aws

관리 설명서

Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser: 관리 설명서

Table of Contents

Amazon WorkSpaces Secure Browser란? 1
릴리스 이력 1
알아야 할 용어 2
관련 서비스 4
Architecture 4
액세스 5
설정 6
사용자 가입 및 생성 6
에 가입 AWS 계정 6
관리자 액세스 권한이 있는 사용자 생성 6
프로그래밍 방식 액세스 권한 부여 8
네트워킹 9
VPC 설정 10
사용자 연결 23
시작하기 26
웹 포털 생성 26
네트워크 설정 27
포털 설정 27
사용자 설정 29
ID 제공업체 구성 31
시작 40
웹 포털 테스트 41
웹 포털 배포 41
웹 포털 관리 43
웹 포털 세부 정보 보기 43
웹 포털 편집 44
웹 포털 삭제 44
서비스 할당량 관리 44
서비스 할당량 증가 요청 45
포털 증가 요청 46
최대 동시 세션 증가 요청 46
한도 예 47
기타 서비스 할당량 47
SAML IdP 토큰 재인증 48

사용자 활동 로깅 설정 49
세션 로거 설정 49
사용자 액세스 로깅 설정 52
브라우저 정책 관리 53
자습서: 사용자 지정 브라우저 정책 설정 54
기본 브라우저 정책 편집 60
입력 방법 편집기 구성 61
세션 내 로컬라이제이션 구성 63
지원되는 언어 코드 63
사용자 브라우저 설정 65
IP 액세스 제어 관리 66
IP 액세스 제어 그룹 생성 67
IP 액세스 설정 연결 67
IP 액세스 제어 그룹 편집 68
IP 액세스 제어 그룹 삭제 69
Single Sign-On 확장 프로그램 관리 69
Single Sign-On 확장 프로그램에 대한 도메인 식별 70
새 웹 포털에 Single Sign-On 확장 프로그램 추가 70
기존 웹 포털에 Single Sign-On 확장 프로그램 추가 71
Single Sign-On 확장 프로그램 편집 또는 제거 71
웹 콘텐츠 필터링 71
특정 URLs로 브라우징 제한 72
특정 URLs 차단 72
차단 범주 73
URLs의 예 75
Chrome 정책 전송 75
딥 링크 76
딥 링크 설정 76
딥 링크에 URL 필터링 사용 77
세션 관리 대시보드 77
대시보드 액세스 77
대시보드 필터 78
세션 종료 78
세션 기록 78
전송 중 데이터 보호 79
데이터 보호 설정 79

인라인 데이터 수정 80
기본 수정 구성 81
기본 인라인 수정 82
사용자 지정 인라인 수정 84
데이터 보호 설정 생성 85
데이터 보호 설정 연결 86
데이터 보호 설정 편집 87
데이터 보호 설정 삭제 87
브랜딩 사용자 지정 88
포털에 대한 브랜딩 사용자 지정 구성 88
사용자 지정 지침 91
웹 인증 리디렉션 105
포털 설정에서 WebAuthn 리디렉션 활성화 105
로컬 브라우저 정책 구성 106
WebAuthn 리디렉션 사용량 106
WebAuthn 리디렉션 문제 해결 107
도구 모음 제어 108
사용자 지정 도메인 109
포털에 대한 사용자 지정 도메인 구성 110
사용자 지정 도메인 문제 해결 120
보안 122
데이터 보호 123
데이터 암호화 124
인터네트워크 트래픽 개인 정보 보호 132
사용자 액세스 로깅 133
자격 증명 및 액세스 관리 133
대상 133
ID를 통한 인증 134
정책을 사용하여 액세스 관리 135
Amazon WorkSpaces Secure Browser와 IAM의 연동 방식 136
ID 기반 정책 예시 142
AWS 관리형 정책 145
문제 해결 154
서비스 연결 역할 사용 156
인시던트 대응 159
규정 준수 확인 159

복원성 160
인프라 보안 160
구성 및 취약성 분석 161
인터페이스 VPC 엔드포인트(AWS PrivateLink) 161
Amazon WorkSpaces Secure Browser에 대한 고려 사항 162
Amazon WorkSpaces Secure Browser용 인터페이스 VPC 엔드포인트 생성 162
인터페이스 VPC 엔드포인트에 대한 엔드포인트 정책 생성 162
문제 해결 163
보안 모범 사례 164
모니터링 165
CloudWatch를 사용하여 모니터링 165
CloudTrail 로그 168
CloudTrail의 정보 169
로그 파일 항목 170
사용자 활동 로깅 172
세션 로거의 세션 이벤트 172
사용자 액세스 로깅의 세션 이벤트 178
사용자 지침 181
브라우저 및 디바이스 호환성 181
웹 포털 액세스 181
세션 지침 182
세션 시작 182
도구 모음 사용 183
브라우저 사용 185
세션 종료 185
사용자 문제 해결 186
Single Sign-On 확장 프로그램 187
Single Sign-On 확장 프로그램 호환성 188
Single Sign-On 확장 프로그램 설치 188
Single Sign-On 확장 프로그램 문제 해결 188
문서 이력 190
..... cxciv

Amazon WorkSpaces Secure Browser란?

> **Note**
>
> Amazon WorkSpaces Secure Browser의 이전 명칭은 Amazon WorkSpaces Web이었습니다.

Amazon WorkSpaces Secure Browser는 완전 관리형 클라우드 네이티브 호스팅 브라우저 서비스로, 프라이빗 웹 사이트 및 서비스형 소프트웨어(SaaS) 웹 애플리케이션에 안전하게 액세스하고, 온라인 리소스와 상호 작용하며, 일회용 컨테이너에서 인터넷을 탐색하는 데 사용됩니다. WorkSpaces Secure Browser는 사용자의 기존 웹 브라우저에서 작동하므로 어플라이언스, 인프라, 특수 클라이언트 소프트웨어 또는 가상 프라이빗 네트워크(VPN) 연결을 관리해야 하는 IT 부서의 부담을 덜어줍니다. 웹 콘텐츠는 사용자의 웹 브라우저로 스트리밍되는 반면 실제 브라우저와 웹 콘텐츠는 격리됩니다 AWS. Amazon WorkSpaces 및 Amazon WorkSpaces 애플리케이션과 같은 AWS 최종 사용자 컴퓨팅 서비스를 지원하는 것과 동일한 기본 기술을 사용하면 WorkSpaces Secure Browser가 기존 가상 데스크톱보다 비용 효율적이며 회사 소유 디바이스에 관리 소프트웨어를 제공하는 것보다 복잡성을 줄일 수 있습니다. WorkSpaces Secure Browser는 웹 콘텐츠를 스트리밍하여 데이터 유출 위험을 줄입니다. HTML, 문서 객체 모델(DOM) 또는 민감한 회사 데이터는 로컬 시스템으로 전송되지 않습니다. 또한 디바이스, 기업 네트워크 및 인터넷을 서로 격리하여 브라우저 공격 표면을 사실상 제거합니다.

