기존 리소스에 태그를 추가하면 해당 태그는 다음 달 첫날까지 비용 할당 보고서에 표시되지 않습니다. 예를 들어 7월 15일에 기존 WorkSpaces 씬 클라이언트 디바이스에 태그를 추가하면 8월 1일까지 비용 할당 보고서에 태그가 표시되지 않습니다. 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

> **Note**
>
> Cost Explorer에서 WorkSpaces 씬 클라이언트 리소스 태그를 보려면 AWS Billing 사용 설명서의 사용자 정의 비용 할당 태그 활성화에 나와 있는 지침에 따라 WorkSpaces 씬 클라이언트 리소스에 적용한 태그를 활성화해야 합니다.
> 태그는 활성화 후 24시간에 표시되지만 해당 태그와 연결된 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 Explorer는 태그가 활성화된 시점의 비용 데이터만 표시합니다. 현재로서는 과거 데이터가 제공되지 않습니다.

태그를 지정할 수 있는 리소스:

- WorkSpaces 씬 클라이언트 환경에서 다음 리소스를 생성할 때 해당 리소스에 태그를 추가할 수 있습니다.
- WorkSpaces 씬 클라이언트 환경, 디바이스 및 소프트웨어 세트 유형의 기존 리소스에 태그를 추가할 수 있습니다.
- 디바이스를 등록할 때 자동으로 적용되도록 환경의 디바이스에 대한 태그를 구성할 수 있습니다.

태그 제한

- 리소스당 최대 태그 수 - 50개
- 최대 키 길이 - 유니코드 문자 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.
- 태그 이름 또는 값은 AWS 사용하기 위해 예약되어 있으므로 `aws:` 접두사를 사용하지 마세요. 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다.

콘솔을 사용하여 기존 환경의 태그를 관리하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 환경을 선택하여 세부 정보 페이지를 엽니다.
3. 편집을 선택합니다.
4. 태그 섹션에서 다음 중 하나 이상을 수행합니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
   - 태그를 업데이트하려면 값 값을 편집합니다.
   - 태그를 삭제하려면 태그 옆의 제거를 선택합니다.
5. 태그 업데이트가 완료되면 저장을 선택합니다.

콘솔을 사용하여 기존 디바이스의 태그를 관리하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 디바이스를 선택하여 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 값 값을 편집합니다.
   - 태그를 삭제하려면 태그 옆의 제거를 선택합니다.
6. 태그 업데이트가 완료되면 저장을 선택합니다.

콘솔을 사용하여 새 디바이스의 태그를 관리하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.

2. 환경을 선택하여 세부 정보 페이지를 엽니다.
3. 편집을 선택합니다.
4. 디바이스 생성 태그 섹션에서 다음 중 하나 이상을 수행합니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키 및 값의 값을 편집합니다.
   - 태그를 업데이트하려면 값 값을 편집합니다.
   - 태그를 삭제하려면 태그 옆의 제거를 선택합니다.
5. 태그 업데이트가 완료되면 저장을 선택합니다.

디바이스가 생성되면 환경에 등록되고 디바이스 생성 태그가 적용됩니다. 이는 새 디바이스 등록 중에만 발생합니다. 또한 `aws:thinclient:environment-id` 시스템 태그는 값으로 사용되는 환경 ID와 함께 적용됩니다.

콘솔을 사용하여 소프트웨어 업데이트에 대한 태그를 관리하려면

1. WorkSpaces 씬 클라이언트 콘솔을 엽니다.
2. 소프트웨어 업데이트를 선택하여 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 값 값을 편집합니다.
   - 태그를 삭제하려면 태그 옆의 제거를 선택합니다.
5. 태그 업데이트가 완료되면 저장을 선택합니다.

Amazon WorkSpaces 씬 클라이언트의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

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

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드.는 안전하게 사용할 수 있는 서비스 AWS 도 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon WorkSpaces 씬 클라이언트에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 WorkSpaces 씬 클라이언트 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 WorkSpaces 씬 클라이언트를 구성하는 방법을 보여줍니다. WorkSpaces 씬 클라이언트 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 배울 수도 있습니다.

주제

- Amazon WorkSpaces 씬 클라이언트의 데이터 보호
- Amazon WorkSpaces 씬 클라이언트의 ID 및 액세스 관리
- Amazon WorkSpaces 씬 클라이언트의 복원력
- Amazon WorkSpaces 씬 클라이언트에서 취약성 분석 및 관리

Amazon WorkSpaces 씬 클라이언트의 데이터 보호

AWS 공동 책임 모델 Amazon WorkSpaces 씬 클라이언트의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버

시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 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 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 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 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 WorkSpaces 씬 클라이언트 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 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 증명을 URL에 포함해서는 안 됩니다.

Amazon WorkSpaces 씬 클라이언트는 WorkSpaces 씬 클라이언트 디바이스의 사용자 사용 및 가상 데스크톱 서비스와의 상호 작용에 대한 정보를 수집하고 제공합니다. 예를 들어 사용 가능한 메모리, 네트워크 진단, 네트워크 정보, 디바이스 연결, SAML 자격 증명, 디바이스 식별 정보 및 충돌 보고서가 있습니다. 이 정보는 서비스를 제공하는 데 사용되며 서비스에 대한 사용자 경험을 개선하는 데 사용될 수 있습니다. 또한 사용자에게 서비스를 제공하기 위한 목적으로만 사용자가 서비스를 사용하는 AWS 리전 외부로 정보가 전송될 수 있습니다. 당사는이 정보를 AWS 개인 정보 보호 고지에 따라 처리합니다.

