aws

관리 설명서

아마존 WorkSpaces 시큐어 브라우저

아마존 WorkSpaces 시큐어 브라우저: 관리 설명서

Table of Contents

Amazon WorkSpaces 보안 브라우저란 무엇입니까? 1
릴리스 이력 1
보안 브라우저 사용 시 알아두어야 할 용어 WorkSpaces 2
관련 서비스 4
아키텍처 4
WorkSpaces 보안 브라우저 액세스 5
WorkSpaces 보안 브라우저 설정 6
사용자 가입 및 생성 6
등록하십시오. AWS 계정 6
관리자 액세스 권한이 있는 사용자 생성 6
프로그래밍 방식 액세스 권한 부여 8
네트워킹 및 액세스 9
VPC 요구 사항 9
VPC 설정 권장 사항 19
지원되는 가용 영역 20
VPC 연결 22
클라이언트/사용자 연결 23
WorkSpaces 보안 브라우저 시작하기 26
1단계: 웹 포털 생성 26
네트워크 설정 구성 27
포털 설정 구성 27
사용자 설정 구성 29
ID 제공업체 구성 30
검토 및 시작 39
2단계: 웹 포털 테스트 39
3단계: 웹 포털 배포 40
다음 단계 41
웹 포털 관리 42
웹 포털 세부 정보 보기 42
웹 포털 편집 42
웹 포털 삭제 43
포털의 서비스 할당량을 관리합니다. 43
포털 증액 요청 44
최대 동시 세션 증가를 요청하세요. 45

한도 예시 ... 46
서비스 할당량 관리 ... 46
기타 서비스 할당량 ... 46
SAML IdP 토큰 재인증 간격 제어 ... 47
사용자 액세스 로깅 설정 ... 47
샘플 로그 ... 49
브라우저 정책을 설정하거나 편집합니다. ... 50
사용자 지정 브라우저 정책 설정(예시) ... 51
기본 브라우저 정책을 편집합니다. ... 57
입력 방법 편집기(IME) 구성 ... 58
세션 내 로컬라이제이션 구성 ... 59
IP 액세스 제어 설정(선택 사항) ... 62
IP 액세스 제어 그룹 생성 ... 63
IP 액세스 설정의 웹 포털 연결 ... 63
IP 액세스 제어 그룹 편집 ... 64
IP 액세스 제어 그룹 삭제 ... 64
Single Sign-On용 확장 프로그램 활성화(선택 사항) ... 64
URL 필터링 설정 ... 67
딥링크 허용 (선택 사항) ... 68
보안 ... 70
데이터 보호 ... 71
데이터 암호화 ... 71
인터네트워크 트래픽 개인 정보 보호 ... 73
사용자 액세스 로깅 ... 74
ID 및 액세스 관리 ... 74
고객 ... 74
ID를 통한 인증 ... 75
정책을 사용한 액세스 관리 ... 78
Amazon WorkSpaces 보안 브라우저의 작동 방식 IAM ... 80
자격 증명 기반 정책 예시 ... 86
AWS 관리형 정책 ... 89
문제 해결 ... 98
서비스 연결 역할 사용 ... 100
사고 대응 ... 104
규정 준수 확인 ... 104
복원력 ... 105

인프라 보안 105
구성 및 취약성 분석 106
보안 모범 사례 106
모니터링 108
를 통한 모니터링 CloudWatch 108
CloudTrail 로그 110
WorkSpaces 보안 브라우저 정보: CloudTrail 110
WorkSpaces 보안 브라우저 로그 파일 항목 이해 111
사용자 액세스 로깅 113
WorkSpaces 보안 브라우저 사용자를 위한 지침 114
브라우저 및 디바이스 호환성 114
웹 포털 액세스 114
세션 지침 115
세션 시작 115
도구 모음 사용 116
브라우저 사용 118
세션 종료 118
문제 해결 119
Single Sign-On을 위한 확장 프로그램 120
호환성 120
설치 121
문제 해결 121
사용 설명서 기록 122
..... cxxvi

Amazon WorkSpaces 보안 브라우저란 무엇입니까?

> **Note**
>
> 아마존 WorkSpaces 시큐어 브라우저는 이전에 아마존 WorkSpaces 웹으로 알려졌습니다.

Amazon WorkSpaces Secure Browser는 완전 관리형 클라우드 네이티브 호스팅 브라우저 서비스로, 일회용 컨테이너에서 사설 웹 사이트 및 software-as-a-service (SaaS) 웹 애플리케이션에 안전하게 액세스하고, 온라인 리소스와 상호 작용하고, 인터넷을 검색하는 데 사용됩니다. WorkSpaces Secure Browser는 IT 부서에 어플라이언스, 인프라, 특수 클라이언트 소프트웨어 또는 가상 사설망 (VPN) 연결을 관리하는 부담을 주지 않으면서 사용자의 기존 웹 브라우저와도 호환됩니다. 웹 콘텐츠는 사용자의 웹 브라우저로 스트리밍되는 반면 실제 브라우저와 웹 콘텐츠는 분리됩니다. AWS Amazon WorkSpaces 및 Amazon AppStream 2.0과 같은 AWS 최종 사용자 컴퓨팅 서비스를 지원하는 동일한 기반 기술을 사용함으로써 WorkSpaces Secure Browser는 기존 가상 데스크톱보다 비용 효율적이며 회사 소유 장치에 관리 소프트웨어를 제공하는 것에 비해 복잡성을 줄일 수 있습니다. WorkSpaces Secure Browser는 스트리밍 웹 콘텐츠를 통한 데이터 유출 위험을 줄여줍니다. HTML, 문서 개체 모델 (DOM) 또는 민감한 회사 데이터는 로컬 시스템으로 전송되지 않습니다. 장치, 기업 네트워크 및 인터넷을 서로 격리함으로써 브라우저 공격 표면이 사실상 제거됩니다.

모든 세션에 엔터프라이즈 브라우저 정책 (URL 허용/차단 포함) 을 적용할 수 있으며 클립보드, 파일 전송 및 프린터에 대한 세션 수준 제어를 포함합니다. IP 액세스 제어를 사용하여 신뢰할 수 있는 네트워크 또는 장치에 대한 액세스를 제한할 수도 있습니다. WorkSpaces 보안 브라우저는 설치 및 운영이 쉽습니다. 각 세션은 회사 정책 및 설정이 적용된 완전히 패치된 새로운 버전의 Chrome 브라우저로 실행됩니다.

릴리스 이력

2024년 5월 20일, 아마존 WorkSpaces 웹은 아마존 WorkSpaces 보안 브라우저로 이름이 변경되었습니다. 기존 고객의 경우 서비스를 통해 사용자 또는 리소스를 관리하는 방식에는 변화가 없었습니다. 다음 목록은 이번 이름 변경으로 인해 발생한 해당 업데이트를 설명합니다.

workspaces-web API 네임스페이스는 이전 버전과의 호환성을 위해 변경되지 않은 상태로 유지됩니다. 따라서 다음 리소스는 여전히 동일합니다.

- CLI 명령

- 아마존 CloudWatch 메트릭스. 자세한 정보는 the section called “를 통한 모니터링 CloudWatch”을 참조하세요.
- 서비스 엔드포인트. 자세한 내용은 Amazon WorkSpaces 보안 브라우저 엔드포인트 및 할당량을 참조하십시오.
- AWS CloudFormation 리소스. 자세한 내용은 Amazon WorkSpaces 보안 브라우저 리소스 유형 참조를 참조하십시오.
- 워크스페이스-웹을 포함하는 서비스 연결 역할. 자세한 정보는 the section called “서비스 연결 역할 사용”을 참조하세요.
- 워크스페이스-웹을 포함하는 콘솔 URL.
- 워크스페이스-웹을 포함하는 설명서 URL. 자세한 내용은 Amazon WorkSpaces 보안 브라우저 설명서를 참조하십시오.
- 기존 ReadOnly 관리 역할. 자세한 정보는 the section called “AWS 관리형 정책”을 참조하세요.
- KMS 권한 부여 이름.
- UAL (사용자 활동 로깅) Kinesis 스트림 접두사입니다.

또한 기존 포털 URL은 동일하게 유지됩니다. <UUID>2024년 5월 20일 이전에 생성된 포털의 URL은.workspaces-web.com 형식을 사용했습니다. WorkSpaces 보안 브라우저 포털에서는 이 형식과 workspaces-web.com 도메인을 계속 사용합니다.

보안 브라우저 사용 시 알아두어야 할 용어 WorkSpaces

WorkSpaces 보안 브라우저를 시작하는 데 도움이 되도록 다음 개념을 숙지해야 합니다.

ID 제공업체(IdP)

IdP는 사용자의 보안 인증 정보를 확인합니다. 그런 다음 인증 어설션을 발행하여 서비스 제공업체에 액세스 권한을 제공합니다. 기존 IdP가 WorkSpaces 보안 브라우저에서 작동하도록 구성할 수 있습니다.

ID 제공업체(IdP)를 구성하는 절차는 IdP에 따라 다릅니다.

서비스 제공업체 메타데이터 파일을 IdP에 업로드해야 합니다. 그렇지 않으면 사용자가 로그인할 수 없습니다. 또한 사용자에게 IdP에서 WorkSpaces 보안 브라우저를 사용할 수 있는 액세스 권한을 부여해야 합니다.

ID 제공업체(IdP) 메타데이터 문서

WorkSpaces Secure Browser에서 신뢰를 구축하려면 ID 공급자 (IdP) 의 특정 메타데이터가 필요합니다. IdP에서 다운로드한 메타데이터 교환 파일을 업로드하여 WorkSpaces Secure Browser에 이 메타데이터를 추가할 수 있습니다.

서비스 제공업체(SP)

서비스 제공업체는 인증 어설션을 수락하고 사용자에게 서비스를 제공합니다. WorkSpaces 보안 브라우저는 IdP로 인증된 사용자에게 서비스 공급자 역할을 합니다.

서비스 제공업체(SP) 메타데이터 문서

서비스 제공업체 메타데이터 세부 정보를 ID 제공업체(IdP)의 구성 인터페이스에 추가해야 합니다. 이 구성 프로세스의 세부 사항은 제공업체마다 다릅니다.

SAML 2.0

IdP와 서비스 제공업체 간에 인증 및 권한 부여 데이터를 교환하기 위한 표준입니다.

Virtual Private Cloud(VPC)

기존 또는 새 VPC, 해당 서브넷, 보안 그룹을 사용하여 콘텐츠를 Secure Browser와 연결할 수 있습니다. WorkSpaces

서브넷은 인터넷에 안정적으로 연결되어 있어야 하며, VPC와 서브넷은 사용자가 이러한 리소스에 액세스할 수 있도록 내부 및 서비스형 소프트웨어(SaaS) 웹 사이트에 안정적으로 연결되어 있어야 합니다.

나열된 VPC, 서브넷 및 보안 그룹은 Secure Browser 콘솔과 동일한 지역에서 가져온 것입니다 WorkSpaces .

신뢰할 수 있는 스토어

WorkSpaces 보안 브라우저를 통해 웹 사이트에 액세스하는 사용자가 NET: :ERR_CERT_INVALID와 같은 개인 정보 보호 오류를 수신하는 경우 해당 사이트는 사설 인증 기관 (PCA) 에서 서명한 인증서를 사용하고 있을 수 있습니다. 신뢰할 수 있는 스토어에서 PCA를 추가하거나 변경해야 할 수 있습니다. 또한 사용자 장치에서 웹 사이트를 로드하기 위해 특정 인증서를 설치해야 하는 경우 사용자가 Secure Browser에서 해당 사이트에 액세스할 수 있도록 하려면 해당 인증서를 신뢰 저장소에 추가해야 합니다. WorkSpaces

공개적으로 액세스할 수 있는 웹 사이트는 일반적으로 신뢰할 수 있는 스토어를 변경할 필요가 없습니다.

웹 포털

웹 포털을 통해 사용자는 브라우저에서 내부 및 SaaS 웹 사이트에 액세스할 수 있습니다. 계정별로 지원되는 모든 리전에 하나의 웹 포털을 생성할 수 있습니다. 두 개 이상의 포털에 대한 한도 증가를 요청하려면 지원팀에 문의하십시오.

웹 포털 엔드포인트

웹 포털 엔드포인트는 사용자가 포털에 구성된 ID 제공업체로 로그인한 후 웹 포털을 시작하는 액세스 포인트입니다.

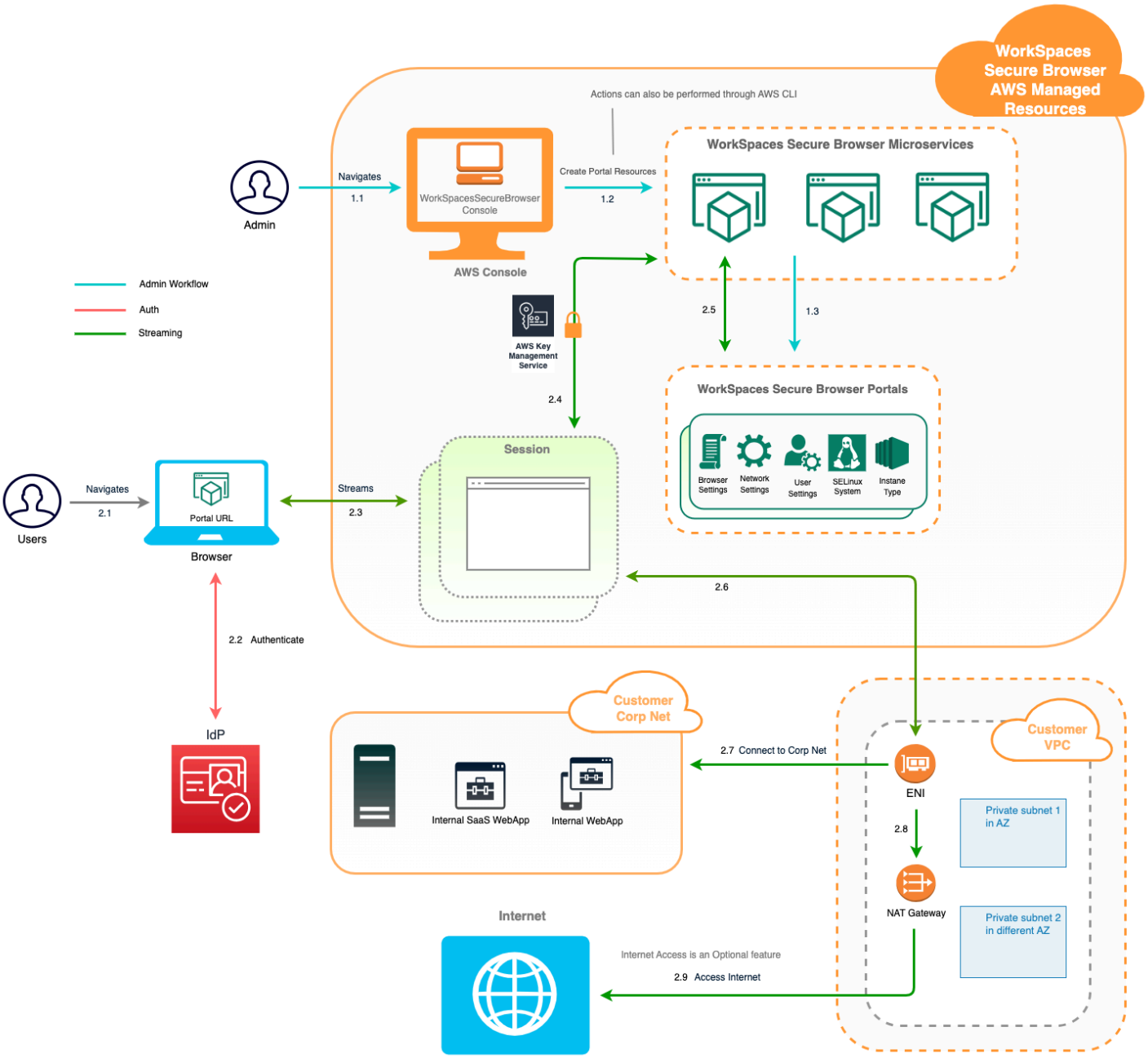
엔드포인트는 인터넷에서 공개적으로 사용할 수 있으며 네트워크에 내장할 수 있습니다.

관련 서비스

WorkSpaces 보안 브라우저는 AWS 최종 사용자 컴퓨팅 포트폴리오의 WorkSpaces Amazon에서 제공하는 기능입니다. WorkSpaces 및 AppStream 2.0과 비교하여 WorkSpaces 보안 브라우저는 안전한 웹 기반 워크로드를 지원하도록 특별히 구축되었습니다. WorkSpaces Secure Browser는 AWS에서 필요에 따라 용량, 크기 조정 및 이미지를 프로비저닝하고 업데이트하여 자동으로 관리됩니다. 예를 들어 데스크톱 리소스에 액세스해야 하는 소프트웨어 개발자에게는 영구 Workspace Desktop을 제공하고 데스크톱 컴퓨터의 일부 내부 및 SaaS 웹 사이트 (네트워크 외부에 호스팅된 웹 사이트 포함) 에만 액세스해야 하는 컨택 센터 사용자에게는 WorkSpaces Secure Browser를 제공하도록 선택할 수 있습니다.

아키텍처

다음 다이어그램은 WorkSpaces 보안 브라우저의 아키텍처를 보여줍니다.



WorkSpaces 보안 브라우저 액세스

관리자는 WorkSpaces WorkSpaces 보안 브라우저 콘솔, SDK, CLI 또는 API를 통해 보안 브라우저에 액세스합니다. 사용자는 WorkSpaces 보안 브라우저 엔드포인트를 통해 액세스합니다.

WorkSpaces 보안 브라우저 설정

내부 웹 사이트 및 SaaS 애플리케이션에 연결되도록 WorkSpaces Secure Browser를 구성하려면 먼저 다음 사전 요구 사항을 완료해야 합니다.

주제

- 사용자 가입 및 생성
- 프로그래밍 방식 액세스 권한 부여
- 네트워킹 및 액세스

사용자 가입 및 생성

등록하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

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

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 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.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

프로그래밍 방식 액세스 권한 부여

사용자가 AWS 외부 사용자와 상호 작용하려는 경우 프로그래밍 방식의 액세스가 필요합니다. AWS Management Console프로그래밍 방식의 액세스 권한을 부여하는 방법은 액세스하는 사용자 유형에 따라 다릅니다. AWS

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAM Identity Center가 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • AWS CLI 에 대한 내용은 사용 설명서의 AWS CLI사용을 AWS IAM Identity Center위한 구성을 참조하십시오.AWS Command Line Interface • AWS SDK, 도구 및 AWS API의 경우 AWS SDK 및 도구 참조 안내서의 IAM ID 센터 인증을 참조하십시오.
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 방식 요청에 서명할 수 있습니다. AWS	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따르십시오.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 에 대한 내용은 사용 설명서의 IAM 사용자 자격 증명을 사용한 인증을 참조하십시오. AWS CLIAWS Command Line Interface

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		• AWS SDK 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용한 인증을 참조하십시오.AWS • AWS API의 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하십시오.

네트워킹 및 액세스

다음 항목에서는 사용자가 연결할 수 있도록 WorkSpaces Secure Browser 스트리밍 인스턴스를 설정하는 방법을 설명합니다. 또한 WorkSpaces Secure Browser 스트리밍 인스턴스가 인터넷뿐 아니라 VPC 리소스에 액세스할 수 있도록 하는 방법도 설명합니다.

주제

- VPC 요구 사항
- VPC 설정 권장 사항
- 지원되는 가용 영역
- VPC 연결
- 클라이언트/사용자 연결

VPC 요구 사항

WorkSpaces 보안 브라우저 포털을 생성할 때 계정에서 VPC를 선택합니다. 서로 다른 두 개의 가용 영역에서 두 개 이상의 서브넷이 있어야 합니다. VPC 및 서브넷은 다음과 같은 요구 사항을 충족해야 합니다.

- VPC는 기본 테넌시를 가지고 있어야 합니다. 전용 테넌시가 있는 VPC는 지원되지 않습니다.
- 가용성 고려 시에는 서로 다른 두 개의 가용 영역에 생성된 둘 이상의 서브넷이 필요합니다. 서브넷에는 예상 WorkSpaces 보안 브라우저 트래픽을 지원할 수 있는 충분한 IP 주소가 있어야 합니다. 최대 동시 세션 수를 수용하기에 적합한 클라이언트 IP 주소를 허용하는 서브넷 마스크를 사용하여 각 서브넷을 구성합니다. 자세한 정보는 새 VPC 생성 및 구성을 참조하세요.

- 모든 서브넷은 사용자가 WorkSpaces Secure Browser를 통해 액세스할 수 있는 내부 콘텐츠 (사내 AWS 클라우드 또는 온프레미스) 에 안정적으로 연결되어 있어야 합니다.

가용성 및 규모 조정 여부를 고려하여 서로 다른 가용 영역에서 세 개의 서브넷을 선택하는 것이 좋습니다. 자세한 정보는 새 VPC 생성 및 구성을 참조하세요.

WorkSpaces Secure Browser는 인터넷 액세스를 가능하게 하기 위해 스트리밍 인스턴스에 퍼블릭 IP 주소를 할당하지 않습니다. 퍼블릭 IP 주소는 인터넷에서 스트리밍 인스턴스에 액세스할 수 있게 합니다. 따라서 퍼블릭 서브넷에 연결된 스트리밍 인스턴스는 인터넷에 액세스할 수 없습니다. WorkSpaces Secure Browser 포털에서 퍼블릭 인터넷 콘텐츠와 프라이빗 VPC 콘텐츠 모두에 액세스할 수 있게 하려면 의 단계를 완료하세요. 무제한 인터넷 브라우징 활성화(권장)

새 VPC 생성 및 구성

이 섹션에서는 VPC 마법사를 사용하여 퍼블릭 서브넷 하나와 프라이빗 서브넷 하나가 있는 VPC를 생성하는 방법에 대해 설명합니다. 이 프로세스의 일부로 마법사는 인터넷 게이트웨이와 NAT 게이트웨이를 생성합니다. 이는 퍼블릭 서브넷과 연결된 사용자 지정 라우팅 테이블도 생성합니다. 그런 다음 프라이빗 서브넷과 연결된 기본 라우팅 테이블을 업데이트합니다. NAT 게이트웨이는 VPC의 퍼블릭 서브넷에서 자동으로 생성됩니다.

마법사를 사용하여 VPC 구성을 생성한 후 두 번째 프라이빗 서브넷을 추가합니다. 이 구성에 대한 자세한 내용은 퍼블릭 및 프라이빗 서브넷이 있는 VPC(NAT)를 참조하십시오.

1단계: 탄력적 IP 주소 할당

VPC를 생성하기 전에 WorkSpaces 보안 브라우저 지역에 엘라스틱 IP 주소를 할당해야 합니다. 할당이 완료되면 탄력적 IP 주소를 NAT 게이트웨이와 연결할 수 있습니다. 탄력적 IP 주소로 VPC의 다른 스트리밍 인스턴스에 주소를 신속하게 다시 매핑하여 스트리밍 인스턴스의 오류를 숨길 수 있습니다. 자세한 내용은 탄력적인 IP 주소 섹션을 참조하십시오.

> **Note**
>
> 사용하는 탄력적인 IP 주소에 요금이 부과될 수 있습니다. 자세한 내용은 탄력적 IP 주소 요금을 참조하십시오.

탄력적 IP 주소가 없는 경우에는 다음 단계를 완료합니다. 기존 탄력적 IP 주소를 사용하려면 해당 주소가 다른 인스턴스 또는 네트워크 인터페이스와 현재 연결되어 있지 않은지 먼저 확인해야 합니다.

탄력적 IP 주소 할당

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 [Network & Security]에서 [Elastic IPs]를 선택합니다.
3. 새 주소 할당을 선택한 다음 할당을 선택합니다.
4. 콘솔에 표시된 탄력적 IP 주소를 기록해 둡니다.
5. 탄력적 IP 창의 오른쪽 위에서 × 아이콘을 클릭하여 창을 닫습니다.

2단계: 새 VPC 생성

퍼블릭 서브넷 하나와 프라이빗 서브넷 하나가 있는 새 VPC를 생성하려면 다음 단계를 수행합니다.