모든 세션에 엔터프라이즈 브라우저 정책(URL 허용/차단 포함)을 적용할 수 있으며 클립보드, 파일 전송 및 프린터에 대한 세션 수준 제어를 포함할 수 있습니다. 또한 IP 액세스 제어를 사용하여 신뢰할 수 있는 네트워크 또는 디바이스에 대한 액세스를 제한할 수 있습니다. WorkSpaces Secure Browser는 설정 및 운영이 쉽습니다. 각 세션은 회사 정책과 설정이 적용된 새롭고 완전히 패치된 버전의 Chrome 브라우저로 시작됩니다.

Amazon WorkSpaces Secure Browser 릴리스 이력

2024년 5월 20일 Amazon WorkSpaces Web의 이름이 Amazon WorkSpaces Secure Browser로 변경되었습니다. 기존 고객의 경우 서비스에서 사용자나 리소스를 관리하는 방식은 변경되지 않았습니다. 다음 목록에서는 이번 이름 변경으로 인해 적용된 업데이트에 대해 설명합니다.

Workspaces-web API 네임스페이스는 이전 버전과의 호환성을 위해 변경되지 않았습니다. 따라서 다음 리소스는 동일합니다.

- CLI 명령

- Amazon CloudWatch 지표 자세한 내용은 the section called “CloudWatch를 사용하여 모니터링” 단원을 참조하십시오.
- 서비스 엔드포인트. 자세한 내용은 Amazon WorkSpaces Secure Browser 엔드포인트 및 할당량을 참조하세요.
- AWS CloudFormation 리소스. 자세한 내용은 Amazon WorkSpaces Secure Browser 리소스 유형 참조를 참조하세요.
- Workspaces-web이 포함된 서비스 연결 역할. 자세한 내용은 the section called “서비스 연결 역할 사용” 단원을 참조하십시오.
- Workspaces-web이 포함된 콘솔 URL
- Workspaces-web이 포함된 문서 URL. 자세한 내용은 Amazon WorkSpaces Secure Browser 설명서를 참조하세요.
- 기존 ReadOnly 관리형 역할. 자세한 내용은 the section called “AWS 관리형 정책” 단원을 참조하십시오.
- KMS 권한 부여 이름
- UAL(User-Activity Logging) Kinesis 스트림 접두사

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

Amazon WorkSpaces Secure Browser 사용 시 알아야 할 용어

WorkSpaces Secure Browser를 시작하기 전에 다음 개념을 익혀야 합니다.

ID 제공업체(IdP)

IdP는 사용자의 보안 인증 정보를 확인합니다. 그런 다음 인증 어설션을 발행하여 서비스 제공업체에 액세스 권한을 제공합니다. WorkSpaces Secure Browser에서 작동하도록 기존 IdP를 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. IdP에서 WorkSpaces Secure Browser를 사용할 수 있도록 사용자에게 액세스 권한을 부여해야 합니다.

ID 제공업체(IdP) 메타데이터 문서

WorkSpaces Secure Browser는 신뢰를 구축하기 위해 ID 제공업체(IdP)의 특정 메타데이터를 필요로 합니다. 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 Secure Browser는 IdP로부터 인증을 받은 사용자에게 서비스 제공업체 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 WorkSpaces Secure Browser와 연결할 수 있습니다.

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, 보안 그룹은 WorkSpaces Secure Browser 콘솔과 동일한 리전에서 가져온 것입니다.

신뢰할 수 있는 스토어

WorkSpaces Secure Browser를 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 웹 사이트를 로드하기 위해 사용자 디바이스에서 특정 인증서를 설치해야 하는 경우 사용자가 WorkSpaces Secure Browser에서 해당 사이트에 액세스할 수 있으려면 해당 인증서를 신뢰할 수 있는 스토어에 추가해야 합니다.

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.

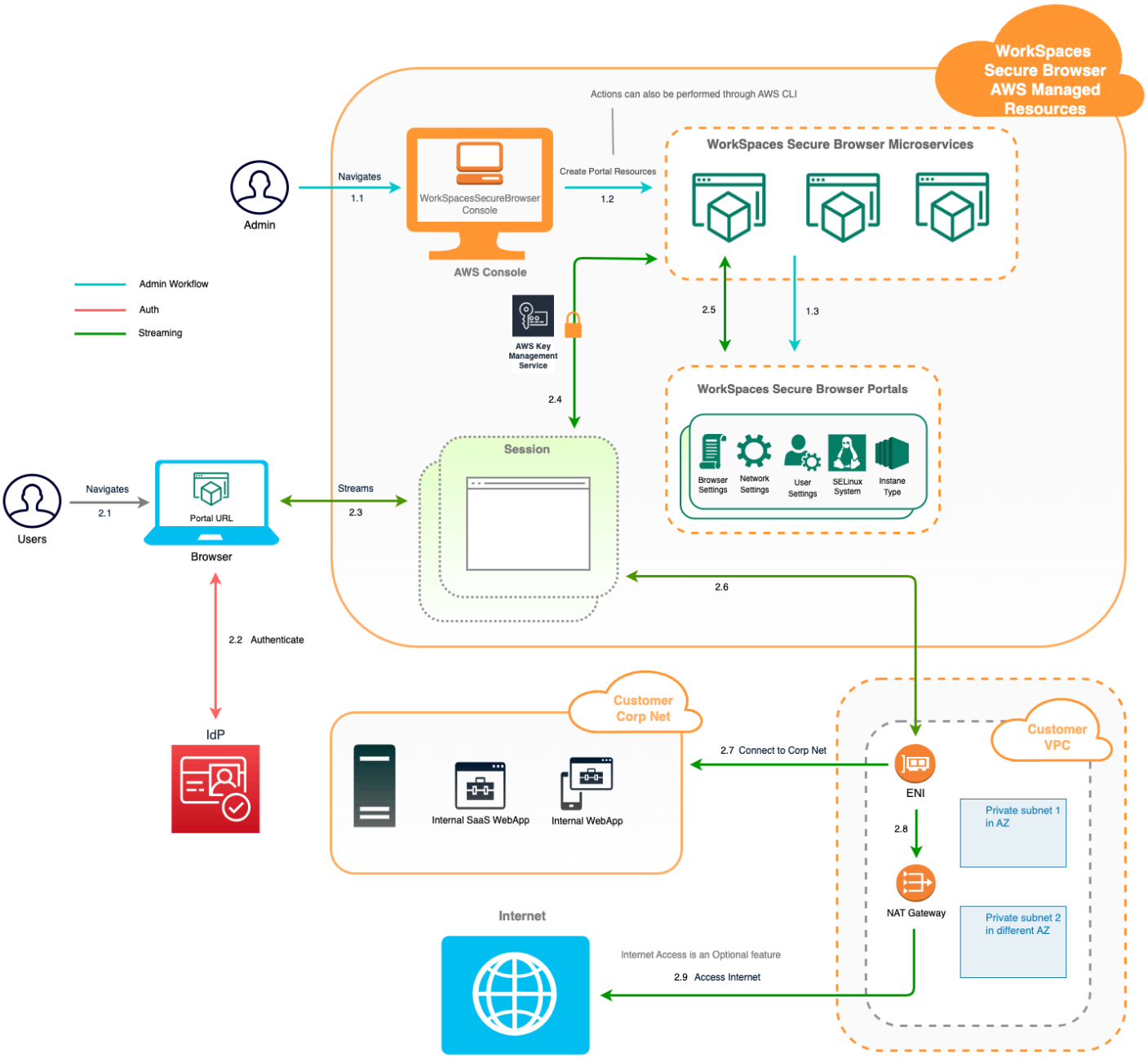
AWS Amazon WorkSpaces Secure Browser와 관련된 서비스