주제

데이터 암호화

WorkSpaces 씬 클라이언트는 사용자 설정, 디바이스 식별자, ID 공급자 정보, 스트리밍 데스크톱 식별자 등의 환경 및 디바이스 사용자 지정 데이터를 수집합니다. WorkSpaces 씬 클라이언트는 세션 타임스탬프도 수집합니다. 수집된 데이터는 Amazon DynamoDB 및 Amazon S3에 저장됩니다. WorkSpaces 씬 클라이언트는 암호화에 AWS Key Management Service (KMS)를 사용합니다.

콘텐츠를 보호하려면 다음 지침을 따릅니다.

- 최소 권한 액세스를 구현하고 WorkSpaces 씬 클라이언트 작업에 사용할 특정 역할을 생성합니다.
- 제공된 키로 WorkSpaces씬 클라이언트가 저장 데이터를 암호화할 수 있도록 고객 관리형 키를 제공하여 데이터를 처음부터 끝까지 보호합니다.
- 환경 활성화 코드와 사용자 보안 인증 정보를 공유하지 않도록 주의해야 합니다.
  - 관리자는 WorkSpaces 씬 클라이언트 콘솔에 로그인해야 하며, 사용자는 보안 인증 정보를 사용하여 스트리밍 데스크톱에 로그인하려면 WorkSpaces 씬 클라이언트 설치 시에 활성화 코드를 제공해야 합니다.
  - 물리적 액세스 권한이 있는 사용자는 WorkSpaces 씬 클라이언트를 설정할 수 있지만, 로그인하기 위한 유효한 활성화 코드와 사용자 보안 인증 정보가 없으면 세션을 시작할 수 없습니다.
- 사용자는 디바이스 도구 모음을 사용하여 화면을 잠그거나 재부팅하거나 디바이스를 종료하도록 선택하여 세션을 명시적으로 종료할 수 있습니다. 이렇게 하면 디바이스 세션이 삭제되고 세션 보안 인증 정보가 지워집니다.

WorkSpaces 씬 클라이언트는 AWS KMS를 사용하여 민감한 모든 데이터를 암호화하여 기본적으로 콘텐츠와 메타데이터를 보호합니다. 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 씬 클라이언트는 기본적으로 암호화를 제공하여 AWS 소유 암호화 키를 사용하여 저장된 민감한 고객 데이터를 보호합니다.

- AWS 소유 키 - Amazon WorkSpaces 씬 클라이언트는 기본적으로 이러한 키를 사용하여 개인 식별 데이터를 자동으로 암호화합니다. AWS 소유 키를 보거나 관리하거나 사용하거나 사용을 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 씬 클라이언트는 사용자가 생성, 소유 및 관리하는 대칭 고객 관리형 키 사용을 지원하여 기존 AWS 소유 암호화에 두 번째 암호화 계층을 추가합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.
  - 키 정책 수립 및 유지
  - IAM 정책 수립 및 유지
  - 키 정책 활성화 및 비활성화
  - 키 암호화 자료 교체
  - 태그 추가
  - 키 별칭 만들기
  - 삭제를 위한 스케줄 키

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

다음 표에는 Amazon WorkSpaces 씬 클라이언트가 개인 식별 데이터를 암호화하는 방법이 요약되어 있습니다.

데이터 유형	AWS 소유 키 암호화	고객 관리형 키 암호화 (선택 사항)
환경 이름	활성화됨	활성화됨

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

> **Note**
>
> Amazon WorkSpaces 씬 클라이언트는 AWS 소유 키를 사용하여 개인 식별 데이터를 무료로 보호하여 저장 시 암호화를 자동으로 활성화합니다.
> 그러나 고객 관리형 키를 사용하는 경우 AWS KMS 요금이 적용됩니다. 요금에 대한 자세한 내용은 AWS 키 관리 서비스 요금을 참조하세요.

Amazon WorkSpaces 씬 클라이언트가 AWS KMS를 사용하는 방법

Amazon WorkSpaces 씬 클라이언트에서 고객 관리형 키를 사용하려면 키 정책이 필요합니다.

Amazon WorkSpaces 씬 클라이언트는 다음과 같은 내부 작업에 고객 관리형 키를 사용하려면 키 정책이 필요합니다.

- AWS KMS에 데이터를 암호화하는 `GenerateDataKey` 요청을 보냅니다.
- AWS KMS에 `Decrypt` 요청을 전송하여 암호화된 데이터를 해독합니다.