새 VPC 생성

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 [VPC Dashboard]를 선택합니다.
3. VPC 마법사 시작을 선택합니다.
4. 1단계: VPC 구성 선택에서 퍼블릭 및 프라이빗 서브넷이 있는 VPC를 선택한 후 선택을 선택합니다.
5. 2단계: 퍼블릭 및 프라이빗 서브넷이 있는 VPC에서 다음과 같이 VPC를 구성합니다.
   - IPv4 CIDR 블록에 VPC의 IPv4 CIDR 블록을 지정합니다.
   - IPv6 CIDR 블록은 기본값인 IPv6 CIDR 블록 없음을 유지합니다.
   - VPC 이름에 VPC의 고유 이름을 입력합니다.
   - 다음과 같이 퍼블릭 서브넷을 구성합니다.
     - 퍼블릭 서브넷의 IPv4 CIDR에 서브넷의 CIDR 블록을 지정합니다.
     - 가용 영역은 기본값인 기본 설정 없음을 유지합니다.
     - 퍼블릭 서브넷 이름에 서브넷의 이름을 입력합니다. 예를 들어 **`WorkSpaces Secure Browser Public Subnet`**입니다.
   - 다음과 같이 첫 번째 프라이빗 서브넷을 구성합니다.
     - 프라이빗 서브넷의 IPv4 CIDR에 서브넷의 CIDR 블록을 지정합니다. 지정한 값을 기록해 둡니다.
     - 가용 영역에서 특정 영역을 선택하고 선택한 영역을 기록해 둡니다.

- 프라이빗 서브넷 이름에 서브넷의 이름을 입력합니다. 예를 들어 **WorkSpaces Secure Browser Private Subnet1**입니다.

- 나머지 필드는 기본값을 유지합니다(해당할 경우).
- 생성한 탄력적 IP 주소에 해당하는 값을 탄력적 IP 할당 ID에서 선택합니다. 이 주소가 NAT 게이트웨이에 할당됩니다. 탄력적 IP 주소가 없으면 https://console.aws.amazon.com/vpc/의 Amazon VPC 콘솔을 사용하여 주소를 생성합니다.
- 환경에 Amazon S3 엔드포인트가 필요한 경우에는 서비스 엔드포인트에서 하나를 지정합니다.

  Amazon S3 엔드포인트를 지정하려면 다음을 수행합니다.

  1. 엔드포인트 추가를 선택합니다.
  2. 서비스에서 com.amazonaws를 선택합니다. .s3 **##** 항목. 여기서 ### VPC를 AWS 리전 생성하려는 위치입니다.
  3. 서브넷의 경우 프라이빗 서브넷을 선택합니다.
  4. 정책은 기본값인 모든 액세스를 유지합니다.
- DNS 호스트 이름 활성화는 기본값인 예를 유지합니다.
- 하드웨어 테넌시는 기본값인 기본값을 유지합니다.
- VPC 생성을 선택합니다.
- VPC를 설정하는 데 몇 분 정도 걸립니다. VPC가 생성되면 [OK]를 선택합니다.

3단계: 두 번째 프라이빗 서브넷 추가

이전 단계에서는 퍼블릭 서브넷 하나와 프라이빗 서브넷 하나를 포함하는 VPC를 생성했습니다. 다음 단계를 완료하여 두 번째 프라이빗 서브넷을 VPC에 추가합니다. 두 번째 프라이빗 서브넷은 첫 번째 프라이빗 서브넷과 다른 가용 영역에 추가하는 것이 좋습니다.

두 번째 프라이빗 서브넷 추가

1. 탐색 창에서 서브넷을 선택합니다.
2. 이전 단계에서 생성한 첫 번째 프라이빗 서브넷을 선택합니다. 서브넷 목록 아래에 있는 설명 탭에서 이 서브넷의 가용 영역을 기록해 둡니다.
3. 서브넷 창의 왼쪽 위에서 서브넷 생성을 선택합니다.
4. 이름 태그에 프라이빗 서브넷의 이름을 입력합니다. 예를 들어 **WorkSpaces Secure Browser Private Subnet2**입니다.
5. VPC에서 이전 단계에서 생성한 VPC를 선택합니다.

6. 가용 영역에서 첫 번째 프라이빗 서브넷에 사용 중인 것이 아닌 다른 가용 영역을 선택합니다. 다른 가용 영역을 선택하면 내결함성이 향상되고 용량 부족 오류를 방지할 수 있습니다.
7. IPv4 CIDR 블록에 새 서브넷의 고유한 CIDR 블록 범위를 지정합니다. 예를 들어 첫 번째 프라이빗 서브넷의 IPv4 CIDR 블록 범위가 **10.0.1.0/24**인 경우 두 번째 프라이빗 서브넷은 CIDR 블록 범위를 **10.0.2.0/24**로 지정할 수 있습니다.
8. 생성을 선택합니다.
9. 서브넷이 생성되면 닫기를 선택합니다.

4단계: 서브넷 라우팅 테이블 확인 및 이름 지정

VPC를 생성 및 구성한 후 다음 단계를 완료하여 라우팅 테이블의 이름을 지정합니다. 다음 세부 정보가 라우팅 테이블에 맞는지 확인해야 합니다.

- NAT 게이트웨이가 상주하는 서브넷과 연결된 라우팅 테이블에는 인터넷 트래픽을 인터넷 게이트웨이로 가리키는 라우팅이 포함되어 있어야 합니다. 그러면 NAT 게이트웨이가 인터넷에 액세스할 수 있습니다.
- 프라이빗 서브넷과 연결된 라우팅 테이블은 인터넷 트래픽을 NAT 게이트웨이로 가리키도록 구성되어야 합니다. 그러면 프라이빗 서브넷의 스트리밍 인스턴스가 인터넷과 통신할 수 있습니다.

서브넷 라우팅 테이블 확인 및 이름 지정

1. 탐색 창에서 서브넷을 선택한 후 생성한 퍼블릭 서브넷을 선택합니다. 예: WorkSpaces 시큐어 브라우저 2.0 퍼블릭 서브넷.
2. 라우팅 테이블 탭에서 라우팅 테이블의 ID를 선택합니다. rtb-12345678을 예로 들 수 있습니다.
3. 라우팅 테이블을 선택합니다. 이름에서 편집(연필) 아이콘을 선택하고 테이블 이름을 입력합니다. 예를 들어, **workspacesweb-public-routetable**을 이름으로 입력할 수 있습니다. 확인 표시를 선택하여 이름을 저장합니다.
4. 퍼블릭 라우팅 테이블이 선택된 상태에서, 경로 탭에서 로컬 트래픽용 경로 하나와 다른 모든 트래픽을 VPC의 인터넷 게이트웨이로 전송하는 또 하나의 경로가 있는지 확인합니다. 다음 표는 이들 두 경로에 대해 설명합니다.

대상 주소	대상	설명
퍼블릭 서브넷 IPv4 CIDR 블록(예: 10.0.0.0/20)	로컬	퍼블릭 서브넷 IPv4 CIDR 블록의 IPv4 주소로 향하는 리

대상 주소	대상	설명
		소스의 모든 트래픽입니다. 이 트래픽은 VPC 내에서 로컬로 라우팅됩니다.
다른 모든 IPv4 주소로 향하는 트래픽(예: 0.0.0.0/0)	아웃바운드(igw-ID)	다른 모든 IPv4 주소로 향하는 트래픽은 VPC 마법사에서 생성한 인터넷 게이트웨이(igw-ID로 식별됨)로 라우팅됩니다.

5. 탐색 창에서 서브넷을 선택합니다. 그런 다음 생성한 첫 번째 프라이빗 서브넷(예: **`WorkSpaces Secure Browser Private Subnet1`**)을 선택합니다.
6. 라우팅 테이블 탭에서 라우팅 테이블의 ID를 선택합니다.
7. 라우팅 테이블을 선택합니다. 이름에서 편집(연필) 아이콘을 선택하고 테이블 이름을 입력합니다. 예를 들어, **`workspacesweb-private-routetable`**을 이름으로 입력할 수 있습니다. 이름을 저장하려면 확인 표시를 선택합니다.
8. 경로 탭에서 라우팅 테이블에 다음 라우팅이 포함되어 있는지 확인합니다.

대상 주소	대상	설명
퍼블릭 서브넷 IPv4 CIDR 블록(예: 10.0.0/20)	로컬	퍼블릭 서브넷 IPv4 CIDR 블록의 IPv4 주소로 향하는 리소스의 모든 트래픽은 VPC 내에서 로컬로 라우팅됩니다.
다른 모든 IPv4 주소로 향하는 트래픽(예: 0.0.0.0/0)	아웃바운드(nat-ID)	다른 모든 IPv4 주소로 향하는 트래픽은 NAT 게이트웨이(nat-ID로 식별됨)로 라우팅됩니다.
S3 버킷으로 향하는 트래픽(S3 엔드포인트를 지정한 경우 해당)[pl-ID (com.amazonaws.region.s3)]	스토리지(vpce-ID)	S3 버킷으로 향하는 트래픽은 S3 엔드포인트(vpce-ID로 식별됨)로 라우팅됩니다.

9. 탐색 창에서 서브넷을 선택합니다. 그런 다음 생성한 두 번째 프라이빗 서브넷(예: **WorkSpaces Secure Browser Private Subnet2**)을 선택합니다.
10. 라우팅 테이블 탭에서 선택된 라우팅 테이블이 프라이빗 라우팅 테이블(예: **workspacesweb-private-routetable**)인지 확인합니다. 라우팅 테이블이 다르다면 편집을 선택하고 프라이빗 라우팅 테이블을 대신 선택합니다.

무제한 인터넷 브라우징 활성화(권장)

아래 단계에 따라 무제한 인터넷 브라우징이 가능한 NAT 게이트웨이가 있는 VPC를 구성합니다. 이렇게 하면 WorkSpaces Secure Browser가 퍼블릭 인터넷상의 사이트와 VPC에서 호스팅되거나 VPC에 연결된 프라이빗 사이트에 액세스할 수 있습니다.

무제한 인터넷 브라우징이 가능한 NAT 게이트웨이가 있는 VPC 구성

WorkSpaces Secure Browser 포털에서 퍼블릭 인터넷 콘텐츠와 프라이빗 VPC 콘텐츠 모두에 액세스할 수 있게 하려면 다음 단계를 따르세요.

> **Note**
>
> VPC를 이미 구성한 경우 다음 단계를 완료하여 VPC에 NAT 게이트웨이를 추가합니다. 새 VPC를 생성해야 하는 경우 새 VPC 생성 및 구성 섹션을 참조하십시오.

1. NAT 게이트웨이를 생성하려면 NAT 게이트웨이 만들기 단계를 완료합니다. 이 NAT 게이트웨이가 퍼블릭 연결이 가능하고 VPC의 퍼블릭 서브넷에 있는지 확인합니다.
2. 서로 다른 가용 영역에서 두 개 이상의 서브넷을 지정해야 합니다. 서브넷을 서로 다른 가용 영역에 할당하면 가용성과 내결함성을 높일 수 있습니다. 두 번째 프라이빗 서브넷을 만드는 방법에 대한 자세한 내용은 the section called “3단계: 두 번째 프라이빗 서브넷 추가” 섹션을 참조하십시오.

   > **Note**
   >
   > 모든 스트리밍 인스턴스가 인터넷에 액세스할 수 있도록 하려면 퍼블릭 서브넷을 WorkSpaces Secure Browser 포털에 연결하지 마십시오.

3. 인터넷 바운드 트래픽을 NAT 게이트웨이로 가리키도록 프라이빗 서브넷과 연결된 라우팅 테이블을 업데이트합니다. 그러면 프라이빗 서브넷의 스트리밍 인스턴스가 인터넷과 통신할 수 있습니다. 라우팅 테이블을 프라이빗 서브넷과 연결하는 방법에 대한 자세한 내용은 라우팅 테이블 구성 단계를 확인합니다.

제한된 인터넷 브라우징 활성화 (아웃바운드 HTTP 프록시 사용)

WorkSpaces Secure Browser 포털의 권장 네트워크 설정은 NAT 게이트웨이가 있는 프라이빗 서브넷을 사용하여 포털에서 퍼블릭 인터넷과 프라이빗 콘텐츠를 모두 탐색할 수 있도록 하는 것입니다. 자세한 정보는 the section called “무제한 인터넷 브라우징 활성화(권장)”을 참조하세요. 하지만 웹 프록시를 사용하여 WorkSpaces Secure Browser 포털에서 인터넷으로의 아웃바운드 통신을 제어해야 할 수도 있습니다. 예를 들어 웹 프록시를 인터넷 게이트웨이로 사용하는 경우 도메인 허용 목록 및 콘텐츠 필터링과 같은 예방적 보안 제어를 구현할 수 있습니다. 또한 웹 페이지 또는 소프트웨어 업데이트와 같이 자주 액세스하는 리소스를 로컬에 캐싱하여 대역폭 사용량을 줄이고 네트워크 성능을 개선할 수 있습니다. 일부 사용 사례의 경우 웹 프록시를 통해서만 액세스할 수 있는 비공개 콘텐츠가 있을 수 있습니다.

관리 대상 기기 또는 가상 환경 이미지에서 프록시 설정을 구성하는 방법에 이미 익숙할 수 있습니다. 하지만 디바이스를 제어할 수 없는 경우 (예: 기업에서 소유하거나 관리하지 않는 디바이스를 사용자가 사용하는 경우) 또는 가상 환경에 맞게 이미지를 관리해야 하는 경우 문제가 발생할 수 있습니다. WorkSpaces 보안 브라우저를 사용하면 웹 브라우저에 내장된 Chrome의 정책을 사용하여 프록시 설정을 지정할 수 있습니다. WorkSpaces 보안 브라우저용 HTTP 아웃바운드 프록시를 설정하여 이 작업을 수행할 수 있습니다.

이 솔루션은 권장 아웃바운드 VPC 프록시 설정을 기반으로 합니다. 프록시 솔루션은 오픈 소스 HTTP 프록시 Squid를 기반으로 합니다. 그런 다음 WorkSpaces 보안 브라우저 설정을 사용하여 프록시 엔드포인트에 연결하도록 WorkSpaces 보안 브라우저 포털을 구성합니다. 자세한 내용은 도메인 화이트리스트 및 콘텐츠 필터링을 사용하여 아웃바운드 VPC 프록시를 설정하는 방법을 참조하십시오.

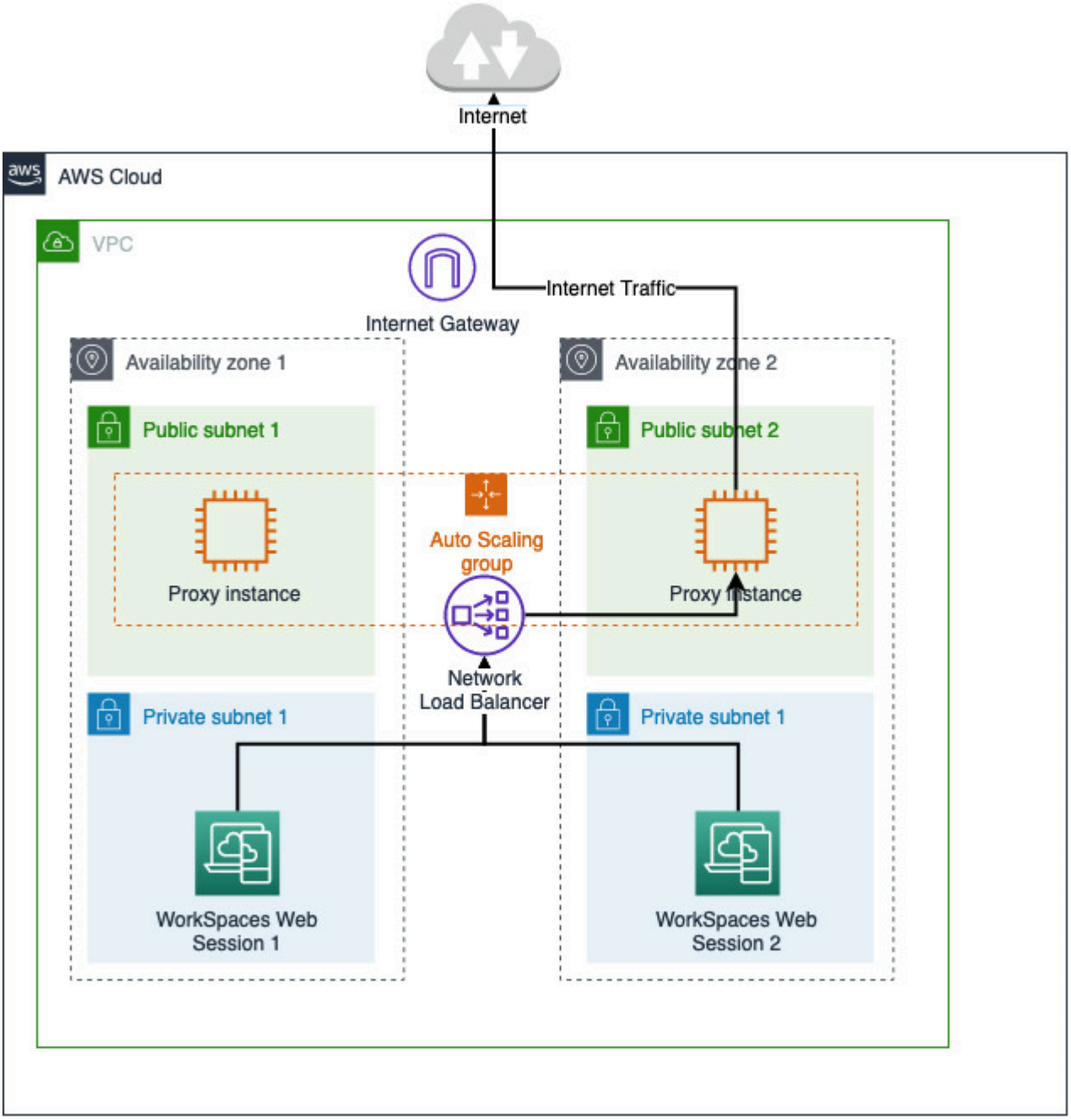
이 솔루션은 다음과 같은 이점을 제공합니다.

- 네트워크 로드 밸런서에서 호스팅하는 자동 크기 조정 Amazon EC2 인스턴스 그룹을 포함하는 아웃바운드 프록시입니다. 프록시 인스턴스는 퍼블릭 서브넷에 있으며, 각 인스턴스는 엘라스틱 IP로 연결되어 있어 인터넷에 액세스할 수 있습니다.
- 프라이빗 서브넷에 배포되는 WorkSpaces 보안 브라우저 포털. 인터넷 액세스를 활성화하도록 NAT 게이트웨이를 구성할 필요는 없습니다. 대신 모든 인터넷 트래픽이 아웃바운드 프록시를 통과하도록 브라우저 정책을 구성합니다. 자체 프록시를 사용하려는 경우 WorkSpaces Secure Browser 포털 설정도 비슷합니다.

아키텍처

다음은 VPC의 일반적인 프록시 설정 예제입니다. 프록시 Amazon EC2 인스턴스는 퍼블릭 서브넷에 있으며 Elastic IP와 연결되어 있으므로 인터넷에 액세스할 수 있습니다. 네트워크 로드 밸런서는 프록

시 인스턴스의 Auto Scaling 그룹을 호스팅합니다. 이렇게 하면 프록시 인스턴스가 자동으로 확장되고 네트워크 로드 밸런서가 단일 프록시 엔드포인트가 되어 WorkSpaces Secure Browser 세션에서 사용할 수 있습니다.



사전 조건

시작하기 전에 다음 사전 요구 사항을 충족하는지 확인하세요.

- 퍼블릭 및 프라이빗 서브넷이 여러 가용 영역 (AZ) 에 분산되어 있는 이미 배포된 VPC가 필요합니다. VPC 환경을 설정하는 방법에 대한 자세한 내용은 기본 VPC를 참조하십시오.

- WorkSpaces Secure Browser 세션이 있는 프라이빗 서브넷에서 액세스할 수 있는 단일 프록시 엔드포인트 (예: 네트워크 로드 밸런서 DNS 이름) 가 필요합니다. 기존 프록시를 사용하려면 프라이빗 서브넷에서 액세스할 수 있는 단일 엔드포인트도 있어야 합니다.

보안 브라우저용 WorkSpaces HTTP 아웃바운드 프록시를 설정합니다.

WorkSpaces 보안 브라우저용 HTTP 아웃바운드 프록시를 설정하려면 다음 단계를 따르십시오.

1. 예제 아웃바운드 프록시를 VPC에 배포하려면 도메인 화이트리스트 및 콘텐츠 필터링을 사용하여 아웃바운드 VPC 프록시를 설정하는 방법의 단계를 따르십시오.
   a. “설치 (일회성 설정)" 의 단계에 따라 템플릿을 계정에 배포하십시오. CloudFormation 템플릿 매개변수로 적합한 VPC와 서브넷을 CloudFormation 선택해야 합니다.
   b. 배포 후에는 CloudFormation 출력 파라미터 OutboundProxy도메인 및 OutboundProxy 포트를 찾으세요. 프록시의 DNS 이름 및 포트입니다.
   c. 이미 자체 프록시가 있는 경우 이 단계를 건너뛰고 프록시의 DNS 이름과 포트를 사용하세요.
2. WorkSpaces 보안 브라우저 콘솔에서 포털을 선택한 다음 편집을 선택합니다.
   a. 네트워크 연결 세부 정보에서 프록시에 액세스할 수 있는 VPC와 프라이빗 서브넷을 선택합니다.
   b. 정책 설정에서 JSON 편집기를 사용하여 다음 ProxySettings 정책을 추가합니다. `ProxyServer`필드는 프록시의 DNS 이름 및 포트여야 합니다. ProxySettings 정책에 대한 자세한 내용은 을 참조하십시오 ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. WorkSpaces 보안 브라우저 세션에서 Chrome에 프록시가 적용된 것을 확인할 수 있습니다. Chrome은 관리자의 프록시 설정을 사용하고 있습니다.

4. chrome: //policy 및 Chrome 정책 탭으로 이동하여 정책이 적용되었는지 확인합니다.
5. WorkSpaces 보안 브라우저 세션이 NAT 게이트웨이 없이 인터넷 콘텐츠를 성공적으로 탐색할 수 있는지 확인하십시오. CloudWatch 로그에서 Squid 프록시 액세스 로그가 기록되어 있는지 확인합니다.

문제 해결

Chrome 정책이 적용된 후에도 WorkSpaces 보안 브라우저 세션에서 여전히 인터넷에 액세스할 수 없는 경우 다음 단계에 따라 문제를 해결해 보세요.

- WorkSpaces Secure Browser 포털이 있는 프라이빗 서브넷에서 프록시 엔드포인트에 액세스할 수 있는지 확인하세요. 이렇게 하려면 프라이빗 서브넷에 EC2 인스턴스를 만들고 프라이빗 EC2 인스턴스에서 프록시 엔드포인트로의 연결을 테스트하십시오.
- 프록시가 인터넷에 액세스할 수 있는지 확인하십시오.
- Chrome 정책이 올바른지 확인하세요.
  - 정책 `ProxyServer` 필드의 다음 형식을 확인하세요`<Proxy DNS name>:<Proxy port>`. 접두사에는 `http://` `https://` OR가 없어야 합니다.
  - WorkSpaces 보안 브라우저 세션에서 Chrome을 사용하여 chrome: //policy로 이동하여 정책이 성공적으로 ProxySettings 적용되었는지 확인합니다.

VPC 설정 권장 사항

다음 권장 사항은 VPC를 보다 효과적이고 안전하게 구성하는 데 도움이 될 수 있습니다.

전체 VPC 구성

- VPC 구성이 규모 조정 요구 사항을 지원할 수 있는지 확인합니다.
- WorkSpaces 보안 브라우저 서비스 할당량 (한도라고도 함) 이 예상 수요를 충분히 지원할 수 있는지 확인하세요. 할당량 증가를 요청하려면 https://console.aws.amazon.com/servicequotas/에서 서비스 할당량 콘솔을 사용합니다. 기본 WorkSpaces 보안 브라우저 할당량에 대한 자세한 내용은 을 참조하십시오. the section called “포털의 서비스 할당량을 관리합니다.”
- 스트리밍 세션에 인터넷 액세스를 제공하려는 경우 퍼블릭 서브넷에 NAT 게이트웨이가 있는 VPC를 구성하는 것이 좋습니다.

탄력적 네트워크 인터페이스

- 스트리밍 기간 동안 각 WorkSpaces Secure Browser 세션에는 자체 Elastic Network 인터페이스가 필요합니다. WorkSpaces Secure Browser는 플릿의 최대 용량만큼 엘라스틱 네트워크 인터페이스 (ENI) 를 생성합니다. 기본적으로 리전당 ENI 한도는 5,000입니다. 자세한 정보는 네트워크 인터페이스를 참조하십시오.

  수천 개의 동시 스트리밍 세션과 같은 대규모 배포의 용량을 계획할 때는 최대 사용량에 필요할 수 있는 ENI의 수를 고려합니다. ENI 한도는 웹 포털에 구성한 최대 동시 사용량 한도 이상으로 유지하는 것이 좋습니다.