WorkSpaces Secure Browser와 관련된 여러 AWS 서비스가 있습니다.

WorkSpaces Secure Browser는 AWS 최종 사용자 컴퓨팅 포트폴리오에 있는 Amazon WorkSpaces의 기능입니다. WorkSpaces 및 AppStream 2.0과 비교하여 WorkSpaces Secure Browser는 안전한 웹 기반 워크로드를 지원하도록 특별히 구축되었습니다. WorkSpaces Secure Browser는 자동으로 관리되므로, 용량, 규모 조정, 이미지는 AWS에서 필요에 따라 프로비저닝 및 업데이트됩니다. 예를 들어 데스크톱 리소스에 액세스해야 하는 소프트웨어 개발자에게는 영구 Workspace Desktop을 제공하고 데스크톱 컴퓨터에서 소수의 내부 및 SaaS 웹 사이트(네트워크 외부에 호스팅되는 웹 사이트 포함)에만 액세스해야 하는 콜센터 사용자에게는 WorkSpaces Secure Browser를 제공할 수 있습니다.

Amazon WorkSpaces Secure Browser의 아키텍처

다음 다이어그램은 WorkSpaces Secure Browser의 아키텍처입니다.



Amazon WorkSpaces Secure Browser에 액세스

WorkSpaces Secure Browser에는 여러 가지 방법으로 액세스할 수 있습니다.

관리자는 WorkSpaces Secure Browser 콘솔, SDK, CLI 또는 API를 통해 WorkSpaces 보안 브라우저에 액세스합니다. 사용자는 WorkSpaces Secure Browser 엔드포인트를 통해 액세스할 수 있습니다.

Amazon WorkSpaces Secure Browser 설정

내부 웹 사이트 및 SaaS 애플리케이션에 연결하도록 WorkSpaces Secure Browser를 구성하려면 먼저 다음 사전 조건을 완료해야 합니다.

주제

- 사용자 가입 및 생성
- 프로그래밍 방식 액세스 권한 부여
- Amazon WorkSpaces Secure Browser용 네트워킹

사용자 가입 및 생성

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

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

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

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

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

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

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

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

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

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 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

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 참조하세요. AWS 로그인

추가 사용자에게 액세스 권한 할당

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

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

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

프로그래밍 방식 액세스 권한 부여

사용자는 AWS 외부에서와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

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

프로그래밍 방식 액세스가 필요한 사용자	목적	방법
IAM	(권장) 콘솔 자격 증명을 임시 자격 증명으로 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS 로컬 개발을 위한 로그인을 참조하세요. • AWS SDKs 경우 SDK 및 도구 참조 안내서의 AWS 로컬 개발을 위한 로그인을 참조하세요. AWS SDKs
작업 인력 ID (IAM Identity Center에서 관리되는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center 참조하세요. • AWS SDKs, 도구 및 AWS APIs 경우 SDK 및 도구 참조 안내서의 IAM Identity

프로그래밍 방식 액세스가 필요한 사용자	목적	방법
		Center 인증을 참조하세요. AWS SDKs
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	IAM 사용 설명서의 AWS 리소스에서 임시 자격 증명 사용의 지침을 따릅니다.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 사용 AWS Command Line Interface 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 참조하세요. • AWS SDKs 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용하여 인증을 참조하세요. AWS SDKs • AWS APIs 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요.

Amazon WorkSpaces Secure Browser용 네트워킹

다음 주제에서는 사용자가 연결할 수 있도록 WorkSpaces Secure Browser 스트리밍 인스턴스를 설정하는 방법에 대해 설명합니다. 또한 인터넷뿐만 아니라 VPC 리소스에 액세스할 수 있도록 WorkSpaces Secure Browser 스트리밍 인스턴스를 활성화하는 방법에 대해서도 설명합니다.

주제

- Amazon WorkSpaces Secure Browser용 VPC 설정
- Amazon WorkSpaces Secure Browser에 대한 사용자 연결 활성화

Amazon WorkSpaces Secure Browser용 VPC 설정

WorkSpaces Secure Browser용 VPC를 설정하고 구성하려면 다음 단계를 완료합니다.

주제

- Amazon WorkSpaces Secure Browser에 대한 VPC 요구 사항
- Amazon WorkSpaces Secure Browser용 새 VPC 생성
- Amazon WorkSpaces Secure Browser의 인터넷 브라우징 활성화
- WorkSpaces Secure Browser용 VPC 모범 사례
- Amazon WorkSpaces Secure Browser에서 지원되는 가용 영역

Amazon WorkSpaces Secure Browser에 대한 VPC 요구 사항

WorkSpaces Secure Browser 포털을 생성하는 동안 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 예상되는 Workspaces Secure Browser 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 내용은 Amazon WorkSpaces Secure Browser용 새 VPC 생성 단원을 참조하십시오.
- 모든 서브넷은 사용자가 WorkSpaces Secure Browser를 사용하여 액세스할 수 있는 AWS 클라우드 또는 온프레미스에 있는 모든 내부 콘텐츠에 안정적으로 연결되어 있어야 합니다.