언제든지 고객 관리형 키에 대한 서비스의 액세스를 제거할 수 있습니다. 그렇게 하면 Amazon WorkSpaces 씬 클라이언트는 고객 관리형 키로 암호화된 데이터에 액세스할 수 없으며, 이는 해당 데이터에 의존하는 모든 작업에 영향을 미치고 비동기식 워크플로에서 오류 및 실패로 이어집니다. 예를 들어 WorkSpaces 씬 클라이언트가 액세스할 수 없는 환경 세부 정보를 가져오려고 하면 작업이 `AccessDeniedException` 오류를 반환합니다. 또한 WorkSpaces 씬 클라이언트 디바이스가 WorkSpaces 씬 클라이언트 환경을 사용할 수 없게 됩니다.

고객 관리형 키 생성

AWS Management Console 또는 AWS KMS API 작업을 사용하여 대칭 고객 관리형 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 정책에서는 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 만들 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서에서 고객 관리형 키 액세스 관리를 참조하세요.

Amazon WorkSpaces 씬 클라이언트 리소스에서 고객 관리형 키를 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- `kms:DescribeKey` - Amazon WorkSpaces 씬 클라이언트가 키를 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.
- `kms:GenerateDataKey` - 고객 관리형 키를 사용하여 데이터를 암호화하도록 허용합니다.
- `kms:Decrypt` - 고객 관리형 키를 사용하여 데이터를 복호화하도록 허용합니다.

다음은 Amazon WorkSpaces 씬 클라이언트에 대해 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"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
 data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                         "arn:aws:thinclient:region:111122223333:*",
                    "kms:EncryptionContext:aws:thinclient:arn":
                         "arn:aws:thinclient:region: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*"
            ],
            "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 관리형 키 지정

두 번째 암호화 계층으로서 다음 리소스에 고객 관리형 키를 지정할 수 있습니다.

- WorkSpaces 씬 클라이언트 환경

환경을 생성할 때 Amazon WorkSpaces 씬 클라이언트가 개인 식별 데이터를 암호화하는 데 사용하는 `kmsKeyArn`를 제공하여 데이터 키를 지정할 수 있습니다.

- `kmsKeyArn` - AWS KMS 고객 관리형 키의 키 식별자입니다. 키 ARN을 제공합니다.

고객 관리형 키로 암호화된 WorkSpaces 씬 클라이언트 환경에 새 WorkSpaces 씬 클라이언트 디바이스가 추가되면 WorkSpaces 씬 클라이언트 디바이스는 WorkSpaces 씬 클라이언트 환경에서 고객 관리형 키 설정을 상속합니다.

암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함하는 선택적 키-값 페어 세트입니다.

AWS KMS는 암호화 컨텍스트를 추가 인증 데이터로 사용하여 인증된 암호화를 지원합니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함하면 AWS KMS는 암호화 컨텍스트를 암호화된 데이터에 바인딩합니다. 데이터를 복호화하려면 요청에 동일한 암호화 컨텍스트를 포함합니다.

Amazon WorkSpaces 씬 클라이언트 암호화 컨텍스트

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

다음은 환경 암호화 컨텍스트입니다.

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

다음은 디바이스 암호화 컨텍스트입니다.

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

모니터링을 위한 암호화 컨텍스트 사용

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

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

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

다음 예는 Amazon WorkSpaces `DescribeKey`씬 클라이언트가 고객 관리형 키로 암호화된 데이터에 액세스하기 위해 호출한 KMS 작업을 모니터링하기 위한 , `Decrypt`, `GenerateDataKey`에 대한 AWS CloudTrail 이벤트입니다.

다음 예제에서는 WorkSpaces 씬 클라이언트 환경에 `encryptionContext` 대해를 볼 수 있습니다. WorkSpaces 씬 클라이언트 디바이스에 대해 유사한 CloudTrail 이벤트가 기록됩니다.

DescribeKey

Amazon WorkSpaces 씬 클라이언트는 `DescribeKey` 작업을 사용하여 KMS 고객 관리형 AWS 키를 확인합니다.

다음 예제 이벤트는 `DescribeKey` 작업을 기록합니다.


```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
```

```
    "eventTime": "2024-04-08T13:44:22Z",
    "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"
}
```


GenerateDataKey

Amazon WorkSpaces 씬 클라이언트는 GenerateDataKey 작업을 사용하여 데이터를 암호화합니다.

다음 예제 이벤트는 GenerateDataKey 작업을 기록합니다.


```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
```

```
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

Amazon WorkSpaces 씬 클라이언트가 GenerateDataKey 저장 디바이스 정보를 사용하는 경우 GenerateDataKey 작업을 사용하여 데이터를 암호화합니다.

이 GenerateDataKey 작업은 Sid "Amazon WorkSpaces 씬 클라이언트 서비스가 데이터를 암호화 및 복호화하도록 허용"을 사용하여 KMS 키 정책 문에서 허용됩니다.

다음 예제 이벤트는 GenerateDataKey 작업을 기록합니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces 씬 클라이언트는 `Decrypt` 작업을 사용하여 데이터를 복호화합니다.

다음 예제 이벤트는 `Decrypt` 작업을 기록합니다.

```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
```

```
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt (by service)

WorkSpaces 씬 클라이언트 디바이스가 환경 또는 디바이스 정보에 액세스하면 `Decrypt` 작업을 사용하여 데이터를 복호화합니다. 이 `Decrypt` 작업은 Sid "Amazon WorkSpaces 씬 클라이언트 서비스가 데이터를 암호화하고 복호화하도록 허용"을 사용하여 KMS 키 정책 문에서 허용됩니다.