서브넷

- 사용자를 확장하기 위한 계획을 세울 때는 각 WorkSpaces Secure Browser 세션마다 구성된 서브넷의 고유한 클라이언트 IP 주소가 필요하다는 점을 염두에 두십시오. 따라서 서브넷에 구성된 클라이언트 IP 주소 스페이스의 크기에 따라 동시에 스트리밍할 수 있는 사용자 수가 결정됩니다.
- 예상되는 최대 동시 사용자 수를 수용하기에 적합한 클라이언트 IP 주소를 허용하는 서브넷 마스크를 사용하여 각 프라이빗 서브넷을 구성하는 것이 좋습니다. 또한 예상 증가율을 고려하여 IP 주소의 추가를 고려할 수도 있습니다. 자세한 내용은 IPv4의 VPC 및 서브넷 규모 조정을 참조하십시오.
- 가용성 및 규모 조정을 고려하여 원하는 지역에서 WorkSpaces Secure Browser가 지원하는 고유한 가용 영역 각각에 서브넷을 구성하는 것이 좋습니다. 자세한 정보는 the section called “새 VPC 생성 및 구성”을 참조하세요.
- 서브넷을 통해 웹 애플리케이션에 필요한 네트워크 리소스에 액세스할 수 있는지 확인합니다.

보안 그룹

- 보안 그룹을 사용하여 VPC에 대한 추가 액세스 제어를 제공합니다.

  VPC에 속하는 보안 그룹을 사용하면 웹 애플리케이션에 필요한 WorkSpaces Secure Browser 스트리밍 인스턴스와 네트워크 리소스 간의 네트워크 트래픽을 제어할 수 있습니다. 보안 그룹은 웹 애플리케이션에 필요한 네트워크 리소스에 대한 액세스를 제공해야 합니다.

지원되는 가용 영역

WorkSpaces Secure Browser와 함께 사용할 가상 사설 클라우드 (VPC) 를 생성할 때 VPC의 서브넷은 보안 브라우저를 시작하는 지역의 서로 다른 가용 영역에 있어야 합니다. WorkSpaces 각 가용 영역은 다른 가용 영역에서 발생한 장애를 격리시킬 수 있도록 서로 분리된 공간이어야 합니다. 별도의 가용 영역에서 인스턴스를 시작함으로써 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수

있습니다. 각 서브넷은 단일 가용 영역 내에서만 존재해야 하며, 여러 영역으로 스케일 아웃할 수 없습니다. 복원력을 극대화하려면 원하는 리전에서 지원되는 각 AZ에 대해 서브넷을 구성하는 것이 좋습니다.

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

계정에 대해 가용 영역을 조정하려면 가용 영역에 대한 고유하고 일관된 식별자인 AZ ID를 사용해야 합니다. 예를 들어, use1-az2 는 us-east-1 해당 지역의 AZ ID이며 모든 계정에서 동일한 위치를 가집니다. AWS

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

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

지역명	리전 코드	지원되는 AZ ID
미국 동부(버지니아 북부)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
미국 서부(오리건)	us-west-2	usw2-az1, usw2-az2, usw2-az3
아시아 태평양(뭄바이)	ap-south-1	aps1-az1, aps1-az3
아시아 태평양(서울)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
아시아 태평양(싱가포르)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
아시아 태평양(시드니)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3

지역명	리전 코드	지원되는 AZ ID
아시아 태평양(도쿄)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
캐나다(중부)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
유럽(프랑크푸르트)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
유럽(아일랜드)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
유럽(런던)	eu-west-2	euw2-az1, euw2-az2

가용 영역 및 AZ ID에 대한 자세한 내용은 Amazon EC2 사용 설명서의 지역, 가용 영역 및 로컬 영역을 참조하십시오.

VPC 연결

각 WorkSpaces Secure Browser 스트리밍 인스턴스에는 VPC 내 리소스뿐만 아니라 NAT 게이트웨이가 있는 프라이빗 서브넷이 설정된 경우 인터넷에도 연결할 수 있는 고객 네트워크 인터페이스가 있습니다.

인터넷 연결을 위해 모든 대상에 대해 다음 포트가 열려 있어야 합니다. 수정된 보안 그룹 또는 사용자 지정 보안 그룹을 사용하는 경우에는 필요한 규칙을 수동으로 추가해야 합니다. 자세한 내용은 보안 그룹 규칙을 참조하십시오.

> **Note**
>
> 이는 송신 트래픽에도 적용됩니다.

- TCP 80(HTTP)
- TCP 443(HTTPS)
- UDP 8433

클라이언트/사용자 연결

WorkSpaces Secure Browser는 퍼블릭 인터넷을 통해 스트리밍 연결을 라우팅하도록 구성되어 있습니다. 사용자를 인증하고 WorkSpaces Secure Browser가 작동하는 데 필요한 웹 자산을 제공하려면 인터넷 연결이 필요합니다. 이러한 트래픽을 허용하려면 허용된 도메인 섹션에 나열된 도메인을 허용해야 합니다.

다음 항목에서는 WorkSpaces Secure Browser에 대한 사용자 연결을 활성화하는 방법에 대한 정보를 제공합니다.

주제

- IP 주소 및 포트 요구 사항
- 허용된 도메인

IP 주소 및 포트 요구 사항

WorkSpaces Secure Browser 인스턴스에 액세스하려면 사용자 장치가 다음 포트를 통한 아웃바운드 액세스가 필요합니다.

- 포트 443(TCP)
  - 포트 443은 인터넷 엔드포인트를 사용할 때 사용자의 디바이스와 스트리밍 인스턴스 간의 HTTPS 통신에 사용됩니다. 일반적으로 최종 사용자가 스트리밍 세션 도중 웹을 탐색할 때 웹 브라우저는 트래픽 스트리밍을 위해 높은 범위에 있는 소스 포트를 임의로 선택합니다. 따라서 이 포트에 대한 반송 트래픽이 허용되는지 확인해야 합니다.
  - 이 포트는 허용된 도메인에 나열된 필수 도메인에 개방되어 있어야 합니다.
  - AWS 세션 게이트웨이 및 CloudFront 도메인이 확인할 수 있는 범위를 포함하여 현재 IP 주소 범위를 JSON 형식으로 게시합니다. .json 파일을 다운로드하고 현재 범위를 보는 방법에 대한 자세한 내용은 AWS IP 주소 범위를 참조하십시오. 또는 사용 중인 경우 AWS Tools for Windows PowerShell명령을 사용하여 동일한 정보에 액세스할 수 있습니다. Get-AWSPublicIpAddressRange PowerShell 자세한 내용은 AWS의 퍼블릭 IP 주소 범위 쿼리 섹션을 참조하십시오.
- (선택 사항) 포트 53(UDP)
  - 포트 53은 사용자의 디바이스와 DNS 서버 간의 통신에 사용됩니다.
  - 도메인 이름 확인에 DNS 서버를 사용하지 않을 경우, 이 포트는 선택 사항입니다.
  - 퍼블릭 도메인 이름을 확인할 수 있도록 DNS 서버의 IP 주소에 대해 포트가 열려 있어야 합니다.

허용된 도메인

사용자가 로컬 브라우저에서 웹 포털에 액세스할 수 있게 하려면 사용자가 서비스에 액세스하려는 네트워크의 허용 목록에 다음 도메인을 추가해야 합니다.

다음 표에서 *{region}* 를 운영 중인 웹 포털의 지역 코드로 바꾸십시오. 예: s3. 유럽 (아일랜드) 지역 웹 포털의 경우 *{region}* .amazonaws.com은 s3.eu-west-1.amazonaws.com 이어야 합니다. 지역 코드 목록은 Amazon WorkSpaces 보안 브라우저 엔드포인트 및 할당량을 참조하십시오.

범주	도메인 또는 IP 주소
WorkSpaces 보안 브라우저 스트리밍 자산	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces 보안 브라우저 정적 자산	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces 보안 브라우저 인증	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces 보안 브라우저 지표 및 보고	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

구성된 ID 제공업체에 따라 추가 도메인 목록을 표시하도록 허용해야 할 수도 있습니다. IdP 설명서를 검토하여 WorkSpaces Secure Browser가 해당 공급자를 사용하려면 허용 목록이 필요한 도메인을 식

별하십시오. IAM Identity Center를 사용하는 경우 자세한 내용은 IAM Identity Center 사전 조건을 참조하십시오.

WorkSpaces 보안 브라우저 시작하기

다음 단계에 따라 WorkSpaces Secure Browser 웹 포털을 만들고 사용자에게 기존 브라우저에서 내부 및 SaaS 웹 사이트에 액세스할 수 있도록 하십시오. 계정별로 지원되는 모든 리전에 하나의 웹 포털을 생성할 수 있습니다.

> **Note**
>
> 두 개 이상의 포털에 대한 한도 증가를 요청하려면 AWS 계정 ID, 요청할 포털 수 등을 포함하여 지원팀에 문의하세요. AWS 리전

이 프로세스는 일반적으로 웹 포털 생성 마법사를 사용할 경우 5분 정도 소요되며 포털이 활성화되려면 최대 15분이 추가로 소요됩니다.

웹 포털 설정과 관련된 비용은 없습니다. WorkSpaces Secure Browser는 서비스를 적극적으로 사용하는 사용자에게 저렴한 월별 요금을 포함한 pay-as-you-go 가격을 제공합니다. 선불 비용, 라이선스 또는 장기 약정이 필요 없습니다.

> **Important**
>
> 시작하기 전에는 웹 포털에 필요한 사전 조건을 완료해야 합니다. 사전 조건에 대한 자세한 내용은 WorkSpaces 보안 브라우저 설정 섹션을 참조하십시오.

주제

- 1단계: 웹 포털 생성
- 2단계: 웹 포털 테스트
- 3단계: 웹 포털 배포
- 다음 단계

1단계: 웹 포털 생성

웹 포털을 생성하려면 아래 단계를 따릅니다.

주제

- 네트워크 설정 구성
- 포털 설정 구성
- 사용자 설정 구성
- ID 제공업체 구성
- 검토 및 시작

네트워크 설정 구성

1. https://console.aws.amazon.com/workspaces-web/home 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다.
2. WorkSpaces 보안 브라우저를 선택한 다음 웹 포털을 선택한 다음 웹 포털 생성을 선택합니다.
3. 1단계: 네트워킹 연결 지정 페이지에서 다음 단계를 완료하여 VPC를 웹 포털에 연결하고 VPC와 서브넷을 구성합니다.

    1. 네트워킹 세부 정보에서 사용자가 WorkSpaces Secure Browser를 통해 액세스하도록 하려는 콘텐츠에 연결된 VPC를 선택하십시오.
    2. 다음 요구 사항을 충족하는 프라이빗 서브넷을 최대 3개까지 선택합니다. 자세한 정보는 네트워킹 및 액세스을 참조하세요.
        - 포털을 생성하려면 최소 2개의 프라이빗 서브넷을 선택해야 합니다.
        - 웹 포털의 높은 가용성을 보장하려면 VPC의 고유 가용 영역에 최대 수의 프라이빗 서브넷을 제공하는 것이 좋습니다.
    3. 보안 그룹 선택

포털 설정 구성

2단계: 웹 포털 설정 구성 페이지에서 다음 단계를 완료하여 세션을 시작할 때의 사용자 브라우징 환경을 사용자 지정합니다.

1. 웹 포털 세부 정보의 표시 이름에 웹 포털의 식별 가능한 이름을 입력합니다.
2. 인스턴스 유형에서 드롭다운 메뉴에서 웹 포털의 인스턴스 유형을 선택합니다. 그런 다음 웹 포털의 최대 동시 사용자 한도를 입력합니다. 자세한 정보는 the section called “포털의 서비스 할당량을 관리합니다.”을 참조하세요.

> **Note**
>
> 새 인스턴스 유형을 선택하면 월간 활성 사용자당 비용이 변경됩니다. 자세한 내용은 Amazon WorkSpaces 보안 브라우저 요금을 참조하십시오.

3. 사용자 액세스 로깅의 Kinesis 스트림 ID에 데이터를 보내려는 Amazon Kinesis 데이터 스트림을 선택합니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.
4. 정책 설정에서 다음을 완료합니다.

   - 정책 옵션에서 시각적 편집기 또는 JSON 파일 업로드를 선택합니다. 두 방법 중 하나를 사용하여 웹 포털의 정책 구성 세부 정보를 제공할 수 있습니다. 자세한 정보는 the section called “브라우저 정책을 설정하거나 편집합니다.”을 참조하세요.
     - WorkSpaces 보안 브라우저에는 Chrome 엔터프라이즈 정책에 대한 지원이 포함됩니다. 시각적 편집기를 사용하거나 정책 파일을 수동으로 업로드하여 정책을 추가하고 관리할 수 있습니다. 언제든지 두 옵션 간에 전환할 수 있습니다.
     - 정책 파일을 업로드하면 콘솔 내 파일에서 가용 정책을 확인할 수 있습니다. 하지만 시각적 편집기에서 모든 정책을 편집할 수는 없습니다. 시각적 편집기로 편집할 수 없는 JSON 파일의 정책은 콘솔의 추가 JSON 정책에 나열되어 있습니다. 이러한 정책을 변경하려면 정책을 수동으로 편집해야 합니다.
   - (선택 사항) 시작 URL - 선택 사항에 사용자가 브라우저를 실행할 때 홈페이지로 사용할 도메인을 입력합니다. VPC는 이 URL에 안정적으로 연결되어 있어야 합니다.
   - 사용자 세션 중에 이러한 기능을 켜거나 끄려면 사생활 보호 모드 및 기록 삭제를 선택하거나 선택 해제합니다.

     > **Note**
     >
     > 비공개로 브라우징하는 동안 또는 사용자가 브라우저 기록을 삭제하기 전에 방문한 URL은 사용자 액세스 로깅에 기록될 수 없습니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.

   - URL 필터링에서 세션 중에 사용자가 방문할 수 있는 URL을 구성할 수 있습니다. 자세한 정보는 the section called “URL 필터링 설정”을 참조하세요.
   - (선택 사항) 사용자가 브라우저에서 볼 수 있는 북마크의 표시 이름, 도메인, 폴더를 브라우저 북마크 - 선택 사항에 입력합니다. 그런 다음 북마크 추가를 선택합니다.

> **Note**
>
> 도메인은 브라우저 북마크의 필수 필드입니다.
> Chrome에서 사용자는 북마크 도구 모음의 관리형 북마크 폴더에서 관리되는 북마크를 찾을 수 있습니다.

- (선택 사항) 포털에 태그를 추가합니다. 태그를 사용하여 AWS 리소스를 검색하거나 필터링할 수 있습니다. 태그는 키와 선택적 값으로 구성되며 포털 리소스와 연결됩니다.

5. 신뢰할 수 있는 네트워크에 대한 액세스를 제한할지 여부를 IP 액세스 제어(선택 사항)에서 선택합니다. 자세한 정보는 the section called “IP 액세스 제어 설정(선택 사항)”을 참조하세요.
6. 다음을 선택하여 계속 진행합니다.

사용자 설정 구성

3단계: 사용자 설정 선택 페이지에서 다음 단계를 완료하여 사용자가 세션 중에 상단 탐색 표시줄에서 액세스할 수 있는 기능을 선택한 후 다음을 선택합니다.

1. 사용자 권한에서 Single Sign-On용 확장 프로그램을 활성화할지 여부를 선택합니다. 자세한 정보는 the section called “Single Sign-On용 확장 프로그램 활성화(선택 사항)”을 참조하세요.
2. 클립보드 권한에서 비활성화됨 또는 활성화됨을 선택합니다.
3. 파일 전송에서 비활성화됨 또는 활성화됨을 선택합니다.
4. 사용자가 웹 포털에서 로컬 장치로 인쇄하도록 허용하려면 허용됨 또는 허용되지 않음을 선택합니다.
5. 사용자가 웹 포털에 딥링크를 걸 수 있도록 허용하려면 허용됨 또는 허용되지 않음을 선택합니다. 딥링크에 대한 자세한 내용은 을 참조하십시오. the section called “딥링크 허용 (선택 사항)”
6. 사용자 설정 세부 정보에서 다음을 지정합니다.

   - 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 세션을 종료하면 연결 끊기 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. 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.

ID 제공업체 구성

다음 단계를 사용하여 ID 공급자 (IdP) 를 구성하십시오.

주제

- ID 제공자 유형을 선택합니다.
- 표준 인증 유형을 구성하십시오.
- IAM ID 센터 인증 유형을 구성합니다.
- ID 제공자 유형을 변경하십시오.

ID 제공자 유형을 선택합니다.

WorkSpaces 보안 브라우저는 표준 및 두 가지 인증 유형을 제공합니다 AWS IAM Identity Center. ID 제공자 구성 페이지에서 포털에 사용할 인증 유형을 선택합니다.

- 표준 (기본 옵션) 의 경우 타사 SAML 2.0 ID 공급자 (예: Okta 또는 Ping) 를 포털과 직접 페더레이션하세요. 자세한 정보는 the section called “표준 인증 유형을 구성하십시오.”을 참조하세요. 표준 유형은 SP에서 시작한 인증 흐름과 IdP에서 시작한 인증 흐름을 모두 지원합니다.

- IAM ID 센터 (고급 옵션) 의 경우 IAM ID 센터를 포털과 페더레이션하십시오. 이 인증 유형을 사용하려면 IAM ID 센터와 WorkSpaces 보안 브라우저 포털이 모두 같은 위치에 있어야 합니다. AWS 리전 자세한 정보는 the section called “IAM ID 센터 인증 유형을 구성합니다.”을 참조하세요.

표준 인증 유형을 구성하십시오.

표준 (기본값) 의 경우 타사 SAML 2.0 ID 공급자 (예: Okta 또는 Ping) 를 포털과 직접 페더레이션하십시오.

표준 ID 유형은 SAML 2.0 준수 IdP를 사용하여 service-provider-initiated (SP 시작) 및 identity-provider-initiated (IdP 시작) 로그인 흐름을 지원할 수 있습니다.

1단계: 보안 브라우저에서 ID 공급자 구성 시작 WorkSpaces

다음 단계를 완료하여 ID 공급자를 구성하십시오.

1. 생성 마법사의 ID 제공업체(IdP) 구성 페이지에서 표준을 선택합니다.
2. 표준 IdP로 계속하기를 선택합니다.
3. SP 메타데이터 파일을 다운로드하고 개별 메타데이터 값을 보려면 탭을 열어 두십시오.
   - SP 메타데이터 파일을 사용할 수 있는 경우 메타데이터 파일 다운로드를 선택하여 서비스 공급자 (SP) 메타데이터 문서를 다운로드하고 다음 단계에서 서비스 제공자 메타데이터 파일을 IdP에 업로드합니다. 이렇게 하지 않으면 사용자는 로그인할 수 없습니다.
   - 공급자가 SP 메타데이터 파일을 업로드하지 않는 경우 메타데이터 값을 수동으로 입력하십시오.
4. SAML 로그인 유형 선택에서 SP에서 시작한 SAML 어설션과 IdP에서 시작한 SAML 어설션 중 하나를 선택하거나 SP에서 시작한 SAML 어설션만 선택합니다.
   - SP에서 시작한 SAML 어설션과 IdP에서 시작한 SAML 어설션을 통해 포털에서 두 가지 유형의 로그인 흐름을 모두 지원할 수 있습니다. IdP 시작 흐름을 지원하는 포털을 사용하면 사용자가 포털 URL을 방문하여 세션을 시작할 필요 없이 서비스 ID 페더레이션 엔드포인트에 SAML 어설션을 제시할 수 있습니다.
     - 포털에서 요청하지 않은 IdP 개시 SAML 어설션을 수락하도록 허용하려면 이 옵션을 선택합니다.
     - 이 옵션을 사용하려면 SAML 2.0 ID 공급자에 기본 릴레이 상태를 구성해야 합니다. 포털의 릴레이 상태 매개변수는 콘솔의 IdP 시작 SAML 로그인 아래에 있거나, 의 SP 메타데이터 파일에서 복사할 수 있습니다. `<md:IdPInitRelayState>`
     - 참고

- 릴레이 상태의 형식은 다음과 같습니다. `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`
- SP 메타데이터 파일에서 값을 복사하여 붙여넣는 경우 `&` 로 변경해야 & 합니다. `&`XML 이스케이프 문자입니다.

- 포털이 SP에서 시작한 로그인 플로우만 지원하도록 하려면 SP에서 시작한 SAML 어설션만 선택하십시오. 이 옵션은 IdP가 시작한 로그인 플로우에서 요청하지 않은 SAML 어설션을 거부합니다.

> **Note**
>
> 일부 타사의 경우 IdPs SP에서 시작한 흐름을 활용하여 IdP에서 시작한 인증 환경을 제공할 수 있는 사용자 지정 SAML 애플리케이션을 만들 수 있습니다. 예를 들어 Okta 북마크 애플리케이션 추가를 참조하십시오.

5. 이 공급자에 대한 SAML 서명 요청을 활성화할지 여부를 선택합니다. SP에서 시작한 인증을 사용하면 IdP가 포털에서 인증 요청이 오는지 확인할 수 있으므로 다른 타사 요청을 수락하지 못하게 됩니다.

   a. 서명 인증서를 다운로드하여 IdP에 업로드합니다. 단일 로그아웃에도 동일한 서명 인증서를 사용할 수 있습니다.

   b. IdP에서 서명된 요청을 활성화합니다. 이름은 IdP에 따라 다를 수 있습니다.

   > **Note**
   >
   > 지원되는 유일한 요청 및 기본 요청 서명 알고리즘은 RSA-SHA256 입니다.

6. 암호화된 SAML 어설션 필요를 활성화할지 여부를 선택합니다. 이렇게 하면 IdP에서 가져온 SAML 어설션을 암호화할 수 있습니다. IdP와 보안 브라우저 간의 SAML 어설션에서 데이터가 가로채지는 것을 방지할 수 있습니다. WorkSpaces

> **Note**
>
> 이 단계에서는 암호화 인증서를 사용할 수 없습니다. 포털이 시작된 후에 생성됩니다. 포털을 실행한 후 암호화 인증서를 다운로드하여 IdP에 업로드합니다. 그런 다음 IdP에서 어설션 암호화를 활성화합니다 (IdP에 따라 이름이 다를 수 있음).

7. 싱글 로그아웃을 활성화할지 여부를 선택합니다. 단일 로그아웃을 사용하면 최종 사용자가 한 번의 작업으로 IdP WorkSpaces 및 Secure Browser 세션 모두에서 로그아웃할 수 있습니다.

   a. WorkSpaces 보안 브라우저에서 서명 인증서를 다운로드하고 IdP에 업로드합니다. 이는 이전 단계에서 요청 서명에 사용한 것과 동일한 서명 인증서입니다.

   b. 단일 로그아웃을 사용하려면 SAML 2.0 ID 공급자에 단일 로그아웃 URL을 구성해야 합니다. 포털의 단일 로그아웃 URL은 콘솔의 서비스 공급자 (SP) 세부정보 - 개별 메타데이터 값 표시 또는 SP 메타데이터 파일에서 찾을 수 있습니다. `<md:SingleLogoutService>`

   c. IdP에서 싱글 로그아웃을 활성화하십시오. 이름은 IdP에 따라 다를 수 있습니다.

2단계: 자체 IdP에서 ID 제공업체 구성

브라우저에서 새 탭이 열립니다. 이후 IdP를 통해 다음 단계를 완료합니다.

1. 포털 메타데이터를 SAML IdP에 추가합니다.

   이전 단계에서 다운로드한 SP 메타데이터 문서를 IdP에 업로드하거나 메타데이터 값을 복사하여 IdP의 올바른 필드에 붙여넣습니다. 일부 공급자는 파일 업로드를 허용하지 않습니다.

   이 프로세스의 세부 사항은 공급자마다 다를 수 있습니다. IdP 구성에 포털 세부 정보를 추가하는 방법에 the section called “특정 항목에 대한 지침 IdPs” 대한 도움말은 에서 제공자의 설명서를 찾아보십시오.

2. SAML 어설션의 NameID를 확인합니다.

   SAML IdP가 SAML 어설션의 NameID를 사용자 이메일 필드로 채우는지 확인하십시오. NameID와 사용자 이메일은 포털에서 SAML 페더레이션 사용자를 고유하게 식별하는 데 사용됩니다. 영구 SAML 이름 ID 형식을 사용하십시오.

3. 선택 사항: IdP에서 시작한 인증을 위한 릴레이 상태를 구성합니다.

   이전 단계에서 SP 개시 및 IdP 개시 SAML 어설션 수락을 선택한 경우 의 2단계에 따라 IdP 애플리케이션의 기본 릴레이 상태를 the section called “1단계: 보안 브라우저에서 ID 공급자 구성 시작 WorkSpaces ” 설정합니다.

4. 선택 사항: 요청 서명 구성. 이전 단계에서 이 공급자에 대한 SAML 요청 서명을 선택한 경우, 3단계의 the section called “1단계: 보안 브라우저에서 ID 공급자 구성 시작 WorkSpaces ” 단계에 따라 서명 인증서를 IdP에 업로드하고 요청 서명을 활성화하십시오. Okta와 IdPs 같은 일부 서비스에서는 요청 서명을 사용하기 위해 NameID가 “영구” 유형에 속해야 할 수도 있습니다. 위 단계에 따라 SAML 어설션의 NameID를 확인하십시오.