가용성 및 규모 조정 여부를 고려하여 서로 다른 가용 영역에서 세 개의 서브넷을 선택하는 것이 좋습니다. 자세한 내용은 Amazon WorkSpaces Secure Browser용 새 VPC 생성 단원을 참조하십시오.

WorkSpaces Secure Browser는 인터넷 액세스를 활성화하기 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 Amazon WorkSpaces Secure Browser의 무제한 인터넷 브라우징 활성화(권장)에 설명된 단계를 완료합니다.

Amazon WorkSpaces Secure Browser용 새 VPC 생성

이 섹션에서는 VPC 마법사를 사용하여 퍼블릭 및 프라이빗 서브넷이 있는 VPC를 빠르게 생성하는 방법을 설명합니다. 마법사는 인터넷 게이트웨이, NAT 게이트웨이를 자동으로 생성하고 서브넷의 라우팅 테이블을 구성합니다.

이 구성에 대한 자세한 내용은 퍼블릭 및 프라이빗 서브넷이 있는 VPC(NAT)를 참조하십시오.

주제

- 빠른 VPC 설정(1분)
- 서브넷 라우팅 테이블 확인(선택 사항)

빠른 VPC 설정(1분)

인터넷 액세스를 위한 퍼블릭 및 프라이빗 서브넷이 있는 WorkSpaces Secure Browser 전용 VPC를 빠르게 생성하려면 다음 단계를 완료하세요. 기존 VPC를 사용하려면 섹션을 Amazon WorkSpaces Secure Browser에 대한 VPC 요구 사항 참조하여 요구 사항을 충족하는지 확인하세요.

> **Note**
>
> 원하는에 있는지 확인합니다 AWS 리전. 필요한 경우 콘솔에서 리전을 변경할 수 있습니다.

VPC를 빠르게 설정하려면

1. VPC 생성 마법사 열기: 리소스를 사용하여 VPC를 생성합니다. 아래에 지정하지 않는 한 모든 설정을 기본값으로 유지합니다.
   - 생성할 리소스에서 VPC 등을 선택합니다.
   - 이름 태그에서 자동 생성을 선택하고 VPC를 설명하는 이름(예: **`WSB-VPC`**)을 입력합니다.
   - IPv4 CIDR 블록의 경우 기본적으로 VPC는를 사용합니다**`10.0.0.0/16`**. 필요한 경우 다른 IPv4 CIDR 블록을 지정할 수 있습니다.
   - 테넌시에서 기본값을 선택합니다(전용 테넌시VPCs는 지원되지 않음).
   - 가용 영역(AZs) 수에서 2를 선택합니다.
     - AZs 사용자 지정을 확장하고 WorkSpaces Secure Browser에서 지원하는 2개의 서로 다른 가용 영역을 선택합니다. 지원되는 AZsAmazon WorkSpaces Secure Browser에서 지원되는 가용 영역.

- 퍼블릭 서브넷 수에서 2를 선택합니다.
- 프라이빗 서브넷 수에서 2를 선택합니다.
- 서브넷 CIDR 블록의 경우 서브넷의 CIDR 블록을 사용자 지정해야 하는 경우 서브넷 CIDR 블록 사용자 지정을 확장합니다. 각 서브넷에 예상 트래픽에 충분한 IP 주소가 있는지 확인합니다.
- NAT 게이트웨이의 경우 리전을 선택하여 모든 가용 영역에서 프라이빗 서브넷에 대한 인터넷 액세스를 활성화합니다.
- VPC 엔드포인트에서 없음을 선택합니다. NAT 게이트웨이를 통과하지 않고 직접 S3 액세스가 필요한 경우 S3 게이트웨이를 선택합니다.
- DNS 옵션의 경우 DNS 옵션을 활성화(기본값) 상태로 유지하여 VPC 내에서 적절한 이름 확인을 보장합니다.

2. 미리 보기 창을 검토한 다음 VPC 생성을 선택합니다.

> **Note**
>
> NAT 게이트웨이 및 VPC 엔드포인트에는 추가 요금이 적용됩니다. 자세한 내용은 VPC 요금 페이지를 참조하세요.

서브넷 라우팅 테이블 확인(선택 사항)

VPC 마법사는 자동으로 라우팅 테이블을 구성합니다. VPC를 수동으로 생성했거나 구성을 확인하려는 경우 라우팅 테이블에 대해 다음 세부 정보가 올바른지 확인할 수 있습니다.

- 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 다음 퍼블릭 서브넷을 선택합니다. 예: WSB-VPC-subnet-public1-us-east-1a.
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.

Destination	대상	설명
퍼블릭 서브넷 IPv4 CIDR 블록(예: 10.0.0.0/20)	로컬	퍼블릭 서브넷 IPv4 CIDR 블록의 IPv4 주소로 향하는 리소스의 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 Subnets를 선택합니다. 그런 다음 프라이빗 서브넷(예: **WSB-VPC-subnet-private1-us-east-1a**)을 선택합니다.
6. 라우팅 테이블 탭에서 라우팅 테이블의 ID를 선택합니다.
7. 라우팅 테이블을 선택합니다. 이름에서 편집(연필) 아이콘을 선택하고 테이블 이름을 입력합니다. 예를 들어, **WSB-VPC-private-routetable**을 이름으로 입력할 수 있습니다. 이름을 저장하려면 확인 표시를 선택합니다.
8. 경로 탭에서 라우팅 테이블에 다음 라우팅이 포함되어 있는지 확인합니다.

Destination	대상	설명
퍼블릭 서브넷 IPv4 CIDR 블록(예: 10.0.0.0/20)	로컬	퍼블릭 서브넷 IPv4 CIDR 블록의 IPv4 주소로 향하는 리소스의 모든 트래픽은 VPC 내에서 로컬로 라우팅됩니다.

Destination	대상	설명
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 Subnets를 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.

Amazon WorkSpaces Secure Browser의 인터넷 브라우징 활성화

무제한 인터넷 브라우징(권장 옵션) 또는 제한된 인터넷 브라우징을 활성화하도록 선택할 수 있습니다.

주제

- Amazon WorkSpaces Secure Browser의 무제한 인터넷 브라우징 활성화(권장)
- Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 활성화
- Amazon WorkSpaces Secure Browser용 인터넷 연결 포트

Amazon WorkSpaces Secure Browser의 무제한 인터넷 브라우징 활성화(권장)

아래 단계에 따라 무제한 인터넷 브라우징이 가능한 NAT 게이트웨이가 있는 VPC를 구성합니다. 이를 통해 WorkSpaces Secure Browser는 퍼블릭 인터넷상의 사이트 및 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 이 단계를 따릅니다.