다음 예제 이벤트는를 통해 승인된 `Decrypt` 작업을 기록합니다. `Grant`

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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 Key Management Service 개발자 안내서를 참조하세요.

전송 중 암호화

WorkSpaces씬 클라이언트는 HTTPS 및 TLS 1.2의 전송 중 데이터를 암호화합니다. 콘솔이나 API 직접 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 WorkSpaces 씬 클라이언트로 전송할 수 있습니다. 여기에는 디바이스의 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 작업 트래픽 개인 정보 보호

관리자는 시작 시간, 보류 중인 소프트웨어 업데이트 정보 등의 WorkSpaces 씬 클라이언트 세션 이벤트를 볼 수 있습니다. 이러한 로그는 암호화되어 WorkSpaces 씬 클라이언트에서 고객에게 안전

하게 전달됩니다. 개별 스트리밍 데스크톱 세션에 대한 사용자 정보와 추가 세부 정보는 데스크톱 서비스에서 기록합니다. 자세한 내용은 WorkSpaces 모니터링, AppStream 2.0 모니터링 및 보고 또는 WorkSpaces Web의 사용자 액세스 로깅을 참조하세요.

Amazon WorkSpaces 씬 클라이언트의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 WorkSpaces 씬 클라이언트 리소스를 사용하도록 누가 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 WorkSpaces 씬 클라이언트에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - WorkSpaces 씬 클라이언트 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 WorkSpaces 씬 클라이언트 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. WorkSpaces 씬 클라이언트의 기능에 액세스할 수 없는 경우에는 Amazon WorkSpaces 씬 클라이언트 보안 인증 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 WorkSpaces 씬 클라이언트 리소스를 책임지고 있는 경우에는 WorkSpaces 씬 클라이언트에 대한 전체 액세스 권한을 가지고 있을 가능성이 있습니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 WorkSpaces 씬 클라이언트 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여

IAM의 기본 개념을 이해하세요. 회사가 WorkSpaces 씬 클라이언트에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon WorkSpaces 씬 클라이언트에서 IAM을 사용하는 방법 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 WorkSpaces 씬 클라이언트에 대한 액세스 권한 관리 정책의 작성 방법을 자세히 알고 싶을 수 있습니다. IAM에서 사용할 수 있는 WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시를 보려면 Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시 섹션을 참조하세요.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. , AWS 계정 루트 사용자 IAM 사용자 또는 IAM 역할을 수임하여 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 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 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업

을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

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

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 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 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 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 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/

id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 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 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 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 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에

나타나 AWS 계정 며 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 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 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, 사용자 및 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 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 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 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어

정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 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 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon WorkSpaces 씬 클라이언트에서 IAM을 사용하는 방법

IAM을 사용하여 WorkSpaces 씬 클라이언트에 대한 액세스를 관리하기 전에 WorkSpaces 씬 클라이언트와 함께 사용할 수 있는 IAM 기능을 알아봅니다.

Amazon WorkSpaces 씬 클라이언트에서 사용할 수 있는 IAM 기능

IAM 기능	WorkSpaces 씬 클라이언트 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 기능	WorkSpaces 씬 클라이언트 지원
ACLs	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 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

WorkSpaces 씬 클라이언트 보안 인증 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시

WorkSpaces 씬 클라이언트 보안 인증 기반 정책의 예시를 보려면 Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시 섹션을 참조하세요.

WorkSpaces 씬 클라이언트 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

WorkSpaces 씬 클라이언트에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 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 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

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

WorkSpaces 씬 클라이언트 작업 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces 씬 클라이언트에서 정의한 작업을 참조하세요.

WorkSpaces 씬 클라이언트의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
thinclient
```

단일 문에서 여러 작업을 지정하려면 다음 예제와 같이 쉼표로 구분합니다.

```
"Action": [
```

```
      "thinclient:action1",
      "thinclient:action2"
         ]
```

WorkSpaces 씬 클라이언트 보안 인증 기반 정책의 예시를 보려면 Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시 섹션을 참조하세요.

WorkSpaces 씬 클라이언트에 대한 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. 문에는 `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 이를 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 해당 ARN 목록을 보려면 서비스 승인 참조에서 Amazon WorkSpaces 씬 클라이언트에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon WorkSpaces 씬 클라이언트에서 정의한 작업을 참조하세요.

WorkSpaces 씬 클라이언트 보안 인증 기반 정책의 예시를 보려면 Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시 섹션을 참조하세요.

WorkSpaces 씬 클라이언트에 사용되는 정책 조건 키

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 작음과 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 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 문의 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 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

WorkSpaces 씬 클라이언트 조건 키 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces 씬 클라이언트에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon WorkSpaces 씬 클라이언트에서 정의한 작업을 참조하세요.

WorkSpaces 씬 클라이언트 보안 인증 기반 정책의 예시를 보려면 Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시 섹션을 참조하세요.

WorkSpaces 씬 클라이언트의 ACL

ACL 지원: 아니요

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

WorkSpaces Thin Client의 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

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

태그에 근거하여 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 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

WorkSpaces 씬 클라이언트에서 임시 보안 인증 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 포함한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommds에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

WorkSpaces 씬 클라이언트의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 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 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 WorkSpaces 씬 클라이언트 기능이 중단될 수 있습니다. WorkSpaces 씬 클라이언트에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

WorkSpaces 씬 클라이언트의 서비스 연결 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 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 서비스를 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amazon WorkSpaces 씬 클라이언트 보안 인증 기반 정책 예시

기본적으로 사용자 및 역할은 WorkSpaces 씬 클라이언트 리소스를 생성하거나 수정할 수 있는 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 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 WorkSpaces씬 클라이언트에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Amazon WorkSpaces 씬 클라이언트에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

정책 모범 사례

보안 인증 기반 정책에 따라 계정에서 사용자가 WorkSpaces 씬 클라이언트 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 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 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- 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 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

WorkSpaces 씬 클라이언트 콘솔 사용

Amazon WorkSpaces 씬 클라이언트 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한은에서 WorkSpaces 씬 클라이언트 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

WorkSpaces 씬 클라이언트에 대한 읽기 전용 액세스 권한 부여

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

JSON