5. 선택 사항: 어설션 암호화를 구성합니다. 이 공급자의 암호화된 SAML 어설션 필요를 선택한 경우 포털 생성이 완료될 때까지 기다린 다음 아래 “메타데이터 업로드”의 4단계에 따라 암호화 인증서를 IdP에 업로드하고 어설션 암호화를 활성화하십시오.
6. 선택 사항: 단일 로그아웃 구성. 단일 로그아웃을 선택한 경우 5단계의 단계에 따라 서명 인증서를 the section called “1단계: 보안 브라우저에서 ID 공급자 구성 시작 WorkSpaces ” IdP에 업로드하고 단일 로그아웃 URL을 입력한 다음 단일 로그아웃을 활성화합니다.
7. IdP의 사용자에게 WorkSpaces 보안 브라우저를 사용할 수 있는 액세스 권한을 부여하십시오.
8. IdP에서 메타데이터 교환 파일을 다운로드합니다. 다음 단계에서 이 메타데이터를 WorkSpaces 보안 브라우저에 업로드할 것입니다.

3단계: WorkSpaces Secure Browser에서 ID 제공자 구성을 완료합니다.

WorkSpaces 보안 브라우저 콘솔로 돌아가십시오. 생성 마법사의 ID 제공자 구성 페이지의 IdP 메타데이터에서 메타데이터 파일을 업로드하거나 IdP의 메타데이터 URL을 입력합니다. 포털은 IdP의 이 메타데이터를 사용하여 신뢰를 구축합니다.

1. 메타데이터 파일을 업로드하려면 IdP 메타데이터 문서에서 파일 선택을 선택합니다. 이전 단계에서 다운로드한 IdP로부터 XML 형식의 메타데이터 파일을 업로드합니다.
2. 메타데이터 URL을 사용하려면 이전 단계에서 설정한 IdP로 이동하여 해당 메타데이터 URL을 얻으십시오. WorkSpaces 보안 브라우저 콘솔로 돌아가서 IdP 메타데이터 URL 아래에 IdP에서 가져온 메타데이터 URL을 입력합니다.
3. 완료되면 다음을 선택합니다.
4. 이 공급자의 암호화된 SAML 어설션 필요 옵션을 활성화한 포털의 경우 포털 IdP 세부정보 섹션에서 암호화 인증서를 다운로드하여 IdP에 업로드해야 합니다. 그런 다음 해당 옵션을 활성화할 수 있습니다.

> **Note**
>
> WorkSpaces 보안 브라우저를 사용하려면 IdP 설정의 SAML 어설션에 제목 또는 NameID를 매핑하고 설정해야 합니다. IdP는 이러한 매핑을 자동으로 생성할 수 있습니다. 이러한 매핑이 올바르게 구성되지 않으면 사용자가 웹 포털에 로그인하여 세션을 시작할 수 없습니다.
>
> WorkSpaces 보안 브라우저를 사용하려면 SAML 응답에 다음과 같은 클레임이 있어야 합니다. <Your SP Entity ID><Your SP ACS URL>콘솔이나 CLI를 통해 포털의 서비스 제공자 세부정보 또는 메타데이터 문서에서 찾을 수 있습니다.

- SP Entity ID를 응답 대상으로 설정하는 Audience 값이 포함된 AudienceRestriction 클레임 예제

```
<saml:AudienceRestriction>
    <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- 원래 SAML 요청 ID의 InResponseTo 값이 포함된 Response 클레임. 예제

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- SP ACS URL Recipient 값과 원래 SAML 요청 ID와 일치하는 InResponseTo 값을 포함하는 SubjectConfirmationData 클레임 예제

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces 보안 브라우저는 요청 파라미터와 SAML 어설션의 유효성을 검사합니다. IdP에서 시작한 SAML 어설션의 경우 요청 세부 정보를 HTTP POST 요청 본문의 RelayState 파라미터 형식으로 지정해야 합니다. 요청 본문에는 SAML 어설션도 파라미터로 포함되어야 합니다. SAMLResponse 이전 단계를 따랐다면 이 두 가지가 모두 있어야 합니다.
다음은 IdP에서 시작한 SAML 공급자의 예제 POST 본문입니다.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

특정 항목에 대한 지침 IdPs

포털의 SAML 페더레이션을 올바르게 구성하려면 아래 링크에서 일반적으로 사용되는 IdPs 설명서를 참조하십시오.

IdP	SAML 애플리케이션 설정	사용자 관리	IDP가 시작한 인증	요청 서명	어설션 암호화	싱글 로그아웃
Okta	SAML 앱 통합 생성	사용자 관리	애플리케이션 통합 마법사 SAML 필드 참조	애플리케이션 통합 마법사 SAML 필드 참조	애플리케이션 통합 마법사 SAML 필드 참조	애플리케이션 통합 마법사 SAML 필드 참조
엔트라	나만의 애플리케이션 만들기	퀵스타트: 사용자 계정 생성 및 할당	엔터프라이즈 애플리케이션을 위한 싱글 사인온 활성화	SAML 요청 서명 확인	마이크로소프트 엔트라 SAML 토큰 암호화 구성	싱글 로그아웃 SAML 프로토콜
Ping	SAML 애플리케이션 추가	사용자	IdP에서 시작하는 SSO 활성화	엔터프라이즈에 대한 인증 요청 로그인 구성 PingOne	PingOne 엔터프라이즈용 암호화를 지원하나요?	SAML 2.0 싱글 로그아웃
한 번의 로그인	SAML 사용자 지정 커넥터 (고급) (4266907)	OneLogin 수동으로 사용자 추가	SAML 사용자 지정 커넥터 (고급) (4266907)	SAML 맞춤형 커넥터 (고급) (4266907)	SAML 맞춤형 커넥터 (고급) (4266907)	SAML 맞춤형 커넥터 (고급) (4266907)
IAM Identity Center	자신만의 SAML 2.0 애플리케이션을 설정하세요	자체 SAML 2.0 애플리케이션을 설정하세요.	자체 SAML 2.0 애플리케이션을 설정하세요.	N/A	해당 사항 없음	N/A

IAM ID 센터 인증 유형을 구성합니다.

IAM ID 센터 유형 (고급) 의 경우 IAM ID 센터를 포털과 페더레이션합니다. 다음 조건에 해당하는 경우에만 이 옵션을 선택하십시오.

- IAM ID 센터는 웹 AWS 계정 포털과 AWS 리전 동일하게 구성됩니다.
- 를 사용하고 AWS Organizations있다면 관리 계정을 사용하고 있는 것입니다.

IAM ID 센터 인증 유형을 사용하여 웹 포털을 생성하기 전에 IAM Identity Center를 독립형 공급자로 설정해야 합니다. 자세한 내용은 IAM Identity Center에서 일반 작업 시작하기를 참조하십시오. 또는 SAML 2.0 IdP를 IAM ID 센터에 연결할 수 있습니다. 자세한 내용은 외부 ID 공급자에 연결을 참조하십시오. 그렇지 않으면 웹 포털에 할당할 사용자나 그룹이 없게 됩니다.

이미 IAM Identity Center를 사용하고 있는 경우 공급자 유형으로 IAM Identity Center를 선택하고 아래 단계에 따라 웹 포털에서 사용자 또는 그룹을 추가, 확인 또는 제거할 수 있습니다.

> **Note**
>
> 이 인증 유형을 사용하려면 IAM ID 센터가 WorkSpaces 보안 브라우저 AWS 계정 포털과 AWS 리전 동일한 위치에 있어야 합니다. IAM ID 센터가 별도의 AWS 계정 AWS 리전 OR에 있는 경우 표준 인증 유형에 대한 지침을 따르십시오. 자세한 정보는 the section called “표준 인증 유형을 구성하십시오.”을 참조하세요.
> 를 사용하는 경우 관리 AWS Organizations계정을 사용하여 IAM Identity Center와 통합된 WorkSpaces 보안 브라우저 포털만 생성할 수 있습니다.

IAM Identity Center를 통한 웹 포털 생성

1. 4단계: ID 제공자 구성에서 포털을 생성하는 동안 선택하십시오. AWS IAM Identity Center
2. [IAM ID 센터 계속 사용] 을 선택합니다.
3. 사용자 및 그룹 할당 페이지에서 사용자 및/또는 그룹 탭을 선택합니다.
4. 포털에 추가하려는 사용자 또는 그룹 옆의 체크박스를 선택합니다.
5. 포털을 생성한 후 연결한 사용자는 IAM Identity Center 사용자 이름과 비밀번호를 사용하여 WorkSpaces Secure Browser에 로그인할 수 있습니다.

IAM Identity Center를 통한 웹 포털 관리

1. 포털을 생성하면 IAM Identity Center 콘솔에 구성된 애플리케이션으로 나열됩니다.
2. 이 애플리케이션의 구성에 액세스하려면 사이드바에서 애플리케이션을 선택하고 웹 포털의 표시 이름과 일치하는 이름을 가진 구성된 애플리케이션을 찾습니다.

> **Note**
>
> 표시 이름을 입력하지 않은 경우에는 포털의 GUID가 대신 표시됩니다. GUID는 웹 포털의 엔드포인트 URL 앞에 붙는 ID입니다.

기존 웹 포털에 사용자 및 그룹 추가

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 편집을 선택합니다.
3. ID 제공업체 설정 및 추가 사용자 및 그룹 할당을 선택합니다. 여기에서 웹 포털에 사용자와 그룹을 추가할 수 있습니다.

> **Note**
>
> IAM Identity Center 콘솔에서는 사용자 또는 그룹을 추가할 수 없습니다. WorkSpaces 보안 브라우저 포털의 편집 페이지에서 이 작업을 수행해야 합니다.

웹 포털의 사용자 및 그룹을 보거나 제거하려면

- 할당된 사용자 테이블에서 사용할 수 있는 작업을 사용하여 이 응용 프로그램에 대한 사용자 접근 권한을 보거나 제거할 수 있습니다. 자세한 내용은 응용 프로그램에 대한 액세스 관리를 참조하십시오.

> **Note**
>
> WorkSpaces Secure Browserportal의 편집 페이지에서는 사용자 및 그룹을 보거나 제거할 수 없습니다. IAM Identity Center 콘솔의 편집 페이지에서 이 작업을 수행해야 합니다.

ID 제공자 유형을 변경하십시오.

언제든지 다음 단계에 따라 포털의 인증 유형을 변경할 수 있습니다.

- IAM ID 센터에서 스탠다드로 변경하려면 의 단계를 따르세요. the section called “표준 인증 유형을 구성하십시오.”
- 스탠다드에서 IAM ID 센터로 변경하려면 의 단계를 따르십시오. the section called “IAM ID 센터 인증 유형을 구성합니다.”

ID 제공자 유형을 변경하면 배포하는 데 최대 15분이 소요될 수 있으며 진행 중인 세션은 자동으로 종료되지 않습니다.

이벤트를 AWS CloudTrail `UpdatePortal` 검사하여 포털의 ID 제공자 유형 변경 사항을 확인할 수 있습니다. 유형은 이벤트의 요청 및 응답 페이로드에서 볼 수 있습니다.

검토 및 시작

1. 웹 포털에 대해 선택한 설정을 5단계: 검토 및 실행 페이지에서 검토합니다. 편집을 선택하여 해당 섹션 내의 설정을 변경할 수 있습니다. 나중에 콘솔의 웹 포털 탭에서 이러한 설정을 변경할 수도 있습니다.
2. 완료했으면 웹 포털 시작을 선택합니다.
3. 웹 포털의 상태를 보려면 웹 포털을 선택하고 해당 포털을 선택한 다음 세부 정보 보기를 선택합니다.

   웹 포털은 다음 상태 중 하나를 가집니다.

   - 미완료 - 웹 포털 구성에 필수 ID 제공업체 설정이 없습니다.
   - 대기 중 - 웹 포털에서 설정 변경 사항을 적용하고 있습니다.
   - 활성 - 웹 포털을 사용할 준비가 되어 있습니다.
4. 포털이 활성 상태가 때까지 최대 15분 정도 걸립니다.

2단계: 웹 포털 테스트

웹 포털을 만든 후에는 WorkSpaces Secure Browser 엔드포인트에 로그인하여 최종 사용자처럼 연결된 웹 사이트를 탐색할 수 있습니다.

the section called “ID 제공업체 구성”에서 이 단계를 이미 완료한 경우에는 이 섹션을 건너뛰고 3단계: 웹 포털 배포의 단계를 수행할 수 있습니다.

1. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/ 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다.
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 세부 정보 보기를 선택합니다.
3. 웹 포털 엔드포인트에서 포털의 지정된 URL로 이동합니다. 웹 포털 엔드포인트는 사용자가 포털에 구성된 ID 제공업체로 로그인한 후 웹 포털을 시작하는 액세스 포인트입니다. 인터넷에서 공개적으로 사용할 수 있으며 네트워크에 내장할 수 있습니다.
4. WorkSpaces 보안 브라우저 로그인 페이지에서 로그인, SAML을 선택하고 SAML 자격 증명을 입력합니다.
5. 세션 준비 중 페이지가 표시되면 WorkSpaces 보안 브라우저 세션이 시작되는 것입니다. 이 페이지를 닫거나 종료하지 마십시오.
6. 웹 브라우저가 시작되고 시작 URL과 브라우저 정책 설정을 통해 구성된 기타 추가 동작이 표시됩니다.
7. 이제 링크를 선택하여 연결된 웹 사이트를 브라우징하거나 주소 표시줄에 URL을 입력할 수 있습니다.

3단계: 웹 포털 배포

사용자가 WorkSpaces Secure Browser 사용을 시작할 준비가 되면 다음 옵션 중에서 선택하여 포털을 배포합니다.

- 포털을 SAML 애플리케이션 게이트웨이에 추가하여 사용자가 IdP에서 직접 세션을 시작할 수 있도록 하세요. SAML 2.0 호환 IdP를 사용하여 IdP에서 시작하는 로그인 흐름을 통해 이 작업을 수행할 수 있습니다. 자세한 내용은 의 SP 개시 및 IdP 개시 SAML 어설션을 참조하십시오. the section called “표준 인증 유형을 구성하십시오.” 또는 SP에서 시작한 흐름을 사용하여 IdP에서 시작한 인증 환경을 제공할 수 있는 사용자 지정 SAML 애플리케이션을 만들 수 있습니다. 자세한 내용은 북마크 앱 통합 생성을 참조하십시오.
- 소유 중인 웹사이트에 포털 URL을 추가하고 브라우저 리디렉션을 사용하여 사용자를 웹 포털로 안내합니다.
- 포털 URL을 사용자에게 이메일로 보내거나 브라우저 홈페이지 또는 북마크로 관리 중인 디바이스로 푸시 다운합니다.

다음 단계

첫 번째 웹 포털을 생성한 후에는 언제든지 세부 정보를 보거나, 세부 정보를 편집하거나, 웹 포털을 삭제할 수 있습니다. 자세한 정보는 웹 포털 관리을 참조하세요.

WorkSpaces 보안 브라우저를 사용할 AWS 계정 수 AWS 리전 있는 각 위치에 웹 포털을 만들 수 있습니다. 각 웹 포털은 언제든지 최대 25개의 사용자 연결을 지원할 수 있습니다. 리전에서 생성할 수 있는 포털 수를 늘리거나 포털에 더 많은 동시 세션을 지원하려면 the section called “포털의 서비스 할당량을 관리합니다.” 섹션을 참조하십시오.

웹 포털 관리

웹 포털을 설정한 후에는 포털의 세부 정보를 보거나 편집할 수 있으며 더 이상 필요하지 않은 포털을 삭제할 수 있습니다.

주제

- 웹 포털 세부 정보 보기
- 웹 포털 편집
- 웹 포털 삭제
- 포털의 서비스 할당량을 관리합니다.
- SAML IdP 토큰 재인증 간격 제어
- 사용자 액세스 로깅 설정
- 브라우저 정책을 설정하거나 편집합니다.
- 입력 방법 편집기(IME) 구성
- 세션 내 로컬라이제이션 구성
- IP 액세스 제어 설정(선택 사항)
- Single Sign-On용 확장 프로그램 활성화(선택 사항)
- URL 필터링 설정
- 딥링크 허용 (선택 사항)

웹 포털 세부 정보 보기

웹 포털 세부 정보 보기

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 세부 정보 보기를 선택합니다.

웹 포털 편집

웹 포털 편집

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 편집을 선택합니다.

> **Note**
>
> 네트워킹 설정 또는 제한 시간 설정을 변경하면 모든 활성 포털 세션이 즉시 종료됩니다. 사용자는 연결이 끊겼으므로 새 세션을 시작하려면 다시 연결해야 합니다. 클립보드 권한, 파일 전송 권한 또는 로컬 디바이스로 인쇄에 대한 변경 사항은 새로운 첫 번째 세션부터 적용됩니다. 현재 활성 세션은 연결이 끊기지 않습니다. 활성 세션에 연결된 사용자는 연결을 끊고 새 세션에 연결할 때까지 변경 사항의 영향을 받지 않습니다.

웹 포털 삭제

웹 포털 삭제

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 삭제를 선택합니다.

포털의 서비스 할당량을 관리합니다.

계정을 만들면 리소스 AWS 계정사용에 대한 기본 서비스 할당량 (한도라고도 함) 이 자동으로 설정됩니다. AWS 서비스관리자는 사용 사례를 지원하기 위해 두 개의 할당량을 늘려야 할 수 있다는 점을 알고 있어야 합니다. 이 두 할당량은 각 지역에서 생성할 수 있는 웹 포털의 수와 각 지역에서 사용 가능한 각 인스턴스 유형에 대해 지원할 수 있는 최대 동시 세션 수입니다. 콘솔의 Service Quotas 페이지에서 이에 대한 증가를 요청할 수 있습니다. AWS

다음 표에는 기본 서비스 할당량 한도가 나와 있습니다.

계정별 기본 할당량 AWS 리전	값
웹 포털	3
최대 동시 세션 - 표준.레귤러	25

계정별 기본 할당량 AWS 리전	값
최대 동시 세션 - 표준.대형	10
최대 동시 세션 - 표준.xlarge	5

> **Important**
>
> 서비스 할당량은 한 번에 하나씩 적용됩니다. AWS 리전 리소스가 더 필요한 AWS 리전 곳마다 서비스 할당량 증가를 요청해야 합니다. 자세한 내용은 Amazon WorkSpaces 보안 브라우저 엔드포인트 및 할당량을 참조하십시오.

서비스 할당량 증가 요청

1. AWS Support 대시보드를 엽니다.
2. 서비스 한도 증가를 선택합니다.

   > **Important**
   >
   > WorkSpaces 보안 브라우저 서비스 할당량은 한 번에 한 지역에만 영향을 미칩니다. 더 많은 리소스가 필요한 각각의 AWS 리전에서 서비스 할당량 증가를 요청해야 합니다. 자세한 내용은 AWS 서비스 엔드포인트를 참조하십시오.

3. 사용 사례 설명에서 다음 정보를 입력합니다.

   - 웹 포털 수 증가를 요청하는 경우에는 이 리소스 유형을 지정하고, AWS 계정 ID, 증가가 필요한 리전, 새 한도 값을 포함하십시오.
   - 최대 동시 세션의 증가를 요청하는 경우에는 이 리소스 유형을 지정하고, AWS 계정 ID, 증가가 필요한 리전, 웹 포털 ARN, 새 한도 값을 포함하십시오.

4. (선택 사항) 다수의 서비스 할당량 증가를 동시에 요청하려면 요청 섹션에서 하나의 할당량 증가 요청을 완료한 다음 다른 요청 추가를 선택합니다.

포털 증액 요청

포털은 서비스의 기본 리소스입니다. 각 포털은 SAML 2.0 ID 공급자와 인터넷 및 개인 웹 콘텐츠에 대한 네트워킹 연결 간의 연결입니다. 각 포털에는 별도의 포털 브라우저 정책과 사용자 설정이 있을 수

있으므로 관리자는 일반적으로 동일한 지역에 여러 포털을 생성하여 다양한 사용 사례를 처리합니다. 예를 들어 그룹 A에게는 제한적인 정책 (예: 클립보드 및 파일 전송 비활성화) 으로 특정 웹 사이트에 대한 액세스 권한을 제공하고, 그룹 B에게는 URL 필터링 없이 일반 인터넷에 액세스할 수 있는 권한을 제공할 수 있습니다. 지원되는 모든 곳에서 포털을 만들 수 있습니다. AWS 리전현재 서비스 가용성을 보려면 지역별 AWS 서비스를 참조하십시오.

서비스 할당량 증가 요청

1. 원하는 지역에서 Service Quotas 페이지를 엽니다.
2. 웹 포털 수를 선택합니다.
3. 계정 수준 증가 요청을 선택합니다.
4. 할당량 증가에서 원하는 할당량 총액을 입력합니다.

최대 동시 세션 증가를 요청하세요.

최대 동시 세션 할당량은 포털에 동시에 연결할 수 있는 최대 사용자 수입니다. 최대 동시 세션의 서비스 할당량 제한이 적절하게 설정되지 않은 경우 사용자가 로그인할 때 세션을 사용할 수 없는 경우가 발생할 수 있습니다. 이 서비스 할당량을 늘리는 것 외에도 고객은 VPC와 서브넷에 최대 동시 세션을 지원할 수 있는 충분한 IP 공간이 있는지 확인해야 합니다.

최대 동시 세션 증가를 요청하려면

1. 원하는 지역에서 Service Quotas 페이지를 엽니다.
2. 늘리려는 인스턴스 유형에 대해 포털당 최대 동시 세션 수를 선택합니다.
3. 계정 수준에서 증가 요청을 선택합니다.
4. 할당량 증가에서 원하는 할당량 총액을 입력합니다.

> **Note**
>
> 대규모 또는 긴급한 증가의 경우 Service Quotas 기록 페이지로 이동하여 요청의 상태 열에 있는 링크를 선택하고 지원 사례로 연결한 다음 사용 사례 및/또는 긴급성에 대한 세부 정보가 포함된 회신을 추가하십시오. 이 정보는 서비스 팀이 요청의 우선 순위를 정하고 계정에 충분한 용량이 할당되도록 하는 데 도움이 됩니다.

한도 예시

예를 들어, 한 관리자가 미국 동부 (버지니아 북부) 에서 총 125명의 사용자를 위한 웹 포털 두 개를 구성하고 있다고 가정해 보겠습니다. 관리자는 웹 포털을 생성하기 전에 첫 번째 웹 포털 (포털 A) 이 100명의 사용자를 지원할 것인지 확인합니다. 관리자는 이러한 사용자를 대상으로 워크플로를 테스트할 때 세션 중 오디오 및 비디오 스트리밍을 지원하기 위해 XL 인스턴스 유형이 필요하다고 판단합니다. 고객 VPC에 호스팅된 단일 정적 웹 페이지에 대한 액세스를 지원하려면 최대 25명의 사용자가 두 번째 웹 포털 (포털 B) 을 사용할 수 있어야 합니다. 이 사용 사례를 테스트할 때 관리자는 표준 인스턴스 유형이 이 사용 사례를 지원할 수 있다고 판단합니다.

포털 A의 경우 관리자는 서비스 할당량 증가 요청을 제출하여 XL 인스턴스의 한도를 지역 기본값 (예: 5) 에서 100으로 늘려야 합니다. 용량이 충족되면 관리자는 웹 포털을 편집하여 용량을 할당할 수 있습니다. 포털 B의 경우 관리자는 할당량 증가를 요청하지 않고 계속 진행할 수 있습니다 (즉, 지역의 표준 인스턴스 유형에 대한 기본 할당량이 25이므로).

서비스 할당량 관리

언제든지 각 지역의 계정에 할당된 서비스 할당량을 보려면 Service Quotas 페이지를 참조하십시오.

기타 서비스 할당량

Service Quotas 페이지에 나열된 다른 할당량을 확인하고 증가를 요청할 수 있습니다. 실제로 대부분의 고객은 이러한 한도에 대한 상향 조정을 요청할 필요가 없다는 것을 알게 될 것입니다. 이러한 할당량은 크게 숫자와 요율이라는 두 가지 유형으로 분류됩니다.

번호 할당량의 경우 웹 포털 수에 대한 서비스 할당량 증가를 제출하면 고유한 포털을 만드는 데 필요한 하위 리소스 수가 자동으로 증가합니다. 이 내용은 Service Quotas 페이지에 반영됩니다. 예를 들어 포털을 3개에서 5개로 늘리도록 요청하면 브라우저와 사용자 설정 모두에 대해 자동으로 서비스 할당량이 3개에서 5개로 늘어납니다. 필요에 따라 하위 리소스를 재사용하거나 새 하위 리소스를 만들 수 있습니다.

드문 경우이긴 하지만 고객이 다른 리소스 할당량의 수나 비율을 높이는 사용 사례를 발견할 수도 있습니다. 예를 들어 관리자는 추가 포털 구성을 테스트하기 위해 브라우저 설정 수를 늘리고 싶을 수 있습니다. 이러한 서비스 할당량 요청은 case-by-case 기준에 따라 검토 및 이행됩니다.

요금 할당량의 경우 계정 포털 한도와 상관없이 Service Quotas에 표시된 요금 한도를 조정할 필요가 없습니다.

SAML IdP 토큰 재인증 간격 제어

사용자가 WorkSpaces Secure Browser 포털을 방문하면 로그인하여 스트리밍 세션을 시작할 수 있습니다. 로그인한 지 5분 미만인 경우를 제외하고 모든 세션은 시작 페이지에서 시작됩니다. 포털은 ID 제공업체(IdP) 토큰을 확인하여 세션을 시작할 때 사용자에게 보안 인증 요구 메시지를 표시할지 여부를 결정합니다. 유효한 IdP 토큰이 없는 사용자는 사용자 이름, 암호 및 다중 인증(MFA)(선택 사항)을 입력하여 스트리밍 세션을 시작해야 합니다. 사용자가 이미 IdP 또는 동일한 IdP로 보호되는 앱에 로그인하여 SAML IdP 토큰을 생성한 경우에는 로그인 보안 인증을 요청하지 않습니다.

유효한 SAML IdP 토큰이 있는 사용자는 보안 브라우저에 WorkSpaces 액세스할 수 있습니다. SAML IdP 토큰을 재인증하는 데 필요한 간격을 제어할 수 있습니다.

SAML IdP 토큰 재인증 간격 제어

1. SAML IdP 제공업체를 통해 IdP 제한 시간을 설정합니다. 사용자가 작업을 완료하는 데 필요한 가장 짧은 시간으로 IdP 제한 시간을 구성하는 것이 좋습니다.

   - Okta에 대한 자세한 내용은 모든 정책에 제한된 세션 시간 적용 섹션을 참조하십시오.
   - Azure AD에 대한 자세한 내용은 인증 세션 제어 구성 섹션을 참조하십시오.
   - 세션에 대한 자세한 내용은 세션 섹션을 참조하십시오.
   - 에 대한 자세한 내용은 세션 AWS IAM Identity Center기간 설정을 참조하십시오.

2. WorkSpaces Secure Browser 포털의 비활성 및 유휴 제한 시간 값을 설정합니다. 이 값은 사용자의 마지막 상호 작용과 비활동으로 인해 WorkSpaces Secure Browser 세션이 종료되는 시점 사이의 시간을 제어합니다. 세션이 종료되면 사용자는 세션 상태(열린 탭, 저장되지 않은 웹 콘텐츠, 기록 등)를 잃고 다음 세션이 시작될 때 새로운 상태로 돌아갑니다. 자세한 내용은 the section called "1단계: 웹 포털 생성"의 5단계를 참조하십시오.

   > **Note**
   >
   > 사용자의 세션 제한 시간이 초과되었는데도 사용자에게 유효한 SAML IdP 토큰이 있는 경우 WorkSpaces 새 Secure Browser 세션을 시작하기 위해 사용자 이름과 암호를 입력할 필요가 없습니다. 토큰 재인증 방법을 제어하려면 이전 단계의 안내를 따릅니다.

사용자 액세스 로깅 설정

사용자 액세스 로깅을 설정하여 사용자 이벤트를 기록할 수 있습니다.

- 세션 시작 - WorkSpaces 보안 브라우저 세션의 시작을 표시합니다.
- 세션 종료 - WorkSpaces 보안 브라우저 세션의 종료를 표시합니다.
- URL 탐색 - 사용자가 로드한 URL을 기록합니다.

> **Note**
>
> URL 탐색 로그는 브라우저 기록에서 기록됩니다. 브라우저 기록에 기록되지 않은 URL(시크릿 모드로 방문했거나 브라우저 기록에서 삭제된 URL)은 로그에 기록되지 않습니다. 브라우저 정책에 따라 시크릿 모드를 해제할지 아니면 방문 기록 삭제를 해제할지는 고객이 결정합니다.

또한 다음과 같은 각 이벤트의 정보가 포함됩니다.

- 이벤트 시간
- 사용자 이름
- 웹 포털 ARN

고객은 보안 브라우저를 사용할 때 발생할 수 있는 잠재적 법적 문제를 이해하고 WorkSpaces 보안 브라우저를 사용할 때 모든 관련 법률 및 규정을 준수하는지 확인할 책임이 있습니다. WorkSpaces 여기에는 애플리케이션 내에서 수행되는 활동을 포함하여 고용주가 직원의 WorkSpaces 보안 브라우저 사용을 모니터링할 수 있는 권한을 규제하는 법률이 포함됩니다.

WorkSpaces 보안 브라우저 포털에서 사용자 액세스 로그를 활성화하면 Amazon Kinesis Data Streams에서 요금이 부과될 수 있습니다. 요금에 대한 자세한 내용은 Amazon Kinesis Data Streams 요금을 참조하십시오.

WorkSpaces 보안 브라우저 콘솔에서 사용자 액세스 로깅을 활성화하려면 사용자 액세스 로깅에서 데이터를 수신하는 데 사용할 Kinesis Stream ID를 선택합니다. 기록된 데이터는 해당 스트림으로 직접 전달됩니다.

Amazon Kinesis 데이터 스트림 생성에 대한 자세한 내용은 Amazon Kinesis Data Streams란? 섹션을 참조하십시오.

> **Note**
>
> WorkSpaces 보안 브라우저에서 로그를 수신하려면 “amazon-workspaces-web-*”로 시작하는 Amazon Kinesis 데이터 스트림이 있어야 합니다. Amazon Kinesis 데이터 스트림에는 서버 측 암호화가 해제되어 있거나 서버 측 암호화에 사용해야 AWS 관리형 키 합니다.
> Amazon Kinesis에서 서버 측 암호화를 설정하는 방법에 대한 자세한 내용은 서버 측 암호화를 시작하는 방법 섹션을 참조하십시오.

샘플 로그

다음은 검증,, 및 을 포함하여 사용 가능한 각 이벤트의 예입니다. StartSessionVisitPageEndSession

각 이벤트에는 다음 필드가 항상 포함됩니다.

- timestamp는 밀리초 단위의 에포크 시간으로 포함됩니다.
- eventType은 문자열로 포함됩니다.
- details는 다른 json 객체로 포함됩니다.
- portalArn과 userName은 Validation을 제외한 모든 이벤트에 포함됩니다.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