> **Note**
>
> VPC를 이미 구성한 경우 다음 단계를 완료하여 VPC에 NAT 게이트웨이를 추가합니다. 새 VPC를 생성해야 하는 경우 Amazon WorkSpaces Secure Browser용 새 VPC 생성 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. 프라이빗 서브넷이 있는 VPC를 생성하는 방법에 대한 자세한 내용은 섹션을 참조하세요the section called “빠른 VPC 설정”.

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

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.

Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 활성화

WorkSpaces Secure Browser 포털의 권장 네트워크 설정은 NAT 게이트웨이를 사용하는 프라이빗 서브넷을 사용하는 것입니다. 이렇게 하면 포털에서 퍼블릭 인터넷 콘텐츠와 프라이빗 콘텐츠를 모두 브라우징할 수 있습니다. 자세한 내용은 the section called “무제한 인터넷 브라우징” 단원을 참조하십시오. 그러나 웹 프록시를 사용하여 WorkSpaces Secure Browser 포털에서 인터넷으로의 아웃바운드 통신을 제어해야 할 수 있습니다. 예를 들어 웹 프록시를 인터넷 게이트웨이로 사용하는 경우 도메인 허용 목록 및 콘텐츠 필터링과 같은 예방 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 프라이빗 콘텐츠가 있을 수 있습니다.

관리형 디바이스 또는 가상 환경의 이미지에서 프록시 설정을 구성하는 데 이미 익숙할 수 있습니다. 하지만 기업에서 소유하거나 관리하지 않는 디바이스를 사용자가 사용하고 있는 경우와 같이 디

바이스를 제어할 수 없거나 가상 환경의 이미지를 관리해야 하는 경우 문제가 발생할 수 있습니다. WorkSpaces Secure Browser를 사용하면 웹 브라우저에 내장된 Chrome 정책을 사용하여 프록시 설정을 설정할 수 있습니다. 이 작업은 WorkSpaces Secure Browser의 HTTP 아웃바운드 프록시를 설정하여 수행할 수 있습니다.

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

이 솔루션은 다음과 같은 이점을 제공합니다.

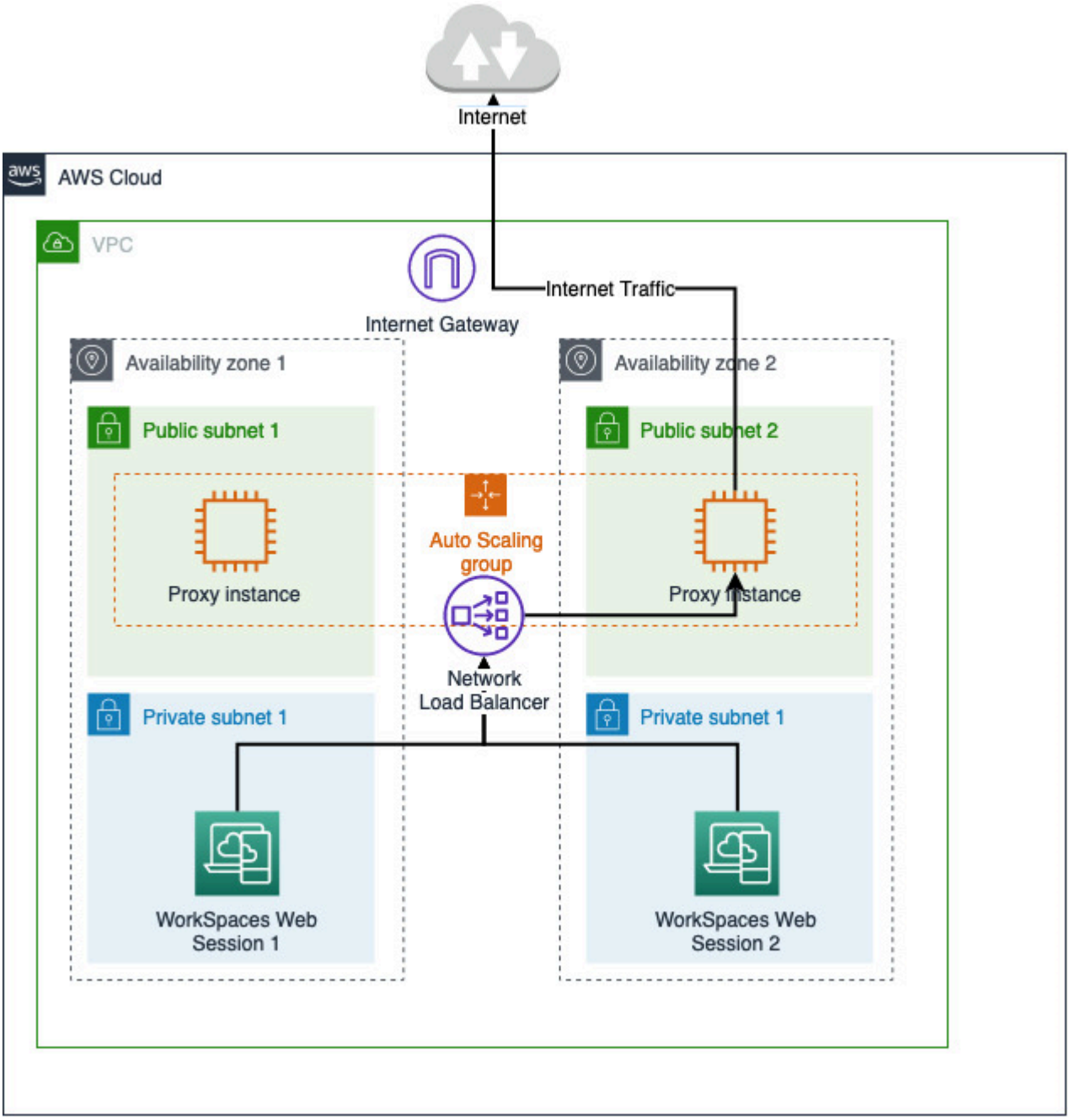
- Network Load Balancer에서 호스팅하는 오토 스케일링 Amazon EC2 인스턴스 그룹으로 구성된 아웃바운드 프록시. 프록시 인스턴스는 퍼블릭 서브넷에 있으며 각 인스턴스는 탄력적 IP로 연결되므로 인터넷에 액세스할 수 있습니다.
- 프라이빗 서브넷에 배포된 WorkSpaces Secure Browser 포털. 인터넷 액세스를 활성화하기 위해 NAT 게이트웨이를 구성할 필요가 없습니다. 대신 모든 인터넷 트래픽이 아웃바운드 프록시를 통과하도록 브라우저 정책을 구성합니다. 자체 프록시를 사용하려는 경우에도 WorkSpaces Secure Browser 포털 설정이 비슷합니다.