```
{
    "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 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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 모든 액세스 권한 부여

이 예제에서는 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.

JSON

```
{
    "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/*"]
        }
    ]
}
```

AWS Amazon WorkSpaces 씬 클라이언트에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonWorkSpacesThinClientReadOnlyAccess

`AmazonWorkSpacesThinClientReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다. 이 정책은 WorkSpaces 씬 클라이언트 서비스 및 해당 종속성에 대한 전체 액세스 권한을 부여합니다. 이 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 가이드의 AmazonWorkSpacesThinClientReadOnlyAccess를 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `thinclient` (WorkSpaces 씬 클라이언트) - 모든 WorkSpaces 씬 클라이언트 작업에 대한 읽기 전용 액세스를 허용합니다.
- `workspaces` (WorkSpaces) - WorkSpaces 디렉터리 및 연결 별칭을 설명할 수 있는 권한을 허용합니다. 이는 WorkSpaces 리소스가 WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.
- `workspaces-web` (WorkSpaces Secure Browser) - WorkSpaces Secure Browser 포털 및 사용자 설정을 설명할 수 있는 권한을 허용합니다. 이는 WorkSpaces Secure Browser 리소스가 WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.
- `appstream` (AppStream 2.0) - AppStream 2.0 스택을 설명할 수 있는 권한을 허용합니다. 이는 AppStream 2.0 리소스가 WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS 관리형 정책: AmazonWorkSpacesThinClientFullAccess

`AmazonWorkSpacesThinClientFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다. 이 정책은 WorkSpaces 씬 클라이언트 서비스 및 해당 종속성에 대한 전체 액세스 권한을 부여합니다. 이 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 안내서의 AmazonWorkSpacesThinClientFullAccess를 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `thinclient` (WorkSpaces 씬 클라이언트) - 모든 WorkSpaces 씬 클라이언트 작업에 대한 전체 액세스를 허용합니다.
- `workspaces` (WorkSpaces) - WorkSpaces 디렉터리 및 연결 별칭을 설명할 수 있는 권한을 허용합니다. 이는 WorkSpaces 리소스가 WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.
- `workspaces-web` (WorkSpaces Secure Browser) - WorkSpaces Secure Browser 포털 및 사용자 설정을 설명할 수 있는 권한을 허용합니다. 이는 WorkSpaces Secure Browser 리소스가

WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.

- `appstream` (AppStream 2.0) - AppStream 2.0 스택을 설명할 수 있는 권한을 허용합니다. 이는 AppStream 2.0 리소스가 WorkSpaces 씬 클라이언트와 호환되는지 확인하는 데 사용됩니다. WorkSpaces 씬 클라이언트 AWS 콘솔에 이러한 리소스를 표시하는 데도 사용됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
```

```
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS 관리형 정책에 대한 WorkSpaces 씬 클라이언트 업데이트

변경 사항	설명	날짜
AmazonWorkSpacesThinClientReadOnlyAccess - 정책 업데이트	WorkSpaces 씬 클라이언트는 디바이스 세부 정보 및 WorkSpaces 연결 별칭에 대한 제한된 읽기 권한을 포함하도록 정책을 업데이트했습니다.	2025년 1월 9일
AmazonWorkSpacesThinClientFullAccess - 정책 업데이트	WorkSpaces 씬 클라이언트는 WorkSpaces 연결 별칭에 대한 제한된 읽기 권한을 포함하도록 정책을 업데이트했습니다.	2025년 1월 9일
AmazonWorkSpacesThinClientReadOnlyAccess - 정책 업데이트	WorkSpaces 씬 클라이언트는 AppStream 2.0, WorkSpaces Web 및 WorkSpaces.	2024년 8월 9일
AmazonWorkSpacesThinClientFullAccess - 새 정책	Amazon WorkSpaces 씬 클라이언트에 대한 전체 액세스 권한과 필요한 관련 서비스에 대한 제한된 액세스를 제공합니다.	2024년 8월 9일
AmazonWorkSpacesThinClientReadOnlyAccess - 새 정책	Amazon WorkSpaces 씬 클라이언트 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.	2024년 7월 19일