```
{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

브라우저 정책을 설정하거나 편집합니다.

WorkSpaces Secure Browser를 사용하면 안정적인 최신 버전에 사용할 수 있는 Chrome 정책을 사용하여 사용자 지정 브라우저 정책을 설정할 수 있습니다. 웹 포털에 적용할 수 있는 정책은 300개가 넘습니다. 자세한 내용은 the section called “사용자 지정 브라우저 정책 설정(예시)” 및 Chrome 엔터프라이즈 정책 목록을 참조하십시오.

콘솔 보기를 사용하여 웹 포털을 생성하면 다음 정책을 적용할 수 있습니다.

- `StartURL`
- 북마크 및 북마크 폴더
- 프라이빗 브라우징 설정 및 해제
- 기록 삭제
- `AllowURL` 및 `BlockURL`을 사용한 URL 필터링

콘솔 보기 정책 사용에 대한 자세한 내용은 WorkSpaces 보안 브라우저 시작하기 섹션을 참조하십시오.

WorkSpaces Secure Browser는 기본 브라우저 정책 구성을 사용자가 지정하는 정책과 함께 모든 포털에 적용합니다. 사용자 지정 JSON 파일을 사용하여 이러한 정책 중 일부를 편집할 수 있습니다. 자세한 정보는 the section called “기본 브라우저 정책을 편집합니다.”을 참조하세요.

주제

- 사용자 지정 브라우저 정책 설정(예시)
- 기본 브라우저 정책을 편집합니다.

사용자 지정 브라우저 정책 설정(예시)

지원되는 Linux용 Chrome 정책은 JSON 파일을 업로드하여 설정할 수 있습니다. Chrome 정책에 대한 자세한 내용은 Chrome 엔터프라이즈 정책 목록을 참조하고 Linux 플랫폼을 선택하십시오. 그런 다음 해당 정책을 검색하여 안정적인 최신 버전을 검토합니다.

다음 예시에서는 다음과 같은 정책 제어 기능을 사용하여 웹 포털을 생성합니다.

- 북마크 설정
- 기본 시작 페이지 설정
- 사용자가 다른 확장 프로그램을 설치하지 못하도록 방지
- 사용자가 기록을 삭제하지 못하도록 방지
- 사용자가 시크릿 모드에 액세스하지 못하도록 방지
- 모든 세션에 Okta 플러그인 확장 프로그램을 사전 설치합니다.

주제

- 1단계: 웹 포털 생성
- 2단계: 정책 수집
- 3단계: 사용자 지정 JSON 정책 파일 생성
- 4단계: 템플릿에 정책 추가
- 5단계: 정책 JSON 파일을 웹 포털에 업로드

1단계: 웹 포털 생성

Chrome 정책 JSON 파일을 업로드하려면 WorkSpaces 보안 브라우저 포털을 생성해야 합니다. 자세한 정보는 the section called “1단계: 웹 포털 생성”을 참조하세요.

2단계: 정책 수집

Chrome 정책에서 원하는 정책을 검색하고 찾습니다. 그런 다음 다음 단계에서 정책을 사용하여 JSON 파일을 생성합니다.

1. Chrome 엔터프라이즈 정책 목록으로 이동합니다.
2. Linux 플랫폼을 선택한 다음 최신 Chrome 버전을 선택합니다.
3. 설정하려는 정책을 검색합니다. 이 예시에서는 확장 프로그램을 찾고 관리하기 위한 정책을 검색합니다. 각 정책에는 설명, Linux 기본 설정 이름, 샘플 값이 포함됩니다.
4. 함께 사용할 경우 비즈니스 요구 사항을 충족하는 세 가지 정책을 검색 결과에서 찾을 수 있습니다.
   - ExtensionSettings— 브라우저 시작 시 확장 프로그램을 설치합니다.
   - ExtensionInstallBlocklist— 특정 확장 프로그램이 설치되지 않도록 합니다.
   - ExtensionInstallAllowlist— 특정 확장 프로그램을 설치할 수 있습니다.
5. 추가 정책은 나머지 요구 사항을 충족합니다.
   - ManagedBookmarks— 웹 페이지에 북마크를 추가합니다.
   - RestoreOnStartupURL - 새 브라우저 창이 시작될 때마다 열리는 웹 페이지를 구성합니다.
   - AllowDeletingBrowserHistory— 사용자가 인터넷 사용 기록을 삭제할 수 있는지 여부를 구성합니다.
   - IncognitoModeAvailability— 사용자가 시크릿 모드에 액세스할 수 있는지 여부를 구성합니다.

3단계: 사용자 지정 JSON 정책 파일 생성

텍스트 편집기, 템플릿 및 이전 단계에서 찾은 정책을 사용하여 JSON 파일을 생성합니다.

1. 텍스트 편집기를 엽니다.
2. 다음 텍스트를 복사하여 텍스트 편집기에 붙여 넣습니다.

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
```

```
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
```

```
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

4단계: 템플릿에 정책 추가

각 비즈니스 요구 사항의 템플릿에 사용자 지정 정책을 추가합니다.

1. 북마크 URL을 설정합니다.
   a. 추가하려는 각 북마크의 `name` 및 `url` 키 쌍을 `value` 키에서 추가합니다.
   b. `bookmark-url-1`을 `https://www.amazon.com`으로 설정합니다.
   c. `bookmark-url-2`를 `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`로 설정합니다.

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. 시작 URL을 설정합니다. 이 정책을 통해 관리자는 사용자가 새 브라우저 창을 열 때 표시되는 웹 페이지를 설정할 수 있습니다.

a. RestoreOnStartup을 4로 설정합니다. 이렇게 하면 URL 목록을 여는 RestoreOnStartup 작업이 설정됩니다. 시작 URL에서 다른 작업을 사용할 수도 있습니다. 자세한 내용은 Chrome 엔터프라이즈 정책 목록을 참조하십시오.

b. RestoreOnStartupURLs를 https://www.aboutamazon.com/news로 설정합니다.

```
 "RestoreOnStartup":
    {
        "value": 4
    },
"RestoreOnStartupURLs":
    {
        "value":
        [
            "https://www.aboutamazon.com/news"
        ]
    },
```

3. 사용자가 브라우저 기록을 삭제하지 못하도록 방지하려면 AllowDeletingBrowserHistory를 false로 설정합니다.

```
 "AllowDeletingBrowserHistory":
    {
        "value": false
    },
```

4. 사용자의 시크릿 모드 액세스 권한을 끄려면 IncognitoModeAvailability를 1로 설정합니다.

```
"IncognitoModeAvailability":
    {
        "value": 1
    }
```

5. 다음 정책을 사용하여 Okta 플러그인을 설정하고 적용합니다.

- ExtensionSettings – 브라우저 시작 시 확장 프로그램을 설치합니다. 확장 프로그램 값은 Okta 플러그인 도움말 페이지에서 확인할 수 있습니다.

- `ExtensionInstallBlocklist` – 특정 확장 프로그램이 설치되지 않도록 방지합니다. * 값을 사용하면 기본적으로 모든 확장 프로그램을 방지할 수 있습니다. 관리자는 `ExtensionInstallAllowlist`에서 허용할 확장을 제어할 수 있습니다.
- `ExtensionInstallAllowlist`를 통해 특정 확장 프로그램을 설치하도록 허용할 수 있습니다. `ExtensionInstallBlocklist`를 *로 설정했으므로 Okta 플러그인 값을 여기에 추가하여 허용합니다.

Okta 플러그인을 켜기 위한 예시 정책은 다음과 같습니다.

```
"ExtensionInstallBlocklist": {
    "value": [
        "*",
        ]
},
"ExtensionInstallAllowlist": {
    "value": [
        "glnpjglilkicbckjpbgcfkogebgllemb",
       ]
},
"ExtensionSettings": {
    "value": {
        "glnpjglilkicbckjpbgcfkogebgllemb": {
            "installation_mode": "force_installed",
            "update_url": "https://clients2.google.com/service/update2/crx",
            "toolbar_pin": "force_pinned"
    }
}
```

5단계: 정책 JSON 파일을 웹 포털에 업로드

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. WorkSpaces 보안 브라우저를 선택한 다음 웹 포털을 선택합니다.
3. 웹 포털을 선택한 다음 편집을 선택합니다.
4. 정책 설정을 선택한 다음 JSON 파일 업로드를 선택합니다.
5. 파일 선택을 선택합니다. JSON 파일을 찾아 선택하고 업로드합니다.

6. 저장을 선택합니다.

기본 브라우저 정책을 편집합니다.

서비스를 제공하기 위해 WorkSpaces Secure Browser는 모든 포털에 기본 브라우저 정책을 적용합니다. 이 기본 정책은 콘솔 보기 또는 JSON 업로드에서 지정하는 정책 외에도 적용됩니다. 다음은 서비스에서 JSON 형식으로 적용한 정책 목록입니다.

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

고객은 다음 정책을 변경할 수 없습니다.

- `DefaultDownloadDirectory` – 이 정책은 편집할 수 없습니다. 서비스는 이 정책의 모든 변경 사항을 덮어씁니다.

- `DownloadDirectory` – 이 정책은 편집할 수 없습니다. 서비스는 이 정책의 모든 변경 사항을 덮어씁니다.

고객은 웹 포털에서 다음 정책을 업데이트할 수 있습니다.

- `DownloadRestrictions` – 기본값은 Chrome Safe Browsing에서 악성으로 식별된 다운로드를 방지하도록 `1`로 설정되어 있습니다. 자세한 내용은 사용자가 유해한 파일을 다운로드하지 못하도록 방지 섹션을 참조하십시오. 이 값을 `0` 또는 `4`로 설정할 수 있습니다.
- `URLAllowlist` 및 `URLBlocklist` 정책은 콘솔 보기 URL 필터링 기능이나 JSON 업로드를 사용하여 확장할 수 있습니다. 하지만 기본 URL은 덮어쓸 수 없습니다. 웹 포털에서 다운로드한 JSON 파일에서는 이러한 정책을 볼 수 없습니다. 하지만 세션 중에 'chrome://policy'를 방문하면 적용된 정책이 원격 브라우저에 표시됩니다.

입력 방법 편집기(IME) 구성

입력 방법 편집기(IME)는 최종 사용자에게 QWERTY 키보드 이외의 키보드 레이아웃을 사용하는 언어로 텍스트를 입력할 수 있는 옵션을 제공하는 유틸리티입니다. IME는 사용자가 일본어, 중국어, 한국어와 같이 더 크고 복잡한 언어 세트를 사용하는 언어로 텍스트를 입력할 수 있도록 도와줍니다. WorkSpaces 보안 브라우저 세션에는 기본적으로 IME 지원이 포함됩니다. 사용자는 세션의 IME 도구 모음에서 또는 키보드 단축키를 사용하여 대체 언어를 선택할 수 있습니다.

현재 WorkSpaces 보안 브라우저의 IME에서 지원되는 언어는 다음과 같습니다.

- 영어
- 중국어 간체(병음)
- 중국어 번체 (주음부호)
- 일본어
- 한국어

IME 도구 모음에서 언어를 선택하려면 다음을 수행합니다.

1. 검은색 상단 패널 표시줄의 오른쪽에 있는 언어 선택기 드롭다운을 선택합니다. 기본적으로 선택기에는 영어의 경우 en이라고 표시됩니다.
2. 드롭다운 메뉴에서 원하는 언어를 선택합니다.
3. 언어를 선택한 후 나타나는 하위 메뉴에서 추가 언어 세부 정보를 선택합니다.

키보드 단축키로 언어를 선택하려면 다음을 사용합니다.

- 모든 IME
  - IME를 앞쪽으로 돌리거나 오른쪽 키보드 레이아웃으로 이동하려면 Shift+Control+Left Alt 키를 누릅니다.
- 일본어
  - 히라가나를 선택하려면 F6 키를 누릅니다.
  - 가타카나를 선택하려면 F7 키를 누릅니다.
  - 라틴어를 선택하려면 F10 키를 누릅니다.
  - 와이드 라틴어를 선택하려면 F9 키를 누릅니다.
  - 직접 입력을 선택하려면 Alt +, Alt+@, Zenkaku Hankaku를 누릅니다.
- 한국어
  - 한국어를 선택하려면 Shift+Space 키를 누릅니다.
  - 한자를 선택하려면 F9 키를 누릅니다.

IME 툴바 및 메뉴를 제거하거나 WorkSpaces Secure Browser 세션에서 온스크린 키보드를 끄려면 다음으로 문의하십시오 AWS Support.

세션 내 로컬라이제이션 구성

사용자가 세션을 시작하면 WorkSpaces Secure Browser는 사용자의 로컬 브라우저 언어 및 시간대 설정을 감지하여 세션에 적용합니다. 이는 세션 중 표시 언어에 영향을 미치므로 표시된 시간이 사용자 위치의 현재 시간과 일치하는지 확인하는 데 도움이 됩니다.

다음 목록은 WorkSpaces Secure Browser에서 현재 지원하는 언어 코드를 보여줍니다. 사용자의 로컬 브라우저가 지원되지 않는 언어 코드를 사용하도록 설정된 경우 세션은 기본적으로 영어(en-US)로 설정됩니다.

- 독일어
  - de – 독일어
  - de-AT – 독일어(오스트리아)
  - de-DE – 독일어(독일)
  - de-CH – 독일어(스위스)
  - de-LI – 독일어(리히텐슈타인)

- 영어
  - en – 영어
  - en-AU – 영어(호주)
  - en-CA – 영어(캐나다)
  - en-IN – 영어(인도)
  - en-NZ – 영어(뉴질랜드)
  - en-ZA – 영어(남아프리카)
  - en-GB – 영어(영국)
  - en-US – 영어(미국)
- 스페인어
  - es – 스페인어
  - es-AR – 스페인어(아르헨티나)
  - es-CL – 스페인어(칠레)
  - es-CO – 스페인어(콜롬비아)
  - es-CR – 스페인어(코스타리카)
  - es-HN – 스페인어(온두라스)
  - es-419 – 스페인어(남미)
  - es-MX – 스페인어(멕시코)
  - es-PE – 스페인어(페루)
  - es-ES – 스페인어(스페인)
  - es-US – 스페인어(미국)
  - es-UY – 스페인어(우루과이)
  - es-VE – 스페인어(베네수엘라)
- 프랑스어
  - fr – 프랑스어
  - fr-CA – 프랑스어(캐나다)
  - fr-FR – 프랑스어(프랑스)
  - fr-CH – 프랑스어(스위스)
- 인도네시아어
  - id – 인도네시아어

  - id-ID – 인도네시아어(인도네시아)
- 이탈리아어
  - it – 이탈리아어
  - it-IT – 이탈리아어(이탈리아)
  - it-CH – 이탈리아어(스위스)
- 일본어
  - ja – 일본어
  - ja-JP – 일본어(일본)
- 한국어
  - ko – 한국어
  - ko-KR – 한국어(한국)
- 포르투갈어
  - pt – 포르투갈어
  - pt-BR – 포르투갈어(브라질)
  - pt-PT – 포르투갈어(포르투갈)
- 중국어
  - zh – 중국어
  - zh-CN – 중국어(중국)
  - zh-HK – 중국어(홍콩)
  - zh-TW – 중국어(대만)

세션 언어는 다음과 같은 우선 순위에 따라 결정됩니다.

1. 웹 포털의 브라우저 설정에 있는 ForcedLanguages정책. 자세한 내용은 ForcedLanguages를 참조하세요.
2. 최종 사용자의 로컬 브라우저 언어 설정.
3. 기본값(영어(en-US)).

시간대는 최종 사용자의 브라우저에 지정된 현지 시간대 설정에 따라 결정됩니다. 표준 시간대 설정이 유효하지 않은 경우 UTC가 사용됩니다.

WorkSpaces 보안 브라우저의 다음 구성 요소는 현지화를 지원합니다.

- WorkSpaces 보안 브라우저 로그인 페이지
- WorkSpaces Secure Browser 포털 상태 메시지 (메시지 로드 및 오류 포함)
- Chrome 브라우저
- 시스템 컨텍스트 메뉴 및 다른 이름으로 저장 창

사용자의 로컬 브라우저 설정을 지정하려면 다음 중 하나를 수행합니다.

- Chrome에서 설정을 선택하고 언어를 선택한 다음 기본 설정에 따라 언어를 정렬합니다.
- Firefox에서 설정, 일반, 언어를 선택하고 드롭다운 메뉴에서 언어를 선택합니다.
- Edge에서 설정을 선택하고 언어를 선택한 다음 기본 설정에 따라 언어를 정렬합니다.

IP 액세스 제어 설정(선택 사항)

WorkSpaces 보안 브라우저를 사용하면 웹 포털에 액세스할 수 있는 IP 주소를 제어할 수 있습니다. IP 액세스 설정을 사용하면 신뢰할 수 있는 IP 주소 그룹을 정의 및 관리하고, 사용자가 신뢰할 수 있는 네트워크에 연결된 경우에만 포털에 액세스하도록 허용할 수 있습니다.

기본적으로 WorkSpaces Secure Browser에서는 사용자가 어디서나 웹 포털에 액세스할 수 있습니다. IP 액세스 제어 그룹은 사용자가 웹 포털에 연결하는 데 사용할 수 있는 IP 주소를 필터링하는 가상 방화벽 역할을 합니다. 웹 포털과 연결된 경우 IP 액세스 설정은 인증 전에 사용자 IP를 탐지하여 연결 가능 여부를 결정합니다. 일단 연결되면 WorkSpaces Secure Browser는 사용자의 IP 주소를 지속적으로 모니터링하여 사용자가 신뢰할 수 있는 네트워크에서 연결 상태를 유지하는지 확인합니다. 사용자의 IP가 변경되면 WorkSpaces Secure Browser가 해당 세션을 감지하고 종료합니다.

CIDR 주소 범위를 지정하려면 IP 액세스 제어 그룹에 규칙을 추가한 다음 그룹을 웹 포털과 연결합니다. 각 IP 액세스 설정을 하나 이상의 웹 포털과 연결할 수 있습니다. 신뢰할 수 있는 네트워크의 퍼블릭 IP 주소 및 IP 주소 범위를 지정하려면 IP 액세스 제어 그룹에 규칙을 추가합니다. 사용자가 NAT 게이트웨이 또는 VPN을 통해 웹 포털에 액세스하는 경우에는 NAT 게이트웨이 또는 VPN에 대한 퍼블릭 IP 주소에서 트래픽을 허용하는 규칙을 생성해야 합니다.