주제

- Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 아키텍처
- Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 사전 조건
- Amazon WorkSpaces Secure Browser용 HTTP 아웃바운드 프록시
- Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 문제 해결

Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 아키텍처

다음은 VPC에서 일반적인 프록시 설정의 예입니다. Amazon EC2 프록시 인스턴스는 퍼블릭 서브넷에 있으며 탄력적 IP로 연결되므로 인터넷에 액세스할 수 있습니다. Network Load Balancer는 프록시 인스턴스의 Auto Scaling 그룹을 호스팅합니다. 이를 통해 프록시 인스턴스가 자동으로 스케일 업되고 Network Load Balancer는 WorkSpaces Secure Browser 세션에서 사용할 수 있는 단일 프록시 엔드포인트가 됩니다.



Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 사전 조건

시작하기 전에 다음 사전 조건을 충족하는지 확인합니다.

- 이미 배포된 VPC가 필요하며, 퍼블릭 및 프라이빗 서브넷이 여러 가용 영역(AZ)에 분산되어 있어야 합니다. VPC 환경을 설정하는 방법에 대한 자세한 내용은 기본 VPC를 참조하세요.

- WorkSpaces Secure Browser 세션이 위치한 프라이빗 서브넷에서 액세스할 수 있는 단일 프록시 엔드포인트(예: Network Load Balancer DNS 이름)가 필요합니다. 기존 프록시를 사용하려면 프라이빗 서브넷에서 액세스할 수 있는 단일 엔드포인트가 있는지 확인합니다.

Amazon WorkSpaces Secure Browser용 HTTP 아웃바운드 프록시

WorkSpaces Secure Browser용 HTTP 아웃바운드 프록시를 설정하려면 다음 단계를 따릅니다.