변경 사항	설명	날짜
WorkSpaces 씬 클라이언트에서 변경 사항 추적 시작	WorkSpaces 씬 클라이언트가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2024년 7월 19일

Amazon WorkSpaces 씬 클라이언트 보안 인증 및 액세스 문제 해결

다음 정보를 사용하여 WorkSpaces 씬 클라이언트 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- WorkSpaces씬 클라이언트에서 작업을 수행할 권한이 없음
- 액세스 키를 보아야 합니다.
- 관리자인데, 다른 사용자가 WorkSpaces 씬 클라이언트에 액세스할 수 있게 허용하려고 합니다
- 내 외부의 사람이 내 WorkSpaces 씬 클라이언트 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

WorkSpaces씬 클라이언트에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 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 `thinclient:`*`ListDevices`* 권한이 없을 때 발생합니다.

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

이 경우 Mateo는 작업을 사용하여 *`my-thin-client-device`* 리소스에 액세스할 수 있도록 정책을 업데이트하도록 관리자에게 요청합니다`thinclient:`*`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 누군가에게에 대한 영구 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 관리를 참조하십시오.

관리자인데, 다른 사용자가 WorkSpaces 씬 클라이언트에 액세스할 수 있게 허용하려고 합니다

다른 사용자가 WorkSpaces 씬 클라이언트에 액세스하도록 허용하려면 액세스 권한이 필요한 사용자 또는 애플리케이션에 권한을 부여해야 합니다. AWS IAM Identity Center 를 사용하여 사용자 및 애플리케이션을 관리하는 경우 사용자 또는 그룹에 권한 세트를 할당하여 액세스 수준을 정의합니다. 권한 세트는 IAM 정책을 자동으로 생성하고 사용자 또는 애플리케이션과 연결된 IAM 역할에 할당합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 권한 세트를 참조하세요.

IAM Identity Center를 사용하지 않는 경우 액세스가 필요한 사용자 또는 애플리케이션에 대한 IAM 엔터티(사용자 또는 역할)를 생성해야 합니다. 그런 다음 WorkSpaces 씬 클라이언트에 대한 올바른 권한을 부여하는 정책을 엔터티에 연결해야 합니다. 권한이 부여되면 사용자 또는 애플리케이션 개발자에게 자격 증명을 제공합니다. 이들은 이 자격 증명을 사용하여 AWS에 액세스합니다. IAM 사용자, 그룹, 정책, 권한 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM ID 및 IAM 정책과 권한을 참조하세요.

자세한 내용은 WorkSpaces 씬 클라이언트에 대한 모든 액세스 권한 부여 단원을 참조하십시오.

내 외부의 사람이 내 WorkSpaces 씬 클라이언트 리소스에 액세스 AWS 계정 하도록 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 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- WorkSpaces 씬 클라이언트에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon WorkSpaces 씬 클라이언트에서 IAM을 사용하는 방법 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Amazon WorkSpaces 씬 클라이언트의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 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.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 WorkSpaces 씬 클라이언트는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

Amazon WorkSpaces 씬 클라이언트에서 취약성 분석 및 관리

구성 및 IT 제어는 AWS 와 사용자 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

Amazon WorkSpaces 씬 클라이언트는 Amazon WorkSpaces, Amazon AppStream 2.0 및 WorkSpaces Web과 상호 통합됩니다. 이러한 각 서비스의 업데이트 관리에 대한 자세한 내용은 다음 링크를 참조하세요.

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

Amazon WorkSpaces 씬 클라이언트 모니터링

모니터링은 Amazon WorkSpaces 씬 클라이언트 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 WorkSpaces 씬 클라이언트를 관찰하고, 문제가 있을 때 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 AWS 제공합니다.

- AWS CloudTrail는 AWS 계정에서 또는 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 를 호출한 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

주제

AWS CloudTrail을 사용하여 Amazon WorkSpaces 씬 클라이언트 API 직접 호출 로깅

Amazon WorkSpaces 씬 클라이언트는 사용자AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스인와 통합됩니다 AWS 서비스. CloudTrail은 WorkSpaces 씬 클라이언트에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처된 호출에는 WorkSpaces 씬 클라이언트 콘솔에서 수행된 호출과 WorkSpaces 씬 클라이언트 API 작업에 대한 코드 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 WorkSpaces 씬 클라이언트에 수행된 요청, 요청이 수행된 IP 주소, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

모든 Amazon WorkSpaces 씬 클라이언트 작업은 CloudTrail에서 로깅되며 Amazon WorkSpaces 씬 클라이언트 API 참조에 문서화됩니다. 예를 들어 `CreateEnvironment`, `DeleteDevice`, `GetSoftwareSet` 작업을 직접 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자로 했는지 사용자 보안 인증으로 했는지 여부.
- IAM Identity Center 사용자를 대신하여 요청이 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화되며 CloudTrail 이벤트 기록에 자동으로 액세스할 수 있습니다. CloudTrail 이벤트 기록은 지난 90일 간 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 자세한 설명은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하세요. Event history(이벤트 기록) 보기는 CloudTrail 요금이 부과되지 않습니다.