> **Note**
>
> 고객은 보안 브라우저를 사용할 때 발생할 수 있는 잠재적인 법적 문제를 이해할 책임이 있으며 WorkSpaces 보안 브라우저를 사용할 때 모든 관련 법률 및 규정을 준수하는지 확인해야 합니다. WorkSpaces 여기에는 애플리케이션 내에서 수행되는 활동을 포함하여 고용주가 직원의 WorkSpaces 보안 브라우저 사용을 모니터링할 수 있는 권한을 규제하는 법률이 포함됩니다.

IP 액세스 제어 그룹 생성

IP 액세스 제어 그룹을 생성하려면 다음 단계를 따릅니다.

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. 탐색 창에서 IP 액세스 제어를 선택합니다.
3. IP 액세스 제어 그룹 생성을 선택합니다.
4. IP 액세스 제어 그룹 생성 대화 상자에서 그룹의 이름(필수)과 설명(선택 사항)을 입력합니다.
5. 소스에 연결할 IP 주소 또는 CIDR IP 범위와 설명(선택 사항)을 입력합니다.
6. 태그에서 각 IP 액세스 제어 그룹의 키 값 쌍을 태그할지 여부를 선택합니다.
7. 규칙 및 태그 추가를 완료하면 저장을 선택합니다.

IP 액세스 설정의 웹 포털 연결

IP 액세스 제어 그룹을 기존 웹 포털에 연결하려면 다음 단계를 따릅니다.

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. 탐색 창에서 웹 포털을 선택합니다.
3. 웹 포털을 선택하고 편집을 선택합니다.
4. IP 액세스 제어 그룹에서 웹 포털의 IP 액세스 제어 그룹을 선택합니다.
5. 저장을 선택합니다.

새 웹 포털 생성 시 IP 액세스 제어 그룹을 연결하려면 다음 단계를 따릅니다.

1. IP 액세스 제어에 액세스하려면 the section called “포털 설정 구성”의 1~4단계를 완료합니다(선택 사항).
2. IP 액세스 제어 생성을 선택합니다.
3. IP 그룹 생성 대화 상자에서 그룹의 이름(필수)과 설명(선택 사항)을 입력합니다.
4. 소스에 연결할 IP 주소 또는 CIDR IP 범위와 설명(선택 사항)을 입력합니다.
5. 태그에서 각 IP 액세스 제어 그룹의 키 값 쌍을 태그할지 여부를 선택합니다.
6. 규칙과 태그를 모두 추가했으면 IP 액세스 제어 생성을 선택합니다.
7. 실행 시 IP 액세스 제어 그룹이 이 웹 포털에 연결됩니다.

IP 액세스 제어 그룹 편집

언제든지 IP 액세스 설정에서 규칙을 삭제할 수 있습니다. 웹 포털에 대한 연결을 허용하는 데 사용된 규칙을 제거하면 현재 세션에 있는 모든 사용자의 웹 포털 연결이 끊어집니다.

IP 액세스 제어 그룹을 편집하려면 다음 단계를 따릅니다.

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. 탐색 창에서 IP 액세스 제어를 선택합니다.
3. 그룹을 선택하고 편집을 선택합니다.
4. 기존 규칙 소스 및 설명(선택 사항)을 편집하거나 규칙을 추가합니다.
5. 태그에서 각 IP 액세스 제어 그룹의 키 값 쌍을 태그할지 여부를 선택합니다.
6. 규칙 및 태그 추가를 완료하면 저장을 선택합니다.
7. 기존 IP 액세스 설정을 업데이트한 경우 새 규칙 또는 편집된 규칙이 적용될 때까지 최대 15분 정도 걸립니다.

IP 액세스 제어 그룹 삭제

언제든지 IP 액세스 제어 그룹에서 규칙을 삭제할 수 있습니다. 웹 포털에 대한 연결을 허용하는 데 사용된 규칙을 제거하면 현재 세션에 있는 모든 사용자의 웹 포털 연결이 끊어집니다.

IP 액세스 제어 그룹을 삭제하려면 다음 단계를 따릅니다.

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. 탐색 창에서 IP 액세스 제어 그룹을 선택합니다.
3. 그룹을 선택하고 삭제를 선택합니다.

Single Sign-On용 확장 프로그램 활성화(선택 사항)

최종 사용자가 더 나은 포털 로그인을 경험할 수 있도록 확장 프로그램을 활성화할 수 있습니다. 예를 들어 Okta를 포털의 SAML 2.0 ID 제공업체(IdP)로 사용하고 세션 중에 사용자가 방문할 웹 사이트의 IdP로도 사용하는 경우에는 확장 프로그램을 사용하여 Okta 로그인 쿠키를 세션에 전달할 수 있습니다. 이후 사용자가 Okta 도메인 쿠키가 필요한 웹 사이트를 방문하면 세션 중에 로그인하지 않고도 웹 사이트에 액세스할 수 있습니다.

Chrome 및 Firefox 브라우저에서는 확장 프로그램이 지원됩니다. 확장 프로그램을 사용하면 사용자가 세션에 로그인할 때 허용된 도메인의 쿠키를 동기화할 수 있습니다. 확장 프로그램은 사용자 로그인을 필요로 하지 않으며 설치 후 사용자가 별도의 조치를 취하지 않아도 쿠키 동기화가 가능하도록 백그라운드에서 작동합니다. 확장 프로그램에는 데이터가 저장되지 않습니다.

포털에 로그인하면 확장 프로그램을 설치하라는 메시지가 표시됩니다.

Chrome의 시크릿 창 또는 Firefox 사생활 보호 브라우징 창에서는 기본적으로 확장 프로그램이 활성화되지 않습니다. 사용자가 수동으로 활성화할 수 있습니다. Chrome에 대한 자세한 내용은 시크릿 모드의 확장 프로그램을 참조하세요. Firefox에 대한 자세한 내용은 사생활 보호 모드의 확장 프로그램을 참조하십시오.

포털의 기존 사용자 설정 구성은 업데이트할 수 있으며, 웹 포털을 처음 생성할 때에도 업데이트할 수 있습니다. 먼저 SAML IdP 및 웹 사이트에 필요한 도메인을 결정합니다. 최대 10개의 도메인을 추가할 수 있습니다.

쿠키를 동기화할 적절한 도메인을 테스트하고 식별하는 것은 사용자의 책임입니다. SSO(Single Sign-On)가 예상대로 작동하려면 IdP 또는 웹 사이트 인증 수준에서 변경이 필요할 수 있습니다.

가장 일반적인 IdP와 함께 사용할 도메인을 확인하려면 다음 표를 참조하십시오.

IdP 및 도메인

IdP	도메인
Okta	okta.com
엔트라 ID	microsoftonline.com
AWS Identity Center	awsapps.com
한 번의 로그인	onelogin.com
Duo	duosecurity.com

다음으로 콘솔에서 웹 포털을 방문하세요. 그런 다음 확장 프로그램을 허용하고 동기화할 도메인의 쿠키를 추가합니다. 아래 단계에 따라 확장 프로그램이 허용된 새 포털을 생성하거나 기존 포털을 업데이트합니다.

새 웹 포털을 생성할 때 확장 프로그램을 허용하려면 다음 단계를 따릅니다.

1. the section called “사용자 설정 구성”에 도달할 때까지 the section called “1단계: 웹 포털 생성”의 단계를 따릅니다.
2. the section called “사용자 설정 구성”의 1단계 중 사용자 권한에서 허용됨을 선택하여 웹 포털의 확장 프로그램을 활성화합니다.
3. 쿠키 동기화를 위한 도메인을 입력하고 새 도메인 추가를 선택합니다.
4. the section called “사용자 설정 구성”의 단계와 the section called “1단계: 웹 포털 생성”의 나머지 섹션을 완료하여 웹 포털을 생성합니다.

기존 웹 포털에 확장 프로그램을 추가하려면 다음 단계를 따릅니다.

1. https://console.aws.amazon.com/workspaces-web/home 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다.
2. 편집할 웹 포털을 선택합니다.
3. 사용자 설정, 사용자 권한, 허용됨을 선택하여 웹 포털의 확장 프로그램을 활성화합니다.
4. 쿠키 동기화를 위한 도메인을 입력하고 새 도메인 추가를 선택합니다.
5. 포털 변경 내용을 저장합니다. 15분 이내에 포털에서 확장 프로그램을 설치하라는 메시지가 표시됩니다.

도메인을 편집하거나 확장 프로그램을 제거하려면 다음 단계를 따릅니다.

1. https://console.aws.amazon.com/workspaces-web/home 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다.
2. 편집할 웹 포털을 선택합니다.
3. 사용자 설정, 사용자 권한, 허용되지 않음을 선택하여 웹 포털의 확장 프로그램을 제거합니다.
4. 개별 도메인을 제거하거나 편집합니다.
5. 일단 제거되면 사용자의 브라우저에 WorkSpaces Secure Browser 확장 프로그램이 설치되어 있더라도 세션은 더 이상 쿠키를 동기화하지 않습니다.

확장 프로그램의 사용자 경험에 대한 자세한 내용은 the section called “Single Sign-On을 위한 확장 프로그램” 섹션을 참조하십시오.

URL 필터링 설정

Chrome 정책을 사용하여 사용자가 원격 브라우저에서 액세스할 수 있는 URL을 필터링할 수 있습니다. Chrome 정책에서는 URL을 필터링하는 두 가지 메커니즘, 즉 URL 허용 목록과 URL 차단 목록을 제공합니다. WorkSpaces 보안 브라우저 콘솔 인터페이스를 사용하여 URL 필터링을 포털 설정으로 구성하거나 사용자 지정 JSON 문의 일부로 추가 (인라인 편집기에서 또는 JSON 파일 업로드) 할 수 있습니다.

콘솔을 사용하여 URL 필터링을 설정하려면

1. 에서 WorkSpaces 보안 브라우저 콘솔을 엽니다https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. WorkSpaces 보안 브라우저, 웹 포털을 선택하고 웹 포털을 선택한 다음 세부 정보 보기를 선택합니다.
3. URL 필터링의 경우 다음 옵션 중에서 선택하십시오.

   - 모든 URL에 대한 접근 허용: 기본적으로 웹 포털은 모든 URL에 대한 접근을 허용합니다. 특정 웹 사이트를 BlockURL 목록에 추가하여 세션 중에 사용자가 해당 사이트를 방문하지 못하도록 할 수 있습니다. 예를 들어, www.anycorp.com을 차단URL 목록에 추가하면 사용자가 세션 중에 www.anycorp.com으로 이동할 수 없게 됩니다.
   - 모든 URL에 대한 액세스 차단: 기본적으로 웹 포털은 모든 URL에 대한 액세스를 차단합니다. URL 허용 목록에 특정 웹 사이트를 추가하여 사용자가 방문할 수 있는 웹 사이트 목록을 관리하고 다른 웹 사이트로 들어오는 트래픽을 차단할 수 있습니다. 세션 중에 사용자가 원클릭으로 액세스할 수 있도록 각 URL을 북마크로 추가하는 것을 고려해 보세요.
   - 고급 구성: AllowUrl 및 BlockURL 목록을 병렬로 만들려면 이 옵션을 선택합니다. URL 허용 목록이 URL 차단 목록보다 우선합니다. 이 옵션은 경로별 URL 필터링을 활성화합니다. 예를 들어 www.anycorp.com을 차단 목록에 추가한 다음 www.anycorp.com/hr을 허용 목록에 추가할 수 있습니다. 이렇게 하면 사용자가 www.anycorp.com/hr을 방문할 수는 있지만 www.anycorp.com/finance와 같은 다른 URL 경로에는 액세스할 수 없습니다.

URL 차단 및 허용 사용에 대한 자세한 지침은 웹 사이트 액세스 허용 또는 차단을 참조하십시오. 최상의 결과를 얻으려면 Chrome의 차단 목록 필터 형식에 따라 이 목록에 URL을 추가하세요. 자세한 내용은 URL 차단 목록 필터 형식을 참조하십시오.

JSON 편집기 또는 파일 업로드를 사용하여 URL 필터링을 설정하려면

1. 정책 설정 모듈에서 JSON 편집기를 선택하고 콘솔 UI 모듈을 사용하지 않고 편집기 또는 파일 업로드 보기를 사용할 수 있습니다.

   - 에디터를 사용하면 고객이 콘솔에서 사용자 지정 정책 설명을 인라인으로 생성할 수 있습니다. 편집기는 정책 생성 중 JSON 명령문의 오류를 강조 표시합니다.
   - 파일 업로드를 통해 고객은 콘솔 외부에서 만든 JSON 파일 (예: 기존 Chrome 브라우저에서 내보낸 파일) 을 추가할 수 있습니다.
2. 웹 포털의 허용/거부 URL 목록의 형식을 올바르게 지정하려면 URL 허용 목록 및 URL 차단 목록에 대한 Chrome 정책 세부정보를 참조하십시오. 자세한 내용은 URL 허용 목록 및 URL 차단 목록을 참조하십시오.

딥링크 허용 (선택 사항)

사용자가 WorkSpaces Secure Browser에 로그인하면 관리자가 설정한 홈 페이지에서 세션을 시작합니다. 세션 중에 사용자를 특정 웹사이트로 연결하는 딥링크를 포털이 수신하도록 허용할 수도 있습니다. 딥링크를 선택하면 딥링크에 지정된 URL이 포털에 표시됩니다. 링크는 세션 시작을 위해 구성된 홈페이지와 함께 표시되거나 세션이 이미 진행 중인 경우 단독으로 표시됩니다. 이 기능을 통해 관리자는 WorkSpaces Secure Browser를 사용하여 보다 동적인 사용자 경험을 만들 수 있습니다. 딥링크에 대한 권한을 허용하려면 사용자 설정을 만들 때 허용을 선택합니다. 자세한 정보는 the section called “사용자 설정 구성”을 참조하세요.

딥링크는 WorkSpaces 보안 브라우저 세션에서 페이지를 엽니다. 세션이 이미 실행 중인 경우 새 탭에서 딥링크가 열립니다. 세션이 아직 실행되고 있지 않은 경우 새 탭에서 딥링크 URL이 열리고 포털 기본 홈페이지가 별도의 탭에서 열립니다. 딥링크에 URL이 두 개 이상 포함된 경우 딥링크 URL이 첫 번째로 포커스가 표시되고, 이후의 각 URL (기본 홈페이지 포함) 이 별도의 탭에 열립니다.

딥링크는 다음 요구 사항을 충족해야 합니다.

- 포털의 딥링크 권한이 허용으로 설정되어 있어야 합니다. 자세한 정보는 the section called “사용자 설정 구성”을 참조하세요.
- 딥링크로 연결하려는 사이트는 URL로 인코딩되어야 합니다. 예를 들어 사용자를 “https://www.example.com/?query=true”에 연결하려면 링크를 https%3A%2F%2fwww.example.com%2F%3fQuery%3Dtrue로 업데이트하십시오.
- 허용 목록에 있는 포털 URL에 다음 형식으로 URL을 추가합니다. 여기서 UUID는 포털 ID입니다.

  <uuid>https://.workspaces-web.com/? DeepLinks=https%3a%2f%2f%2fwww.example.com%2F%3fQuery%3DTrue

- 딥링크는 쉼표로 구분된 URL을 최대 10개까지 포함할 수 있습니다. 예:

  <uuid>https://.workspaces-web.com/? DeepLinks=https%3a%2f%2fwww.example.com%2f%3fQuery%3dTrue, https%3a%2f%2f%2fwww.example.com%2fQuery%3dTrue2, https%3a%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%2f%3fQuery%3DTrue3, https%3a%2f%2fwww.example.com%2f%3fQuery%3dTrue4

이 포털 링크를 공유하는 모든 사용자는 딥링크 값을 조작하여 웹사이트를 방문할 수 있습니다. 단, 포털에서 URL 차단 목록에 없는 도메인에 도달할 수 있는 경우 말입니다. 사용자가 포털을 통해 의도하지 않은 도메인을 방문하지 못하도록 제한적인 허용 목록 또는 차단 목록을 만들려면 URL 필터링을 사용하세요. 포털의 브라우저 설정에서 URL 필터링을 사용하여 포털의 허용 목록 및 차단 목록을 편집할 수 있습니다. 자세한 내용은 웹 사이트 접근 허용 또는 차단을 참조하십시오the section called “URL 필터링 설정”.

Amazon 보안 브라우저의 WorkSpaces 보안

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

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

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

이 설명서는 Amazon WorkSpaces Secure Browser를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표를 충족하도록 Amazon WorkSpaces Secure Browser를 구성하는 방법을 보여줍니다. 또한 Amazon WorkSpaces Secure Browser 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

내용

- Amazon WorkSpaces 보안 브라우저에서의 데이터 보호
- Amazon WorkSpaces 보안 브라우저용 Identity 및 Access Management
- Amazon WorkSpaces 보안 브라우저에서의 사고 대응
- Amazon WorkSpaces 보안 브라우저의 규정 준수 검증
- Amazon WorkSpaces 보안 브라우저의 레질리언스
- Amazon 보안 브라우저의 인프라 WorkSpaces 보안
- Amazon WorkSpaces 보안 브라우저의 구성 및 취약성 분석
- Amazon 보안 브라우저의 WorkSpaces 보안 모범 사례

Amazon WorkSpaces 보안 브라우저에서의 데이터 보호

AWS 공동 책임 모델 공동 책임 모델 이 모델에 설명된 대로 AWS 는 모든 모델을 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 공동 책임 모델 및AWS 보안 GDPR 블로그의 블로그 게시물을 참조하십시오.

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

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSLTLS/를 사용하여 AWS 리소스와 통신하세요. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- API를 사용하여 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API an을 AWS 통해 액세스할 때 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 () 140-3을 참조하십시오. FIPS

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS CLI, 또는 를 AWS 서비스 사용하여 WorkSpaces Secure Browser 또는 기타 장치로 작업하는 경우가 포함됩니다. AWS SDKs 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL a를 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다.

데이터 암호화

Amazon WorkSpaces Secure Browser는 브라우저 설정, 사용자 설정, 네트워크 설정, ID 공급자 정보, 신뢰 저장소 데이터, 신뢰 저장소 인증서 데이터와 같은 포털 사용자 지정 데이터를 수집합니다. WorkSpaces 또한 Secure Browser는 브라우저 정책 데이터, 사용자 기본 설정 (브라우저 설정

용) 및 세션 로그를 수집합니다. 수집된 데이터는 아마존 DynamoDB 및 아마존 S3에 저장됩니다. WorkSpaces 보안 브라우저는 AWS Key Management Service 암호화에 사용합니다.

콘텐츠를 보호하려면 다음 지침을 따릅니다.

- 최소 권한 액세스를 구현하고 WorkSpaces 보안 브라우저 작업에 사용할 특정 역할을 생성합니다. IAM템플릿을 사용하여 전체 접근 역할 또는 읽기 전용 역할을 생성합니다. 자세한 내용은 AWS WorkSpaces 보안 브라우저에 대한 관리형 정책 단원을 참조하십시오.
- WorkSpaces Secure Browser가 사용자가 제공한 키로 저장된 데이터를 암호화할 수 있도록 고객 관리 키를 제공하여 데이터를 종단간 보호하십시오.
- 포털 도메인과 사용자 보안 인증 정보를 공유할 때는 주의해야 합니다.
  - 관리자는 Amazon WorkSpaces 콘솔에 로그인하고 사용자는 WorkSpaces 보안 브라우저 포털에 로그인해야 합니다.
  - 인터넷상의 모든 사용자가 웹 포털에 접근할 수 있지만, 포털에 대한 유효한 사용자 보안 인증 정보가 없으면 세션을 시작할 수 없습니다.
- 사용자는 세션 종료를 선택하여 세션을 명시적으로 종료할 수 있습니다. 이렇게 하면 브라우저 세션을 호스팅하는 인스턴스가 삭제되고 브라우저가 격리됩니다.

WorkSpaces Secure Browser는 기본적으로 모든 민감한 데이터를 로 암호화하여 콘텐츠와 메타데이터를 보호합니다. AWS KMS브라우저 정책 및 사용자 기본 설정을 수집하여 WorkSpaces Secure Browser 세션 중에 정책 및 설정을 적용합니다. 기존 설정을 적용하는 중 오류가 발생하는 경우 사용자는 새 세션에 액세스할 수 없으며 회사 내부 사이트 및 SaaS 애플리케이션에도 액세스할 수 없습니다.

저장 중 암호화

저장 중 암호화는 기본적으로 구성됩니다. WorkSpaces Secure Browser에서 사용되는 고객별 데이터는 를 사용하여 암호화됩니다. AWS KMS WorkSpaces Secure Browser는 사용자가 생성한 리소스에 대해 저장 시 암호화를 제공합니다. 서비스는 리소스 생성 시 AWS KMS 고객 관리 키를 수락하며, 고객 관리 키가 제공되지 않는 경우 AWS 소유 키를 사용하여 저장된 리소스를 암호화합니다. 해당 서비스는 브라우저 세션을 사용자 지정하기 위해 제공할 수 있는 브라우저 정책 문서와 ID 제공업체 구성, 포털의 표시 이름을 암호화합니다. 이 정보는 백엔드에 저장되는 동안 고객 관리 키 또는 AWS 소유 키를 사용하여 암호화된 상태로 유지됩니다.

WorkSpaces 보안 브라우저 리소스를 생성할 때 사용할 키를 결정할 수 있습니다. 해당 리소스의 일부인 데이터가 암호화된 경우 WorkSpaces Secure Browser는 해당 `customerManagedKeyArn` 필드를 암호화의 일부로 `create` API 받아들입니다. 제공된 키는 대칭 AWS KMS 키여야 하며, 이 키를 사용하여 리소스를 생성하는 관리자는 `kms:Decrypt`, `kms:GenerateDataKey`, `kms:CreateGrant`

권한을 가지고 있어야 합니다. 해당 키를 사용하여 리소스를 생성한 후에는 키를 제거하거나 변경할 수 없습니다. 고객 관리형 키를 사용한 경우에는 리소스에 액세스하는 관리자에게 `kms:Decrypt` 및 `kms:GenerateDataKey` 권한이 있어야 합니다. 콘솔을 사용하는 동안 액세스가 거부되었다는 오류가 표시되면 콘솔을 사용하는 사용자에게 사용된 키와 해당 권한이 있는지 확인합니다.

AWS KMS 권한 부여 상태를 확인하여 키 사용 문제를 해결하고 감사할 수 있습니다. 자세한 내용은 권한 부여 관리를 참조하십시오. 포털을 생성하는 동안 WorkSpaces Secure Browser는 서비스가 키에 비동기적으로 액세스할 수 있도록 권한을 생성합니다. 권한 부여 시 제공되는 암호화 컨텍스트 및 권한 부여 상황을 확인하여 키 사용 상태를 확인할 수 있습니다. 암호화 컨텍스트에는 항상 포털 ID와 동일한 값 및 `aws:workspaces-web:portal:id` 키를 갖춘 항목이 포함됩니다. 다른 리소스의 경우 암호화 컨텍스트에는 항상 형식 `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id`의 항목과 해당 리소스 ID가 포함됩니다.

전송 중 암호화

WorkSpaces 보안 브라우저는 전송 중인 데이터 및 1.2를 암호화합니다. HTTPS TLS 콘솔이나 직통 API 통화를 WorkSpaces 사용하여 요청을 보낼 수 있습니다. 전송되는 요청 데이터는 모두 HTTPS 또는 TLS 연결을 통해 전송되어 암호화됩니다. 요청 데이터는 AWS 콘솔에서 또는 AWS SDK WorkSpaces 보안 브라우저로 전송할 수 있습니다. AWS Command Line Interface

전송 중 암호화는 기본적으로 구성되며 보안 연결 (HTTPS,TLS) 은 기본적으로 구성됩니다.

키 관리

자체 고객 관리 AWS KMS 키를 제공하여 고객 정보를 암호화할 수 있습니다. 키를 제공하지 않으면 WorkSpaces Secure Browser는 AWS 소유 키를 사용합니다. 를 사용하여 키를 설정할 수 있습니다 AWS SDK.

인터네트워크 트래픽 개인 정보 보호

Secure Browser와 온프레미스 애플리케이션 간의 WorkSpaces 연결을 보호하려면 WorkSpaces Secure Browser를 사용하여 자체 브라우저 세션을 실행해야 합니다. VPC 온프레미스 애플리케이션에 대한 연결은 사용자가 직접 구성하며 Secure VPC Browser를 통해 제어되지 않습니다. WorkSpaces

계정 간 연결을 보호하기 위해 WorkSpaces Secure Browser는 서비스 연결 역할을 사용하여 고객 계정에 안전하게 연결하고 고객을 대신하여 작업을 실행합니다. 자세한 내용은 보안 브라우저용 WorkSpaces 서비스 연결 역할 사용 단원을 참조하십시오.