1. VPC에 예제 아웃바운드 프록시를 배포하려면 도메인 화이트리스트 및 콘텐츠 필터링으로 아웃바운드 VPC 프록시를 설정하는 방법에 설명된 단계를 따릅니다.
   a. '설치(일회성 설정)'의 단계에 따라 CloudFormation 템플릿을 계정에 배포합니다. 올바른 VPC와 서브넷을 CloudFormation 템플릿 파라미터로 선택해야 합니다.
   b. 배포 후 CloudFormation 출력 파라미터 OutboundProxyDomain 및 OutboundProxyPort를 찾습니다. 이는 프록시의 DNS 이름과 포트입니다.
   c. 이미 자체 프록시가 있는 경우 이 단계를 건너뛰고 프록시의 DNS 이름과 포트를 사용합니다.
2. WorkSpaces Secure Browser 콘솔에서 포털을 선택한 다음 편집을 선택합니다.
   a. 네트워크 연결 세부 정보에서 프록시에 액세스할 수 있는 VPC 및 프라이빗 서브넷을 선택합니다.
   b. 정책 설정에서 JSON 편집기를 사용하여 다음 ProxySettings 정책을 추가합니다. `ProxyServer` 필드는 프록시의 DNS 이름과 포트여야 합니다. ProxySettings 정책에 대한 자세한 내용은 ProxySettings를 참조하세요.

```
{
    "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 Secure Browser 세션에서 Chrome이 관리자에게서 받은 프록시 설정을 사용 중입니다.가 표시되어 Chrome 설정에 프록시가 적용되었음을 확인할 수 있습니다.
4. chrome://policy 및 Chrome 정책 탭으로 이동하여 정책이 적용되었는지 확인합니다.
5. WorkSpaces Secure Browser 세션이 NAT 게이트웨이 없이도 인터넷 콘텐츠를 성공적으로 브라우징할 수 있는지 확인합니다. CloudWatch Logs에서 Squid 프록시 액세스 로그가 기록되었는지 확인합니다.

Amazon WorkSpaces Secure Browser의 제한된 인터넷 브라우징 문제 해결

Chrome 정책을 적용한 후에도 WorkSpaces Secure Browser 세션에서 여전히 인터넷에 액세스할 수 없는 경우 다음 단계에 따라 문제를 해결하세요.

- WorkSpaces Secure Browser 포털이 있는 프라이빗 서브넷에서 프록시 엔드포인트에 액세스할 수 있는지 확인합니다. 이를 확인하려면 프라이빗 서브넷에서 EC2 인스턴스를 생성하고 프라이빗 EC2 인스턴스에서 프록시 엔드포인트로의 연결을 테스트합니다.
- 프록시에서 인터넷에 액세스할 수 있는지 확인합니다.
- Chrome 정책이 올바른지 확인합니다.
  - 정책의 `ProxyServer` 필드가 `<Proxy DNS name>:<Proxy port>` 형식인지 확인합니다. 앞에 `http://` 또는 `https://`가 포함되지 않아야 합니다.
  - WorkSpaces Secure Browser 세션에서 Chrome을 사용하여 chrome://policy로 이동한 후 ProxySettings 정책이 성공적으로 적용되었는지 확인합니다.

Amazon WorkSpaces Secure Browser용 인터넷 연결 포트

각 WorkSpaces Secure Browser 스트리밍 인스턴스에는 고객 네트워크 인터페이스가 있어 VPC 내의 리소스에 연결할 수 있을 뿐만 아니라 NAT 게이트웨이가 있는 프라이빗 서브넷이 설정된 경우 인터넷에 연결할 수 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

WorkSpaces Secure Browser용 VPC 모범 사례

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 Secure Browser 서비스 할당량(한도라고도 함)이 예상 수요를 지원하기에 충분한지 확인합니다. 할당량 증가를 요청하려면 https://console.aws.amazon.com/servicequotas/에서 서비스 할당량 콘솔을 사용합니다. 기본 WorkSpaces Secure Browser 할당량에 대한 자세한 내용은 the section called “서비스 할당량 관리” 단원을 참조하세요.
- 인터넷에 액세스할 수 있는 스트리밍 세션을 제공하려는 경우 퍼블릭 서브넷에서 NAT 게이트웨이가 있는 VPC를 구성하는 것이 좋습니다.

탄력적 네트워크 인터페이스

- 스트리밍 기간 동안에는 각 WorkSpaces Secure Browser 세션에 고유한 탄력적 네트워크 인터페이스가 필요합니다. WorkSpaces Secure Browser의 경우 플릿에 필요한 최대 용량 만큼 탄력적 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

- 사용자 스케일 업 계획을 세울 때는 구성된 서브넷의 고유한 클라이언트 IP 주소가 각 WorkSpaces Secure Browser 세션에 필요합니다. 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 조정 여부를 고려하여 원하는 리전에서 WorkSpaces Secure Browser이 지원하는 고유한 가용 영역 각각에 서브넷을 구성하는 것이 좋습니다. 자세한 내용은 the section called “새 VPC 생성” 단원을 참조하십시오.
- 서브넷을 통해 웹 애플리케이션에 필요한 네트워크 리소스에 액세스할 수 있는지 확인합니다.

보안 그룹

- 보안 그룹을 사용하여 VPC에 대한 추가 액세스 제어를 제공합니다.

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

Amazon WorkSpaces Secure Browser에서 지원되는 가용 영역

WorkSpaces Secure Browser와 함께 사용할 가상 프라이빗 클라우드(VPC)를 생성하는 경우 VPC의 서브넷은 WorkSpaces Secure Browser를 시작하려는 리전의 다른 가용 영역에 있어야 합니다. 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` 리전의 AZ ID이며 모든 AWS 계정에서 위치가 동일합니다.

AZ ID를 확인하면 다른 계정의 리소스를 기준으로 한 계정의 리소스 위치를 확인할 수 있습니다. 예를 들어, AZ ID가 `use1-az2`인 가용 영역의 서브넷을 다른 계정과 공유하면 이 서브넷은 AZ ID가 `use1-az2`인 가용 영역의 계정에서 사용할 수 있습니다. 각 VPC 및 서브넷의 AZ ID가 Amazon VPC 콘솔에 표시됩니다.

WorkSpaces Secure Browser는 지원되는 각 리전의 일부 가용 영역에서만 사용 가능합니다. 다음 표에는 각 리전에 사용할 수 있는 AZ ID가 나와 있습니다. AZ ID를 계정의 가용 영역에 매핑하는 방법을 보려면 AWS RAM 사용 설명서의 리소스의 AZ ID를 참조하세요.

리전 이름	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(싱가포르)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
아시아 태평양(시드니)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
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 리전, 가용 영역 및 로컬 영역을 참조하세요.

Amazon WorkSpaces Secure Browser에 대한 사용자 연결 활성화

WorkSpaces Secure Browser는 퍼블릭 인터넷을 통해 스트리밍 연결을 라우팅하도록 구성되어 있습니다. 따라서 사용자를 인증하고, WorkSpaces Secure Browser 작동에 필요한 웹 자산을 전송하려면 인터넷 연결이 필요합니다. 이러한 트래픽을 허용하려면 Amazon WorkSpaces Secure Browser에 허용되는 도메인 섹션에 나열된 도메인을 허용해야 합니다.

다음 주제에서는 WorkSpaces Secure Browser에 대한 사용자 연결을 활성화하는 방법에 대해 설명합니다.

주제

- Amazon WorkSpaces Secure Browser의 IP 주소 및 포트 요구 사항
- Amazon WorkSpaces Secure Browser에 허용되는 도메인

Amazon WorkSpaces Secure Browser의 IP 주소 및 포트 요구 사항

WorkSpaces Secure Browser 인스턴스에 액세스하려면 다음 포트를 통해 사용자 디바이스로 아웃바운드 액세스를 해야 합니다.

- 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 Amazon WorkSpaces Secure Browser에 허용되는 도메인에 나열된 필수 도메인에 개방되어 있어야 합니다.
  - AWS 는 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. 또는를 사용하는 경우 Get-AWSPublicIpAddressRange PowerShell 명령을 사용하여 동일한 정보에 액세스할 AWS Tools for Windows PowerShell수 있습니다. 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.

Amazon WorkSpaces Secure Browser에 허용되는 도메인

사용자 로컬 브라우저에서 WorkSpaces Secure Browser 서비스에 액세스할 수 있으려면 사용자가 서비스에 액세스하려는 네트워크에서 다음 도메인을 허용 목록에 추가해야 합니다.

다음 표에서 *{region}*은 운영 웹 포털의 리전 코드로 바꿉니다. 예를 들어, 유럽(아일랜드) 지역 웹 포털의 경우 s3.*{region}*.amazonaws.com은 s3.eu-west-1.amazonaws.com이어야 합니다. 리전 코드 목록은 Amazon WorkSpaces Secure Browser 엔드포인트 및 할당량을 참조하세요.