AWS 계정 지난 90일 동안 이벤트를 지속적으로 기록하려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 를 사용하여 생성된 모든 추적 AWS Management Console 은 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정 AWS 리전 의 모든에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Creating a trail for your AWS 계정 및 Creating a trail for an organization을 참조하세요.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS CloudTrail Lake 작업을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail의 WorkSpaces 씬 클라이언트 데이터 이벤트

데이터 이벤트는 리소스에서 또는 리소스에서 수행되는 리소스 작업에 대한 정보를 제공합니다(예: 최종 사용자의 디바이스 등록). 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다. 기본적으로 CloudTrail은 데이터 이벤트를 로깅하지 않습니다. CloudTrail 이벤트 기록은 데이터 이벤트를 기록하지 않습니다.

데이터 이벤트에는 추가 요금이 적용됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail 콘솔 AWS CLI또는 CloudTrail API 작업을 사용하여 WorkSpaces 씬 클라이언트 리소스 유형에 대한 데이터 이벤트를 로깅할 수 있습니다. 데이터 이벤트를 로깅하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Logging data events with the AWS Management Console 및 Logging data events with the AWS Command Line Interface를 참조하세요.

다음 표에는 데이터 이벤트를 로깅할 수 있는 WorkSpaces 씬 클라이언트 리소스 유형이 나열되어 있습니다. 데이터 이벤트 유형(콘솔) 열에는 CloudTrail 콘솔의 데이터 이벤트 유형 목록에서 선택할 값이 표시됩니다. resources.type 값 열에는 AWS CLI 또는 CloudTrail APIs를 사용하여 고급 이벤트 선택기를 구성할 때 지정하는 `resources.type` 값이 표시됩니다. CloudTrail에 로깅되는 데이터 API 열에는 리소스 유형에 대해 CloudTrail에 로깅된 API 호출이 표시됩니다.

데이터 이벤트 유형(콘솔)	resources.type 값	CloudTrail에 로깅되는 데이터 API
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

`eventName`, `readOnly` 및 `resources.ARN` 필드를 필터링하여 중요한 이벤트만 로깅하도록 고급 이벤트 선택기를 구성할 수 있습니다. 이러한 필드에 대한 자세한 내용은 AWS CloudTrail API 참조의 AdvancedFieldSelector 섹션을 참조하세요.

CloudTrail의 WorkSpaces 씬 클라이언트 관리 이벤트

관리 이벤트는의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다 AWS 계정. 이를 컨트롤 플레인 작업이라고도 합니다. 기본적으로 CloudTrail은 관리 이벤트를 로깅합니다.

Amazon WorkSpaces 씬 클라이언트는 모든 WorkSpaces 씬 클라이언트 컨트롤 플레인 작업을 관리 이벤트로 기록합니다. WorkSpaces 씬 클라이언트가 CloudTrail에 로그하는 Amazon WorkSpaces

WorkSpaces 씬 클라이언트 제어 영역 작업 목록은 Amazon WorkSpaces 씬 클라이언트 API 참조를 참조하세요. CloudTrail

WorkSpaces 씬 클라이언트 이벤트 예제

이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청된 API 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 추적이 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

다음 예제는 `RegisterDevice` 작업을 시연하는 CloudTrail 이벤트를 보여줍니다.


```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-06-19T17:13:44Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "RegisterDevice",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "dsn": "G1X11X11111111XX",
        "activationCode": "xxx1xxx1",
        "model": "AFTGAZL"
      },
      "responseElements": null,
      "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
      "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "eventCategory": "Data"
```

```
    }
```

다음 예제는 UpdateDeviceDetails 작업을 시연하는 CloudTrail 이벤트를 보여줍니다.

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "UpdateDeviceDetails",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
      "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsServiceEvent",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "serviceEventDetails": {
        "settings": {
          "network": {
            "ethernet": {
              "addresses": [
                {
                  "gateway": "gateway",
                  "localIp": "localIp",
                  "type": "IPV4"
                }
              ],
              "connectionStatus": "NOT_CONNECTED"
```

```
            },
            "networkInterfaceInUse": "ETHERNET",
            "wifi": {
              "addresses": [
                {
                  "gateway": "gateway",
                  "localIp": "localIp",
                  "type": "IPV4"
                }
              ],
              "connectionStatus": "NOT_CONNECTED"
            }
          },
          "peripherals": {
            "bluetooth": {
              "enabledStatus": "ENABLED"
            },
            "keyboards": [
              {
                "name": "name",
                "type": "USB"
              }
            ],
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
              }
            ],
            "sound": {
              "microphones": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ],
              "speakers": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ]
```