사용자 액세스 로깅

관리자는 시작, 중지 및 URL 방문을 비롯한 WorkSpaces Secure Browser 세션 이벤트를 기록할 수 있습니다. 이러한 로그는 암호화되어 Amazon Kinesis 데이터 스트림을 통해 고객에게 안전하게 전달됩니다. 사용자 액세스 로깅의 검색 정보는 로깅이 구성되지 않은 세션에서 저장되거나 세션에서 사용할 수 없습니다. AWS URL시크릿 모드의 방문이나 브라우저 URLs 기록에서 삭제된 방문은 사용자 액세스 로깅에 기록되지 않습니다.

Amazon WorkSpaces 보안 브라우저용 Identity 및 Access Management

AWS Identity and Access Management (IAM) 는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM관리자는 WorkSpaces Secure Browser 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM추가 비용 없이 사용할 AWS 서비스 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- Amazon WorkSpaces 보안 브라우저의 작동 방식 IAM
- Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제
- AWS WorkSpaces 보안 브라우저에 대한 관리형 정책
- Amazon WorkSpaces 보안 브라우저 ID 및 액세스 문제 해결
- 보안 브라우저용 WorkSpaces 서비스 연결 역할 사용

고객

AWS Identity and Access Management (IAM) 사용 방법은 WorkSpaces 보안 브라우저에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - WorkSpaces Secure Browser 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 WorkSpaces 보안 브라우저 기능을 사용하여 작업을 수

행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. WorkSpaces 보안 브라우저의 기능에 액세스할 수 없는 경우 을 참조하십시오Amazon WorkSpaces 보안 브라우저 ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 WorkSpaces 보안 브라우저 리소스를 담당하는 경우 보안 브라우저에 WorkSpaces 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 사용자가 액세스해야 하는 WorkSpaces 보안 브라우저 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여의 기본 개념을 IAM 이해하십시오. 회사에서 WorkSpaces Secure IAM Browser를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오Amazon WorkSpaces 보안 브라우저의 작동 방식 IAM.

IAM관리자 - 관리자인 경우 IAM WorkSpaces Secure Browser에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다. 에서 IAM 사용할 수 있는 WorkSpaces 보안 브라우저 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM사용자로서 또는 역할을 위임하여 인증 (로그인 AWS) 을 받아야 합니다. AWS 계정 루트 사용자 IAM

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 페더레이션을 AWS 사용하여 액세스하는 경우 간접적으로 역할을 수임하는 것입니다.

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

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 가 AWS 제공됩니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 사용 IAM설명서의 AWS API요청 서명을 참조하십시오.

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

AWS 계정 루트 사용자

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

페더레이션 자격 증명

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

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

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 AWS 계정 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. AWS IAM Identity Center 사용 설명서에서

IAM 사용자 및 그룹

IAM사용자란 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 ID입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 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 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지

고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 ID입니다. IAM사용자와 비슷하지만 특정인과 관련이 있는 것은 아닙니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI or AWS API 작업을 호출하거나 사용자 지정을 사용하여 역할을 수임할 수 URL 있습니다. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 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. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할 수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할이 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 교차 계정 리소스 액세스를 참조하십시오. IAM IAM
- 서비스 간 액세스 — 일부는 다른 기능을 AWS 서비스 사용합니다. AWS 서비스예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행

할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스
- 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon에서 실행 중인 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS API 요청을 보내는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. EC2인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 만들어야 합니다. 인스턴스 프로필에는 역할이 포함되며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

정책을 만들고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

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

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 에서 역할 정보를 가져올 수 AWS API 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

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

리소스 기반 정책

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

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 IAM 정책에서는 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

지원하는 서비스의 VPC 예로는 Amazon S3와 Amazon이 ACLs 있습니다. AWS WAF자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

AWS 일반적이지 않은 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 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는

권한은 객체의 자격 증명 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 내용은 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCPs) - SCPs 조직 또는 OU (조직 단위) 에 대한 최대 권한을 지정하는 JSON AWS Organizations정책입니다. AWS Organizations 기업이 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP AWS 계정 루트 사용자제한합니다. Organizations 및 SCPs 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하십시오.
- 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 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

Amazon WorkSpaces 보안 브라우저의 작동 방식 IAM

보안 브라우저를 IAM 사용하여 WorkSpaces 보안 브라우저에 대한 액세스를 관리하기 전에 WorkSpaces 보안 브라우저에서 사용할 수 있는 IAM 기능에 대해 알아보십시오.

IAMAmazon WorkSpaces 보안 브라우저와 함께 사용할 수 있는 기능

IAM기능	WorkSpaces 보안 브라우저 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예

IAM기능	WorkSpaces 보안 브라우저 지원
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	부분
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

WorkSpaces Secure Browser 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM사용 IAM 설명서에서 함께 작동하는AWS 서비스를 참조하십시오.

보안 브라우저에 대한 ID 기반 정책 WorkSpaces

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 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

보안 브라우저의 ID 기반 정책 예제 WorkSpaces

WorkSpaces Secure Browser ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

보안 브라우저 내의 리소스 기반 정책 WorkSpaces

리소스 기반 정책 지원: 아니요

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

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

WorkSpaces 보안 브라우저의 정책 조치

정책 작업 지원: 예

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

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 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 포함하십시오.

WorkSpaces 보안 브라우저 작업 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하십시오.

WorkSpaces 보안 브라우저의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
workspaces-web
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

WorkSpaces Secure Browser ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

보안 브라우저의 WorkSpaces 정책 리소스

정책 리소스 지원: 예

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

`Resource`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

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

WorkSpaces 보안 브라우저 리소스 유형 및 해당 ARNs 유형의 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Secure Browser에서 정의한 리소스를 참조하십시오. 각 리소스에 어떤 작업을 지정할 수 있는지 알아보려면 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하십시오. ARN

WorkSpaces 보안 브라우저 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

보안 브라우저의 WorkSpaces 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 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 대한 액세스 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

WorkSpaces 보안 브라우저 조건 키 목록을 보려면 서비스 인증 참조의 Amazon WorkSpaces Secure Browser의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하십시오.

WorkSpaces 보안 브라우저 ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

보안 브라우저의 WorkSpaces 액세스 제어 목록 (ACLs)

지원ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

보안 브라우저를 사용한 속성 기반 액세스 제어 () ABAC WorkSpaces

지원 ABAC (정책의 태그): 부분

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부

할 수 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에도 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.

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

보안 브라우저에서 임시 자격 증명 사용 WorkSpaces

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 AWS 서비스 방법을 비롯한 추가 정보는 IAM사용 설명서의 AWS 서비스 해당 자격 증명을 참조하십시오. IAM

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

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 AWS API 있습니다. 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

보안 브라우저에 대한 서비스 간 WorkSpaces 보안 주체 권한

순방향 액세스 세션 지원 (FAS): 예

에서 IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS

를 호출하는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

WorkSpaces 보안 브라우저의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스

> **Warning**
>
> 서비스 역할의 권한을 변경하면 WorkSpaces Secure Browser 기능이 손상될 수 있습니다. WorkSpaces Secure Browser가 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

보안 브라우저의 서비스 연결 역할 WorkSpaces

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 함께 작동하는 AWS 서비스를 참조하십시오. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Amazon WorkSpaces 보안 브라우저의 ID 기반 정책 예제

기본적으로 사용자와 역할에는 WorkSpaces 보안 브라우저 리소스를 생성하거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수도 없습니다 AWS API. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업

을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서에서 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 형식을 비롯하여 WorkSpaces Secure Browser에서 정의한 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 인증 참조의 Amazon WorkSpaces Secure Browser용 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- WorkSpaces 보안 브라우저 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

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

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM사용 설명서의 AWS 관리형 정책 또는 작업 기능에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사

례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM

- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 보안을 강화하려면 이 기능을 MFA 켜십시오. AWS 계정 API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하세요. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

WorkSpaces 보안 브라우저 콘솔 사용

Amazon WorkSpaces Secure Browser 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 WorkSpaces 보안 브라우저 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 AWS API 없습니다. 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자와 역할이 WorkSpaces 보안 브라우저 콘솔을 계속 사용할 수 있도록 하려면 WorkSpaces 보안 브라우저 `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 사용 설명서의 IAM사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 OR를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS API

```
{
    "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": "*"
        }
    ]
}
```

AWS WorkSpaces 보안 브라우저에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이러한 정책은 일반적인 사용 사례를 다루며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스가 새 기능을 지원하기 위해 AWS 관리형 정책에 권한을 추가하는 경우가 있습니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스

는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 `ReadOnlyAccess` AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하십시오.

AWS 관리형 정책: AmazonWorkSpacesWebServiceRolePolicy

`AmazonWorkSpacesWebServiceRolePolicy` 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 WorkSpaces Secure Browser가 사용자를 대신하여 작업을 수행하도록 허용하는 서비스 연결 역할에 연결됩니다. 자세한 정보는 the section called “서비스 연결 역할 사용”을 참조하세요.

이 정책은 WorkSpaces Secure Browser에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 허용하는 관리 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `workspaces-web`— WorkSpaces Secure Browser에서 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있습니다.
- `ec2` – 보안 주체가 VPC, 서브넷 및 가용 영역을 설명하고, 네트워크 인터페이스를 생성, 설명 및 삭제하고 네트워크 인터페이스에 태그를 지정하고, 주소를 연결하거나 연결 해제하고, 라우팅 테이블, 보안 그룹, VPC 엔드포인트를 설명할 수 있습니다.
- `CloudWatch` – 보안 주체가 지표 데이터를 입력할 수 있습니다.
- `Kinesis` – 보안 주체가 Kinesis 데이터 스트림의 요약을 설명하고 사용자 액세스 로깅을 위해 Kinesis 데이터 스트림에 레코드를 넣을 수 있습니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS 관리형 정책: AmazonWorkSpacesSecureBrowserReadOnly

AmazonWorkSpacesSecureBrowserReadOnly 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 AWS 관리 콘솔, SDK 및 CLI를 통해 WorkSpaces 보안 브라우저 및 해당 종속성에 액세스할 수 있는 읽기 전용 권한을 부여합니다. 인증 유형으로 IAM_Identity_Center를 사용하여 포털과 상호 작용하는 데 필요한 권한은 이 정책에 포함되지 않습니다. 이러한 권한을 얻으려면 이 정책을 AWSSSOReadOnly와 결합합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- workspaces-web— AWS 관리 콘솔, SDK 및 WorkSpaces CLI를 통해 보안 브라우저 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.
- ec2 - 보안 주체가 VPC, 서브넷, 보안 그룹을 설명하도록 허용합니다. 이 정보는 WorkSpaces 보안 브라우저의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 VPC, 서브넷 및 보안 그룹을 표시하는 데 사용됩니다.
- Kinesis - 보안 주체가 Kinesis 데이터 스트림을 나열할 수 있도록 허용합니다. WorkSpaces 보안 브라우저의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 Kinesis 데이터 스트림을 표시하는 데 사용됩니다.

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

```
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AmazonWorkSpacesWebReadOnly

`AmazonWorkSpacesWebReadOnly` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 AWS 관리 콘솔, SDK 및 CLI를 통해 WorkSpaces 보안 브라우저 및 해당 종속성에 액세스할 수 있는 읽기 전용 권한을 부여합니다. 인증 유형으로 `IAM_Identity_Center`를 사용하여 포털

과 상호 작용하는 데 필요한 권한은 이 정책에 포함되지 않습니다. 이러한 권한을 얻으려면 이 정책을 AWSSSOReadOnly와 결합합니다.

> **Note**
>
> 현재 이 정책을 사용하고 있다면 새 정책으로 전환하십시오.
> AmazonWorkSpacesSecureBrowserReadOnly

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- workspaces-web— AWS 관리 콘솔, SDK 및 WorkSpaces CLI를 통해 보안 브라우저 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.
- ec2 - 보안 주체가 VPC, 서브넷, 보안 그룹을 설명하도록 허용합니다. 이 정보는 WorkSpaces 보안 브라우저의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 VPC, 서브넷 및 보안 그룹을 표시하는 데 사용됩니다.
- Kinesis - 보안 주체가 Kinesis 데이터 스트림을 나열할 수 있도록 허용합니다. WorkSpaces 보안 브라우저의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 Kinesis 데이터 스트림을 표시하는 데 사용됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
```

```
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces 보안 브라우저에서 AWS 관리형 정책을 업데이트합니다.

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 WorkSpaces Secure Browser의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 사용 설명서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AmazonWorkSpacesSecureBrowserReadOnly - 새 정책	WorkSpaces 보안 브라우저는 AWS 관리 콘솔, SDK 및 CLI를 통해 WorkSpaces 보안 브라우저 및 해당 종속성에 대한 읽기	2024년 6월 24일

변경 사항	설명	날짜
	전용 액세스를 제공하는 새 정책을 추가했습니다.	
AmazonWorkSpacesWebServiceRolePolicy - 정책 업데이트	WorkSpaces 보안 브라우저는 aws:RequestTag/: true로 태그를 지정하고 서브넷 및 보안 그룹 리소스에서 CreateNetworkInterface 작동하도록 제한하고 awsWorkSpacesWebManaged:/: true로 태그가 지정된 ENI로만 DeleteNetworkInterface 제한하도록 정책을 업데이트했습니다. ResourceTag WorkSpacesWebManaged	2022년 12월 15일
AmazonWorkSpacesWebReadOnly - 정책 업데이트	WorkSpaces Secure Browser는 사용자 액세스 로깅에 대한 읽기 권한 및 Kinesis 데이터 스트림 목록을 포함하도록 정책을 업데이트했습니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.	2022년 11월 2일
AmazonWorkSpacesWebServiceRolePolicy - 정책 업데이트	WorkSpaces 보안 브라우저는 Kinesis 데이터 스트림의 요약을 설명하고 사용자 액세스 로깅을 위해 Kinesis 데이터 스트림에 레코드를 추가하도록 정책을 업데이트했습니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.	2022년 10월 17일

변경 사항	설명	날짜
AmazonWorkSpacesWebServiceRolePolicy - 정책 업데이트	WorkSpaces Secure Browser는 ENI 생성 중에 태그를 생성하도록 정책을 업데이트했습니다.	2022년 9월 6일
AmazonWorkSpacesWebServiceRolePolicy - 정책 업데이트	WorkSpaces 보안 브라우저가 정책을 업데이트하여 AWS/Usage 네임스페이스를 API 권한에 추가했습니다. PutMetricData	2022년 4월 6일
AmazonWorkSpacesWebReadOnly - 새 정책	WorkSpaces 보안 브라우저는 AWS 관리 콘솔, SDK 및 CLI를 통해 WorkSpaces 보안 브라우저 및 해당 종속성에 대한 읽기 전용 액세스를 제공하는 새 정책을 추가했습니다.	2021년 11월 30일
AmazonWorkSpacesWebServiceRolePolicy - 새 정책	WorkSpaces Secure Browser는 WorkSpaces Secure Browser에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 허용하는 새 정책을 추가했습니다.	2021년 11월 30일
WorkSpaces 시큐어 브라우저가 변경 사항을 추적하기 시작했습니다.	WorkSpaces Secure Browser는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 11월 30일

Amazon WorkSpaces 보안 브라우저 ID 및 액세스 문제 해결

다음 정보를 사용하면 WorkSpaces Secure Browser 및 에서 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- WorkSpaces 보안 브라우저에서 작업을 수행할 권한이 없습니다.
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사용자가 내 WorkSpaces Secure Browser 리소스에 액세스할 수 있도록 허용하고 싶습니다.

WorkSpaces 보안 브라우저에서 작업을 수행할 권한이 없습니다.

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. workspaces-web:*GetWidget*

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

이 경우 workspaces-web:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류 메시지가 표시되는 경우 WorkSpaces Secure Browser에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다. iam:PassRole

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 WorkSpaces Secure Browser에서 콘솔을 사용하여 작업을 marymajor 수행하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사용자가 내 WorkSpaces Secure Browser 리소스에 액세스할 수 있도록 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하세요.

- WorkSpaces Secure Browser가 이러한 기능을 지원하는지 여부를 알아보려면 을 참조하십시오. Amazon WorkSpaces 보안 브라우저의 작동 방식 IAM
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 사용 설명서의 다른 IAM AWS 계정 사용자에게 액세스 권한 제공을 IAM 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을 참조하십시오. AWS 계정
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

보안 브라우저용 WorkSpaces 서비스 연결 역할 사용

Amazon WorkSpaces 보안 브라우저는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 보안 브라우저에 직접 연결되는 고유한 유형의 IAM 역할입니다. WorkSpaces 서비스 연결 역할은 WorkSpaces Secure Browser에서 미리 정의하며 서비스가 사용자를 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 WorkSpaces Secure Browser를 더 쉽게 설정할 수 있습니다. WorkSpaces 보안 브라우저는 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 WorkSpaces 보안 브라우저만 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스 액세스 권한을 실수로 제거할 수 없으므로 WorkSpaces Secure Browser 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

보안 브라우저에 대한 서비스 연결 역할 권한 WorkSpaces

WorkSpaces Secure Browser는 이름이 지정된 AWSServiceRoleForAmazonWorkSpacesWeb 서비스 연결 역할을 사용합니다. WorkSpaces Secure Browser는 이 서비스 연결 역할을 사용하여 고객 계정의 Amazon EC2 리소스에 액세스하여 인스턴스 및 지표를 스트리밍합니다. CloudWatch

AWSServiceRoleForAmazonWorkSpacesWeb 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- workspaces-web.amazonaws.com

이름이 지정된 역할 권한 정책을 AmazonWorkSpacesWebServiceRolePolicy 통해 WorkSpaces Secure Browser는 지정된 리소스에서 다음 작업을 완료할 수 있습니다. 자세한 정보는 the section called “AmazonWorkSpacesWebServiceRolePolicy”을 참조하세요.

- 작업: all AWS resources에 ec2:DescribeVpcs
- 작업: all AWS resources에 대한 ec2:DescribeSubnets
- 작업: all AWS resources에 대한 ec2:DescribeAvailabilityZones
- 작업: 서브넷 및 보안 그룹 리소스에 aws:RequestTag/WorkSpacesWebManaged: true의 ec2:CreateNetworkInterface
- 작업: all AWS resources에 대한 ec2:DescribeNetworkInterfaces
- 작업: aws:ResourceTag/WorkSpacesWebManaged: true인 네트워크 인터페이스에 ec2:DeleteNetworkInterface
- 작업: all AWS resources에 대한 ec2:DescribeSubnets
- 작업: all AWS resources에 대한 ec2:AssociateAddress
- 작업: all AWS resources에 대한 ec2:DisassociateAddress
- 작업: all AWS resources에 대한 ec2:DescribeRouteTables
- 작업: all AWS resources에 대한 ec2:DescribeSecurityGroups
- 작업: all AWS resources에 대한 ec2:DescribeVpcEndpoints
- 작업: aws:TagKeys: ["WorkSpacesWebManaged"]인 ec2:CreateNetworkInterface 작업에 ec2:CreateTags

- 작업: `all AWS resources`에 대한 `cloudwatch:PutMetricData`
- 작업: `amazon-workspaces-web-`으로 시작하는 이름을 가진 Kinesis 데이터 스트림에 `kinesis:PutRecord`
- 작업: `amazon-workspaces-web-`으로 시작하는 이름을 가진 Kinesis 데이터 스트림에 `kinesis:PutRecords`
- 작업: `amazon-workspaces-web-`으로 시작하는 이름을 가진 Kinesis 데이터 스트림에 `kinesis:DescribeStreamSummary`

IAM 엔터티(예: 사용자, 그룹, 역할)가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 권한을 참조하세요.

보안 브라우저의 서비스 연결 역할 생성 WorkSpaces

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 첫 번째 포털을 생성하면 WorkSpaces 보안 브라우저가 서비스 연결 역할을 자동으로 생성합니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다.

이 서비스 연결 역할을 삭제한 다음 나중에 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 첫 번째 포털을 생성하면 WorkSpaces Secure Browser가 서비스 연결 역할을 다시 생성합니다.

또한 IAM 콘솔을 사용하여 Secure Browser 사용 사례와 함께 서비스 연결 역할을 생성할 수 있습니다. WorkSpaces AWS CLI 또는 AWS API에서 서비스 이름을 사용하여 서비스 연결 역할을 생성합니다. `workspaces-web.amazonaws.com` 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성 단원을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

보안 브라우저의 서비스 연결 역할 편집 WorkSpaces

WorkSpaces 보안 브라우저에서는 `AWSServiceRoleForAmazonWorkSpacesWeb` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때

문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

보안 브라우저의 서비스 연결 역할 삭제 WorkSpaces

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> WorkSpaces Secure Browser 서비스가 리소스를 삭제하려고 할 때 역할을 사용하는 경우 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 WorkSpaces 보안 브라우저 리소스를 삭제하려면 AWSServiceRoleForAmazonWorkSpacesWeb

- 다음 옵션 중 하나를 선택합니다.
  - 콘솔을 사용하는 경우 콘솔에서 모든 포털을 삭제합니다.
  - CLI 또는 API를 사용하는 경우 모든 리소스(예: 브라우저 설정, 네트워크 설정, 사용자 설정, 트러스트 스토어, 사용자 액세스 로깅 설정)를 포털에서 분리하고 이러한 리소스를 삭제한 다음 포털을 삭제합니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForAmazonWorkSpacesWeb 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

WorkSpaces 보안 브라우저 서비스 연결 역할이 지원되는 지역

WorkSpaces Secure Browser는 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하십시오.

Amazon WorkSpaces 보안 브라우저에서의 사고 대응

`SessionFailure`Amazon CloudWatch 지표를 모니터링하여 사고를 감지할 수 있습니다. 사고에 대한 알림을 받으려면 `SessionFailure` 지표에 대한 CloudWatch 경보를 사용하십시오. 자세한 내용은 Amazon을 WorkSpaces 통한 아마존 보안 브라우저 모니터링 CloudWatch을(를) 참조하세요.

Amazon WorkSpaces 보안 브라우저의 규정 준수 검증

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 적합한 애플리케이션을 만드는 AWS HIPAA 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 자격이 있는 것은 아닙니다. HIPAA 자세한 내용은 HIPAA적격 서비스 참조를 참조하십시오.

- AWS 규정AWS 준수 리소스 — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 ()) 를 포함한PCI) 전반의 보안 제어에 대한 지침을 매핑합니다. ISO
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.

- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하는 PCI DSS 등 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon WorkSpaces 보안 브라우저의 레질리언스

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

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

다음은 현재 WorkSpaces 보안 브라우저에서 지원되지 않습니다.

- AZ 또는 리전 간 콘텐츠 백업
- 암호화된 백업
- AZ 또는 리전 간 전송 중인 콘텐츠 암호화
- 기본 또는 자동 백업

높은 인터넷 가용성을 구성하기 위해 VPC 구성을 조정할 수 있습니다. API 가용성을 높이기 위해 적절한 양의 TPS를 요청할 수 있습니다.

Amazon 보안 브라우저의 인프라 WorkSpaces 보안

관리형 서비스인 Amazon WorkSpaces Secure Browser는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참

조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Amazon WorkSpaces Secure Browser에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안 (TLS). TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- (임시 디피-헬만) 또는 (타원 곡선 임시 디피-헬만PFS) 와 같이 완벽한 순방향 기밀성 DHE () 을 갖춘 암호 제품군. ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 보안 주체와 연결된 비밀 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

WorkSpaces 보안 브라우저는 표준 AWS SigV4 인증 및 권한 부여를 모든 서비스에 적용하여 서비스 트래픽을 분리합니다. 고객 리소스 엔드포인트(또는 웹 포털 엔드포인트)는 ID 제공업체가 보호합니다. ID 제공업체(IdP)의 다중 인증 및 기타 보안 메커니즘을 사용하여 트래픽을 추가로 분리할 수 있습니다.

VPC, 서브넷 또는 보안 그룹과 같은 네트워크 설정을 구성하여 모든 인터넷 액세스를 제어할 수 있습니다. 멀티 테넌시 및 VPC 엔드포인트 (PrivateLink) 는 현재 지원되지 않습니다.

Amazon WorkSpaces 보안 브라우저의 구성 및 취약성 분석

WorkSpaces 보안 브라우저는 필요에 따라 Chrome 및 Linux를 포함하여 애플리케이션 및 플랫폼을 업데이트하고 패치합니다. 패치하거나 다시 빌드할 필요는 없습니다. 하지만 사양 및 지침에 따라 WorkSpaces 보안 브라우저를 구성하고 사용자의 WorkSpaces 보안 브라우저 사용을 모니터링하는 것은 사용자의 책임입니다. 모든 서비스 관련 구성 및 취약성 분석은 Secure Browser의 책임입니다. WorkSpaces

웹 포털 수 및 사용자 수와 같은 WorkSpaces Secure Browser 리소스에 대한 한도 증가를 요청할 수 있습니다. WorkSpaces 보안 브라우저는 서비스 및 SLA의 가용성을 보장합니다.

Amazon 보안 브라우저의 WorkSpaces 보안 모범 사례

Amazon WorkSpaces Secure Browser는 자체 보안 정책을 개발하고 구현할 때 사용할 수 있는 다양한 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습

니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주십시오.

Amazon WorkSpaces 보안 브라우저의 모범 사례는 다음과 같습니다.

- WorkSpaces Secure Browser 사용과 관련된 잠재적 보안 이벤트를 CloudWatch 탐지하려면 Amazon을 사용하여 AWS CloudTrail 액세스 기록을 탐지 및 추적하고 로그를 처리하십시오. 자세한 내용은 Amazon을 WorkSpaces 통한 아마존 보안 브라우저 모니터링 CloudWatch 및 를 사용하여 WorkSpaces 보안 브라우저 API 호출 로깅 AWS CloudTrail 섹션을 참조하세요.
- 탐지 제어를 구현하고 이상 징후를 식별하려면 로그와 지표를 사용하십시오 CloudTrail . CloudWatch 자세한 내용은 Amazon을 WorkSpaces 통한 아마존 보안 브라우저 모니터링 CloudWatch 및 를 사용하여 WorkSpaces 보안 브라우저 API 호출 로깅 AWS CloudTrail 섹션을 참조하세요.
- 사용자 액세스 로깅을 설정하여 사용자 이벤트를 기록할 수 있습니다. 자세한 정보는 the section called “사용자 액세스 로깅 설정”을 참조하세요.

WorkSpaces Secure Browser 사용과 관련된 잠재적 보안 이벤트를 방지하려면 다음 모범 사례를 따르십시오.

- 최소 권한 액세스를 구현하고 WorkSpaces 보안 브라우저 작업에 사용할 특정 역할을 생성하십시오. IAM 템플릿을 사용하여 전체 액세스 또는 읽기 전용 역할을 생성합니다. 자세한 내용은 AWS WorkSpaces 보안 브라우저에 대한 관리형 정책을 참조하십시오.
- 포털 도메인과 사용자 보안 인증 정보를 공유할 때는 주의해야 합니다. 인터넷상의 모든 사용자가 웹 포털에 접근할 수 있지만, 포털에 대한 유효한 사용자 보안 인증 정보가 없으면 세션을 시작할 수 없습니다. 웹 포털 보안 인증 정보를 어떻게, 언제, 누구와 공유할지 여부는 신중하게 결정하십시오.

Amazon WorkSpaces 보안 브라우저 모니터링

모니터링은 Amazon WorkSpaces Secure Browser 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS WorkSpaces Secure Browser 포털 및 해당 리소스를 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정된 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 알려줄 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

주제

- Amazon을 WorkSpaces 통한 아마존 보안 브라우저 모니터링 CloudWatch
- 를 사용하여 WorkSpaces 보안 브라우저 API 호출 로깅 AWS CloudTrail
- 사용자 액세스 로깅

Amazon을 WorkSpaces 통한 아마존 보안 브라우저 모니터링 CloudWatch

원시 데이터를 수집하여 읽기 가능한 거의 실시간 지표로 처리하는 를 사용하여 CloudWatch Amazon WorkSpaces Secure Browser를 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수

있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

AWS/WorkSpacesWeb 네임스페이스에 포함된 지표는 다음과 같습니다.

CloudWatch Amazon WorkSpaces 시큐어 브라우저용 메트릭

지표	설명	차원	Statistics	단위
SessionAttempt	Amazon WorkSpaces 보안 브라우저 세션 시도 횟수.	PortalId	Average, Sum, Maximum, Minimum	개수
SessionSuccess	Amazon WorkSpaces 보안 브라우저 세션이 성공적으로 시작된 횟수입니다.	PortalId	Average, Sum, Maximum, Minimum	개수
SessionFailure	실패한 Amazon WorkSpaces 보안 브라우저 세션의 시작 횟수입니다.	PortalId	Average, Sum, Maximum, Minimum	개수
GlobalCpuPercent	Amazon WorkSpaces 보안 브라우저 세션 인스턴스의 CPU 사용량.	PortalId	Average, Sum, Maximum, Minimum	%
GlobalMemoryPercent	Amazon WorkSpaces 보안 브라우저 세션 인스턴스의 메모리 (RAM) 사용량.	PortalId	Average, Sum, Maximum, Minimum	%

> **Note**
>
> 포털의 “SampleCount” 지표 통계를 보거나 `GlobalCpuPercent` 포털에서 활성화된 동시 세션 수를 확인할 수 있습니다. `GlobalMemoryPercent` 데이터 포인트는 각 세션에서 1분에 한 번씩 생성됩니다.

를 사용하여 WorkSpaces 보안 브라우저 API 호출 로깅 AWS CloudTrail

WorkSpaces 보안 브라우저는 Amazon WorkSpaces Secure Browser에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Amazon WorkSpaces 보안 브라우저에 대한 모든 API 호출을 이벤트로 캡처합니다. 여기에는 Amazon WorkSpaces 보안 브라우저 콘솔에서의 호출 및 Amazon WorkSpaces 보안 브라우저 API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Amazon WorkSpaces Secure Browser용 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Amazon WorkSpaces Secure Browser에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 식별할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

WorkSpaces 보안 브라우저 정보: CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. Amazon WorkSpaces Secure Browser에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 이벤트 기록에서는 AWS 계정의 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Amazon WorkSpaces Secure Browser의 이벤트를 포함하여 AWS 계정의 지속적인 이벤트 기록을 보려면 트레일을 생성할 수 있습니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS지역에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합

- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Amazon WorkSpaces 보안 브라우저 작업은 Amazon WorkSpaces API 참조에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어`CreatePortal`, 에 대한 호출 `DeleteUserSettings` 및 `ListBrowserSettings` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

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

- 요청을 루트로 했는지 아니면 IAM 사용자 보안 인증 정보로 했는지 여부.
- 역할 또는 페더레이션 사용자의 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

WorkSpaces 보안 브라우저 로그 파일 항목 이해

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

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