```
            },
            "webcams": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "USB"
              }
            ]
          },
          "powerAndSleep": {
            "sleepAfter": "FIFTEEN_MINUTES"
          }
        },
        "updatedAt": "2024-10-21T17:46:27.624Z"
      },
      "eventCategory": "Data"
    }
```


CloudTrail 레코드 콘텐츠에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail record contents를 참조하세요.

를 사용하여 Amazon WorkSpaces 씬 클라이언트 리소스 생성 AWS CloudFormation

Amazon WorkSpaces 씬 클라이언트는 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 AWS CloudFormation서비스인와 통합됩니다. 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 프로비저닝하고 구성합니다.

를 사용하면 템플릿을 재사용하여 WorkSpaces 씬 클라이언트 리소스를 일관되고 반복적으로 설정할 AWS CloudFormation수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝합니다.

WorkSpaces 씬 클라이언트 및 AWS CloudFormation 템플릿

WorkSpaces 씬 클라이언트 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML 형식의 텍스트 파일 형식입니다. 이러한 템플릿은 AWS CloudFormation 스택에서 프로비저닝하려는 리소스를 설명합니다. JSON 또는 YAML 형식에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 AWS CloudFormation 템플릿을 시작할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

WorkSpaces 씬 클라이언트는에서 환경 생성을 지원합니다 AWS CloudFormation. 환경용 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon WorkSpaces 씬 클라이언트 리소스 유형 참조를 참조하세요.

에 대해 자세히 알아보기 AWS CloudFormation

에 대해 자세히 알아보려면 다음 리소스를 AWS CloudFormation참조하세요.

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

인터페이스 엔드포인트(AWS PrivateLink)를 사용하여 Amazon WorkSpaces 씬 클라이언트에 액세스

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

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

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

WorkSpaces 씬 클라이언트에 대한 고려 사항

WorkSpaces 씬 클라이언트의 인터페이스 엔드포인트를 설정하려면 먼저 AWS PrivateLink 가이드의 고려 사항을 검토합니다.

WorkSpaces 씬 클라이언트에서는 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출 수행을 지원합니다.

WorkSpaces 씬 클라이언트의 인터페이스 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 WorkSpaces 씬 클라이언트에 대한 인터페이스 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 WorkSpaces 씬 클라이언트에 대한 인터페이스 엔드포인트를 생성합니다.

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

인터페이스 엔드포인트에 대해 프라이빗 DNS를 활성화하면 기본 리전 DNS 이름을 사용하여 WorkSpaces 씬 클라이언트에 API 요청을 할 수 있습니다. 예: `api.thinclient.us-east-1.amazonaws.com`.

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 액세스 권한을 부여합니다. VPC에서 WorkSpaces 씬 클라이언트에 부여된 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결합니다.

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 정책은 인터페이스 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 WorkSpaces 씬 클라이언트 작업에 부여합니다.

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

WorkSpaces 씬 클라이언트 관리자 안내서에 대한 문서 기록

다음 표에서는 WorkSpaces 씬 클라이언트 관리자 안내서의 릴리스에 대한 설명서 기록을 설명합니다.

변경 사항	설명	날짜
AWS 관리형 정책: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces 씬 클라이언트에 AmazonWorkSpacesThinClientFullAccess 관리형 정책 버전 2가 추가되었습니다.	2025년 1월 9일
AWS 관리형 정책: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 씬 클라이언트에 AmazonWorkSpacesThinClientReadOnlyAccess 관리형 정책 버전 3이 추가되었습니다.	2025년 1월 9일
AWS CloudTrail을 사용하여 Amazon WorkSpaces 씬 클라이언트 API 호출 로깅 디바이스 설정 Amazon WorkSpaces 씬 클라이언트의 저장 데이터 암호화	데이터 이벤트에 대한 새 섹션이 추가되었습니다. 디바이스 설정에 대한 새 섹션이 추가되었습니다. 저장 데이터 암호화 섹션의 KMS 정보를 업데이트했습니다.	2024년 10월 28일
비즈니스 연속성	비즈니스 연속성 및 재해 복구에 대한 새로운 섹션을 추가했습니다.	2024년 9월 6일
AWS 관리형 정책: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces 씬 클라이언트에 AmazonWorkSpacesThinClientFullAccess 관리형 정책이 추가되었습니다.	2024년 8월 9일

변경 사항	설명	날짜
AWS 관리형 정책: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 씬 클라이언트에 AmazonWorkSpacesThinClientReadOnlyAccess 관리형 정책 버전 2가 추가되었습니다.	2024년 8월 9일
WorkSpaces 씬 클라이언트에 대한 WorkSpaces Personal 구성	새 WorkSpaces Personal에 대한를 업데이트했습니다.	2024년 8월 7일
WorkSpaces 씬 클라이언트에 대한 WorkSpaces 풀 구성	새 WorkSpaces Pools에 대한 새 섹션이 추가되었습니다.	2024년 8월 7일
AWS 관리형 정책: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 씬 클라이언트에 AmazonWorkSpacesThinClientReadOnlyAccess 관리형 정책이 추가되었습니다.	2024년 7월 19일
AWS Amazon WorkSpaces 씬 클라이언트에 대한 관리형 정책	Amazon WorkSpaces 씬 클라이언트가 변경 사항 추적을 시작했습니다.	2024년 7월 19일
Amazon WorkSpaces 씬 클라이언트용 WorkSpaces 구성 Amazon WorkSpaces	운영 체제 목록을 업데이트했습니다.	2024년 2월 12일
Amazon WorkSpaces 씬 클라이언트용 AppStream 2.0 구성	자격 증명 공급자 절차가 업데이트되었습니다.	2024년 2월 12일
초기 릴리스	초기 릴리스	2023년 11월 26일

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