```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
```

```
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "ListBrowserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
        "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    },
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
```

```
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```

사용자 액세스 로깅

Amazon WorkSpaces Secure Browser를 사용하면 고객이 시작, 중지 및 URL 방문을 비롯한 세션 이벤트를 기록할 수 있습니다. 이러한 로그는 웹 포털용으로 지정한 Amazon Kinesis 데이터 스트림으로 전송됩니다. 자세한 내용은 the section called “사용자 액세스 로깅 설정”을(를) 참조하세요.

WorkSpaces 보안 브라우저 사용자를 위한 지침

관리자는 WorkSpaces Secure Browser를 사용하여 내부 웹 사이트, SAAS software-as-a-service (웹 애플리케이션) 또는 인터넷과 같은 회사 웹 사이트에 연결하는 웹 포털을 만듭니다. 최종 사용자는 기존 웹 브라우저를 사용하여 이러한 웹 포털에 액세스한 뒤 세션을 시작하고 콘텐츠에 액세스합니다.

다음 내용은 WorkSpaces Secure Browser 액세스, 세션 시작 및 구성, 도구 모음 및 웹 브라우저 사용에 대해 자세히 알아보려는 최종 사용자를 안내하는 데 도움이 됩니다.

주제

- 브라우저 및 디바이스 호환성
- 웹 포털 액세스
- 세션 지침
- 문제 해결
- Single Sign-On을 위한 확장 프로그램

브라우저 및 디바이스 호환성

Amazon WorkSpaces Secure Browser는 웹 브라우저 내에서 실행되는 NICE DCV 웹 브라우저 클라이언트에서 구동되므로 설치가 필요하지 않습니다. 웹 브라우저 클라이언트는 Chrome 및 Firefox와 같은 일반적인 웹 브라우저와 Windows, macOS 및 Linux와 같은 주요 데스크톱 운영 체제에서 지원됩니다.

웹 브라우저 클라이언트 지원에 대한 up-to-date 자세한 내용은 웹 브라우저 클라이언트를 참조하십시오.

> **Note**
>
> 웹캠은 현재 Google Chrome 및 Microsoft Edge와 같은 Chromium 기반 브라우저에서만 지원됩니다. 현재 애플 사파리와 모질라는 웹캠을 FireFox 지원하지 않습니다.

웹 포털 액세스

관리자는 다음 옵션을 사용하여 웹 포털에 대한 액세스 권한을 제공할 수 있습니다.

- 이메일이나 웹사이트에서 링크를 선택한 다음 SAML ID 보안 인증 정보로 로그인할 수 있습니다.

- SAML ID 제공업체(예: Okta, Ping 또는 Azure)에 로그인하고 SAML 제공업체의 애플리케이션 홈 페이지(예: Okta 최종 사용자 대시보드 또는 Azure Myapps 포털)에서 클릭 한 번으로 세션을 시작할 수 있습니다.

세션 지침

웹 포털에 로그인한 후 세션을 시작하고 세션 중에 다양한 작업을 수행할 수 있습니다.

주제

- 세션 시작
- 도구 모음 사용
- 브라우저 사용
- 세션 종료

세션 시작

로그인하여 세션을 시작하면 세션 실행 중 메시지와 진행률 표시줄이 표시됩니다. 이는 Amazon WorkSpaces Secure Browser가 세션을 생성하고 있음을 나타냅니다. Amazon WorkSpaces Secure Browser는 백그라운드에서 인스턴스를 생성하고, 관리형 웹 브라우저를 시작하고, 관리자 설정 및 브라우저 정책을 적용합니다.

웹 포털에 처음 로그인하는 경우에는 도구 모음에 파란색 + 아이콘이 표시됩니다. 이 아이콘은 도구 모음에서 사용 가능한 기능을 안내하는 자습서가 제공되었음을 나타냅니다. 이 아이콘을 사용하여 다음 방법을 배울 수 있습니다.

- 로컬 브라우저 옆에 있는 잠금 아이콘을 선택하고 클립보드, 마이크, 카메라 옆의 스위치를 켜기로 설정하여 마이크, 웹캠, 클립보드에 대한 브라우저 권한을 허용할 수 있습니다.

> **Note**
>
> 첫 번째 세션을 시작할 때 웹캠 권한을 활성화하면 웹캠이 잠시 활성화되고 컴퓨터의 표시등이 깜박입니다. 이렇게 하면 로컬 브라우저가 웹캠에 액세스할 수 있게 됩니다.

- 브라우저에서 잠금 아이콘을 선택하고 항상 팝업을 허용하도록 설정하여 Amazon WorkSpaces Secure Browser를 활성화하여 추가 모니터 창을 실행합니다.

자습서를 다시 시작하려는 경우 도구 모음, 도움말, 자습서 시작에서 프로필을 선택하면 됩니다.

도구 모음 사용

도구 모음을 이동하려면 도구 모음 상단에서 밝은 막대를 선택하고 원하는 위치로 드래그한 다음 놓습니다.

도구 모음을 축소하려면 도구 모음 위에 마우스를 놓고 위쪽 화살표 버튼을 선택하거나 상단 섹션의 밝은 막대를 두 번 클릭합니다. 화면을 축소하면 더 넓은 화면 공간을 확보할 수 있으며 가장 일반적으로 사용되는 아이콘에 한 번의 클릭으로 액세스할 수 있습니다.

디스플레이 크기를 늘리려면 브라우저 창을 선택하고 확대합니다. 도구 모음 아이콘 및 텍스트의 표시 크기를 늘리려면 도구 모음을 선택하고 확대합니다.

Windows 장치를 확대 또는 축소하려면 다음 단계를 따르십시오.

1. 툴바 또는 웹 콘텐츠를 선택합니다.
2. 확대하려면 Ctrl + +를 누르고 축소하려면 Ctrl + -를 누르십시오.

Mac 기기를 확대 또는 축소하려면 다음 단계를 따르십시오.

1. 툴바 또는 웹 콘텐츠를 선택합니다.
2. 확대하려면 Cmd + +를 누르고 축소하려면 Cmd + -를 누르십시오.

도구 모음을 화면 상단에 고정하려면 도구 모음 모드에서 기본 설정, 일반 및 도킹을 선택합니다.

다음 표에는 도구 모음에서 사용할 수 있는 모든 아이콘에 대한 설명이 나와 있습니다.

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> 관리자가 이러한 권한을 부여하지 않는 한 클립보드 및 파일 아이콘은 기본적으로 숨겨집니다. 관리자만 웹 포털에서 클립보드 및 파일을 활성화하거나 비활성화할 수 있습니다. 이러한 아이콘이 숨겨져 있는데 액세스해야 하는 경우 관리자에게 문의하십시오.

브라우저 사용

세션을 시작하면 관리자가 선택한 URL인 시작 URL이 브라우저에 표시됩니다. 관리자가 시작 URL을 선택하지 않은 경우 Google Chrome에서 기본 새 탭 환경을 볼 수 있습니다.

브라우저에서 탭을 열고, Windows 도구 모음 아이콘 또는 브라우저의 3점 메뉴에서 추가 브라우저 창을 실행하거나, URL 표시줄에서 URL을 입력 또는 검색하거나, 관리형 북마크에서 웹사이트로 이동할 수 있습니다. 웹 포털의 북마크에 액세스하려면 (URL 표시줄 아래) 북마크 바에서 관리형 북마크 폴더를 열거나 URL 표시줄 오른쪽에 있는 3점 메뉴에서 북마크 관리자를 엽니다.

브라우저 창의 크기를 조정하거나 이동하려면 Chrome 탭 스트립을 아래로 드래그합니다. 이렇게 하면 세션 중에 다수의 브라우저 창에서 더 많은 화면 공간을 확보할 수 있습니다.

> **Note**
>
> 시크릿 모드와 같은 브라우저 기능은 관리자가 사용 중지한 경우 세션 중에 사용하지 못할 수 있습니다.

세션 종료

세션을 종료하려면 프로필 및 세션 종료를 선택합니다. 세션이 종료되면 Amazon WorkSpaces Secure Browser는 세션에서 모든 데이터를 삭제합니다. 세션이 종료된 후에는 열린 웹 사이트나 기록 같은 브라우저 데이터, 파일 탐색기의 파일 또는 데이터를 사용할 수 없습니다.

활성 세션 중에 탭을 닫으면 관리자가 설정한 시간이 지났을 때 세션이 종료됩니다. 이 제한 시간이 적용되기 전에 탭을 닫고 웹 포털을 다시 방문하면 현재 세션에 참여하여 열려 있는 웹 사이트 및 파일과 같은 이전 세션 데이터를 모두 볼 수 있습니다.

문제 해결

Amazon WorkSpaces 보안 브라우저 포털에서 로그인할 수 없습니다. "웹 포털이 아직 설정되지 않았습니다. 도움이 필요하면 관리자에게 문의하십시오."라는 오류 메시지를 받았습니다.

관리자가 SAML 2.0 ID 제공업체를 통해 포털 생성을 완료해야 로그인할 수 있습니다. 도움이 필요하면 관리자에게 문의하십시오.

포털에서 세션이 시작되지 않습니다. "세션을 예약하지 못했습니다. 내부 오류가 발생했습니다. 다시 시도하십시오."라는 오류 메시지를 받았습니다.

웹 포털 세션 시작에 문제가 발생했습니다. 세션을 다시 시작해 보십시오. 이 문제가 계속되면 관리자에게 도움을 요청하십시오.

클립보드, 마이크 또는 웹캠을 사용할 수 없습니다.

브라우저 권한을 허용하려면 URL 옆의 잠금 아이콘을 선택하고 클립보드, 마이크, 카메라, 팝업 및 리디렉션 옆에 있는 파란색 스위치를 토글하여 해당 기능을 켭니다.

> **Note**
>
> 웹 브라우저가 비디오 또는 오디오 입력을 지원하지 않는 경우 이러한 옵션은 도구 모음에 표시되지 않습니다.

Amazon WorkSpaces Secure Browser 실시간 오디오-비디오 (AV) 는 로컬 웹캠 비디오 및 마이크 오디오 입력을 브라우저 스트리밍 세션으로 리디렉션합니다. 이렇게 하면 Google Chrome 또는 Microsoft Edge와 같은 Chromium 기반 웹 브라우저를 사용하는 스트리밍 세션 내에서 로컬 디바이스를 사용하여 비디오 및 오디오 회의를 진행할 수 있습니다. Chromium 이외 브라우저에서는 현재 웹캠이 지원되지 않습니다.

Google Chrome을 구성하는 방법에 대한 자세한 내용은 카메라 및 마이크 사용을 참조하십시오.

내 웹 포털에서 추가 모니터 창이 열리지 않습니다.

듀얼 모니터를 실행하려고 하는데 상단 브라우저의 주소 표시줄 끝에 팝업 차단됨 아이콘이 표시되면 해당 아이콘과 팝업 및 리디렉션 항상 허용 옆의 라디오 버튼을 선택합니다. 팝업이 허용되면 도구 모음에서 듀얼 모니터 아이콘을 선택하여 새 창을 열고 모니터에서 창 위치를 변경한 다음 브라우저 탭을 창으로 드래그합니다.

파일 창에서 파일을 다운로드하려고 해도 아무런 변화가 없습니다.

파일 창에서 파일을 다운로드 하려고 하는데 상단 브라우저의 주소 표시줄 끝에 팝업 차단됨 아이콘이 표시되면 해당 아이콘과 팝업 및 리디렉션 항상 허용 옆의 라디오 버튼을 선택합니다. 팝업이 허용된 상태에서 파일을 다시 다운로드해 보십시오.

Single Sign-On을 위한 확장 프로그램

Amazon WorkSpaces Secure Browser는 데스크톱 컴퓨터의 Chrome 및 Firefox 브라우저를 통한 싱글 사인온을 위한 확장 프로그램을 제공합니다. 관리자가 확장 프로그램을 활성화한 경우 로그인할 때 웹 포털에서 확장 프로그램을 설치하라는 메시지를 표시합니다.

Amazon WorkSpaces Secure Browser는 세션 중에 웹 사이트에 싱글 사인온을 가능하게 하는 확장 프로그램을 구축했습니다. 예를 들어, SAML 2.0 ID 제공업체(예: Okta 또는 Ping)를 사용하여 웹 포털에 로그인하고 세션 중에 동일한 ID 제공업체를 사용하는 웹 사이트를 방문하는 경우 확장 프로그램을 사용하면 추가 로그인 프롬프트를 제거하여 웹 사이트에 더 쉽게 액세스할 수 있습니다.

웹 포털에 액세스하기 위해 확장 프로그램을 설치할 필요는 없지만 사용자 이름과 암호를 입력하라는 메시지가 표시되는 횟수를 줄여 환경을 개선할 수 있습니다.

로그인하면 확장 프로그램은 관리자가 세션과 관련하여 나열된 쿠키를 찾습니다. 확장 프로그램이 찾는 모든 데이터는 저장 중이거나 전송 중에 암호화됩니다. 이 데이터는 로컬 브라우저에 저장되지 않습니다. 세션을 종료하면 모든 세션 데이터(예: 열린 탭, 다운로드한 파일, 세션 중에 전달되거나 생성된 쿠키)가 삭제됩니다.

호환성

확장 프로그램은 다음 디바이스에서 사용할 수 있습니다.

- 랩톱
- 데스크톱

확장 프로그램은 다음 브라우저에서 사용할 수 있습니다.

- Chrome
- Firefox

설치

포털에 로그인하면 프롬프트에 따라 Chrome 또는 Firefox 브라우저용 확장 프로그램을 설치합니다. 각 웹 브라우저마다 이 작업을 한 번만 수행하면 됩니다.

디바이스를 전환하거나, 같은 디바이스에서 다른 브라우저로 전환하거나, 로컬 브라우저에서 확장 프로그램을 삭제하는 경우에는 다음 세션을 시작할 때 확장 프로그램을 설치하라는 메시지가 표시됩니다.

확장 프로그램이 예상대로 작동하도록 하려면 시크릿 (Chrome) 또는 사생활 보호 브라우징 (Firefox) 대신 일반 브라우징 창에서 확장 프로그램을 사용하세요.

문제 해결

확장 프로그램을 설치했는데도 세션 중에 로그인하라는 메시지가 계속 표시되는 경우 다음 단계를 따릅니다.

1. 브라우저에 Amazon WorkSpaces 보안 브라우저 확장 프로그램이 설치되어 있는지 확인하십시오. 브라우저 데이터를 삭제한 경우 확장 프로그램이 실수로 제거되었을 수 있습니다.
2. 시크릿 모드 (Chrome) 또는 프라이빗 브라우징 (Firefox) 이 아닌지 확인하십시오. 이러한 모드는 확장 프로그램에 문제를 일으킬 수 있습니다.
3. 문제가 지속되면 포털 관리자에게 문의하여 추가 지원을 받으십시오.

Amazon WorkSpaces 보안 브라우저 관리 가이드의 문서 기록

다음 표에는 Amazon WorkSpaces Secure Browser의 설명서 릴리스가 설명되어 있습니다.

변경 사항	설명	날짜
딥링크 허용	포털이 세션 중에 사용자를 특정 웹사이트로 연결하는 딥링크를 수신할 수 있도록 허용합니다.	2024년 6월 25일
관리형 정책 업데이트	AmazonWorkSpacesSecureBrowserReadOnly 관리형 정책이 추가되었습니다.	2024년 6월 24일
툴바를 사용하여 확대/축소하세요.	툴바를 사용하여 디스플레이, 아이콘 및 텍스트의 크기를 늘릴 수 있습니다.	2024년 5월 1일
새 웹 포털 설정	이제 웹 포털의 인스턴스 유형 및 최대 동시 사용자 제한을 지정할 수 있습니다.	2024년 4월 22일
CloudWatch 지표	추가 GlobalCpuPercent 및 GlobalMemoryPercent 지표.	2024년 2월 26일
URL 필터링 설정	Chrome 정책을 사용하여 사용자가 원격 브라우저에서 액세스할 수 있는 URL을 필터링할 수 있습니다.	2024년 2월 21일
IdP 인증 유형	표준 또는 IAM ID 센터 인증 유형을 선택할 수 있습니다.	2024년 2월 5일
Single Sign-On용 확장 프로그램 활성화	최종 사용자가 더 나은 포털 로그인을 경험할 수 있도록 확장	2023년 8월 28일

	프로그램을 활성화할 수 있습니다.	
Amazon WorkSpaces 보안 브라우저 사용자 지침	Amazon WorkSpaces Secure Browser 액세스, 세션 시작 및 구성, 도구 모음 및 웹 브라우저 사용에 대해 자세히 알아보려는 최종 사용자를 안내하는 데 도움이 되는 콘텐츠가 추가되었습니다.	2023년 7월 17일
IP 액세스 제어	WorkSpaces 보안 브라우저를 사용하면 웹 포털에 액세스할 수 있는 IP 주소를 제어할 수 있습니다.	2023년 5월 31일
관리형 정책 업데이트	업데이트된 AmazonWorkSpacesWebReadOnly 관리형 정책	2023년 5월 15일
ID 제공업체 업데이트 구성	WorkSpaces 보안 브라우저는 표준 및 두 가지 인증 유형을 제공합니다. AWS IAM Identity Center	2023년 3월 15일
브라우저 정책 업데이트	업데이트 및 재구성된 브라우저 정책 섹션	2023년 1월 31일
관리형 정책 업데이트	업데이트된 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책	2022년 12월 15일
허용 목록 및 차단 목록	허용 목록 및 차단 목록을 지정하여 사용자가 액세스할 수 있거나 액세스할 수 없는 도메인 목록을 지정합니다.	2022년 11월 14일

관리형 정책 업데이트	업데이트된 AmazonWorkSpacesWebReadOnly 관리형 정책	2022년 11월 2일
관리형 정책 업데이트	업데이트된 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책	2022년 10월 24일
서버 액세스 로깅	사용자 이벤트를 기록하도록 사용자 액세스 로깅 설정	2022년 10월 17일
네트워킹 업데이트	'네트워킹 및 액세스' 섹션에 대한 다양한 업데이트	2022년 9월 22일
관리형 정책 업데이트	업데이트된 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책	2022년 9월 6일
사용자 세션 구성	입력 방법 편집기(IME) 및 세션 내 로컬라이제이션 구성	2022년 7월 28일
네트워킹 업데이트	'네트워킹 및 액세스' 섹션에 대한 다양한 업데이트	2022년 7월 7일
제한 시간 값	연결 해제 제한 시간(분) 및 유휴 연결 해제 제한 시간(분)을 지정합니다.	2022년 5월 16일
업데이트된 관리형 정책	AWS/사용 네임스페이스를 API 권한에 추가하도록 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책을 업데이트했습니다. PutMetricData	2022년 4월 6일
서비스 연결 역할	AWSServiceRoleForAmazonWorkSpacesWeb 새 서비스 연결 역할	2021년 11월 30일

관리형 정책	새 AmazonWorkSpacesWebReadOnly 관리형 정책	2021년 11월 30일
관리형 정책	새 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책	2021년 11월 30일
최초 릴리스	WorkSpaces 보안 브라우저 관리 가이드의 최초 릴리스	2021년 11월 30일

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