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

구성된 ID 제공업체에 따라 추가 도메인 목록을 표시하도록 허용해야 할 수도 있습니다. WorkSpaces Secure Browser에서 해당 제공업체를 사용하기 위해 허용 목록에 추가해야 할 도메인을 식별하려면

해당 IdP의 설명서를 검토합니다. IAM Identity Center를 사용하는 경우 자세한 내용은 IAM Identity Center 사전 조건을 참조하십시오.

Amazon WorkSpaces Secure Browser 시작하기

다음 단계에 따라 WorkSpaces Secure Browser 포털을 생성하고, 기존 브라우저에서 내부 및 SaaS 웹 사이트에 액세스할 수 있는 권한을 사용자에게 제공합니다. 계정별로 지원되는 모든 리전에 하나의 웹 포털을 생성할 수 있습니다.

> **Note**
>
> 둘 이상의 포털에 대한 한도 증가를 요청하려면 AWS 계정 ID, 요청할 포털 수 및를 사용하여 지원팀에 문의하십시오 AWS 리전.

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

웹 포털 설정에는 비용이 들지 않습니다. WorkSpaces Secure Browser는 서비스를 적극적으로 사용하는 사용자를 위한 합리적인 월별 요금 등 종량제 요금을 청구합니다. 선불 비용, 라이선스 또는 장기 약정이 필요 없습니다.

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

주제

- Amazon WorkSpaces Secure Browser용 웹 포털 생성
- Amazon WorkSpaces Secure Browser에서 웹 포털 테스트
- Amazon WorkSpaces Secure Browser에서 웹 포털 배포

Amazon WorkSpaces Secure Browser용 웹 포털 생성

웹 포털을 생성하려면 아래 단계를 따릅니다.

주제

- Amazon WorkSpaces Secure Browser용 네트워크 설정 구성
- Amazon WorkSpaces Secure Browser에 대한 포털 설정 구성
- Amazon WorkSpaces Secure Browser에 대한 사용자 설정 구성
- Amazon WorkSpaces Secure Browser의 ID 제공업체 구성
- Amazon WorkSpaces Secure Browser를 사용하여 웹 포털 시작

Amazon WorkSpaces Secure Browser용 네트워크 설정 구성

WorkSpaces Secure Browser용 네트워크 설정을 구성하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 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 액세스하려는 콘텐츠에 연결할 수 있는 VPC를 선택합니다.
    2. 다음 요구 사항을 충족하는 프라이빗 서브넷을 최대 3개까지 선택합니다. 자세한 내용은 Amazon WorkSpaces Secure Browser용 네트워킹 단원을 참조하십시오.
        - 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

Amazon WorkSpaces Secure Browser에 대한 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 유형의 드롭다운 메뉴에서 웹 포털의 인스턴스 유형을 선택합니다. 그런 다음 웹 포털의 최대 동시 사용자 한도를 입력합니다. 자세한 내용은 the section called “서비스 할당량 관리” 단원을 참조하십시오.

> **Note**
>
> 새 인스턴스 유형을 선택하면 월별 활성 사용자당 비용이 변경됩니다. 자세한 내용은 Amazon WorkSpaces Secure Browser 요금을 참조하세요.

3. 사용자 지정 도메인에서 기본 포털 엔드포인트 대신 자체 도메인 이름을 통해 액세스할 수 있도록 포털의 사용자 지정 도메인을 구성할 수 있습니다. 자세한 내용은 the section called “사용자 지정 도메인” 단원을 참조하십시오. 이는 선택 사항입니다.
4. 세션 로거에서 세션 로그 파일을 저장할 S3 버킷을 지정할 수 있습니다. 자세한 내용은 the section called “세션 로거 설정” 단원을 참조하십시오. 이는 선택 사항입니다.
5. 사용자 액세스 로깅의 Kinesis 스트림 ID에서 로그 파일을 전송할 Amazon Kinesis 데이터 스트림을 선택합니다. 자세한 내용은 the section called “사용자 활동 로깅 설정” 단원을 참조하십시오. 이는 선택 사항입니다.
6. IP 액세스 제어에서 신뢰할 수 있는 네트워크에 대한 액세스를 제한할지 여부를 선택합니다. 자세한 내용은 the section called “IP 액세스 제어 관리” 단원을 참조하십시오. 이는 선택 사항입니다.
7. 데이터 보호 설정에서 WorkSpaces Secure Browser에 대한 정책을 생성하여 민감한 정보를 수정할 수 있습니다. 자세한 내용은 the section called “데이터 보호 설정” 단원을 참조하십시오. 이는 선택 사항입니다.
8. URL 필터링에서 최종 사용자가 특정 URLs 또는 도메인 범주에 액세스하거나 차단하여 액세스를 제한할 수 있는 URLs을 지정할 수 있습니다. 자세한 내용은 the section called “웹 콘텐츠 필터링” 단원을 참조하십시오. 이는 선택 사항입니다.

    1. 세션 브라우징을 선택한 몇 개의 도메인으로 제한하려면 모든 URLs 차단 토글을 활성화하고 URL 추가를 클릭하여 최종 사용자가 액세스할 수 있는 URLs 목록을 제공합니다.
    2. 최종 사용자의 차단할 URLs 목록을 생성하려면 URL 추가를 클릭하여 차단할 단일 URLs 나열하거나 범주 추가를 클릭하여 차단된 도메인 범주(예: 소셜 네트워킹)를 선택합니다.
9. 정책 설정에서 웹 포털의 안정적인 최신 버전에 사용할 수 있는 Chrome 정책을 사용하여 브라우저 정책을 설정할 수 있습니다. 자세한 내용은 the section called “브라우저 정책 관리” 단원을 참조하십시오. 이는 선택 사항입니다.

    1. 시각적 편집기에서 가장 일반적인 정책 중 일부를 빠르게 선택할 수 있습니다.
        - 시작 URL - 선택 사항에서 사용자가 브라우저를 시작할 때 홈 페이지로 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 내용은 the section called "사용자 활동 로깅 설정" 단원을 참조하십시오.

- 브라우저 북마크 - 선택 사항의 경우 사용자가 브라우저에서 보려는 북마크의 표시 이름, 도메인 및 폴더를 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.

2. 시각적 편집기 대신 JSON 편집기를 사용하여 정책을 직접 추가하거나 편집할 수도 있습니다. 정책의 특정 형식은 Chrome Enterprise 정책 목록을 참조하세요.
3. JSON 파일을 웹 포털에 업로드하여 조직에서 사용되는 Chrome 정책을 가져올 수도 있습니다. 자세한 내용은 섹션을 참조하세요. the section called "자습서: 사용자 지정 브라우저 정책 설정"

   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.

10. 포털에 태그를 추가합니다. 태그를 사용하여 AWS 리소스를 검색하거나 필터링할 수 있습니다. 태그는 키와 선택적 값으로 구성되며 포털 리소스와 연결됩니다. 이는 선택 사항입니다.
11. 다음을 선택하여 계속 진행합니다.

Amazon WorkSpaces Secure Browser에 대한 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. 브랜딩 사용자 지정에서 시각적 요소, 텍스트 콘텐츠 및 서비스 약관을 수정하여 최종 사용자에게 표시되는 로그인 및 로드 화면을 사용자 지정할 수 있습니다. 자세한 내용은 the section called "브랜딩 사용자 지정" 단원을 참조하십시오. 이는 선택 사항입니다.

2. 권한에서 Single Sign-On에 대한 확장을 활성화할지 여부를 선택합니다. 자세한 내용은 the section called “Single Sign-On 확장 프로그램 관리” 단원을 참조하십시오.
3. 사용자가 웹 포털에서 로컬 디바이스로 인쇄할 수 있도록 허용하려면 허용 또는 허용되지 않음을 선택합니다.
4. 사용자가 웹 포털로 딥링크할 수 있도록 허용하려면 허용 또는 허용되지 않음을 선택합니다. 딥링크에 대한 자세한 내용은 the section called “딥 링크” 단원을 참조하세요.
5. 사용자가 포털 세션에서 로컬 인증을 사용하도록 허용에서 허용 또는 허용되지 않음을 선택합니다. 웹 인증에 대한 자세한 내용은 섹션을 참조하세요the section called “웹 인증 리디렉션”.
6. 도구 모음 제어의 기능에서 원하는 설정을 선택합니다.
7. 설정에서 도구 모음 상태(도크 또는 분리됨), 테마(어두움 또는 밝음 모드), 아이콘 가시성, 세션의 최대 디스플레이 해상도를 포함하여 세션 시작 시 도구 모음 프레젠테이션 보기를 관리합니다. 최종 사용자에게 이러한 옵션을 완전히 제어할 수 있도록 이러한 설정을 구성하지 않은 상태로 둡니다. 자세한 내용은 the section called “도구 모음 제어” 단원을 참조하십시오.
8. 세션 제한 시간에 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. 비활성으로 인해 연결이 끊기 전에 사용자에게 알림이 전송됩니다. 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**
     >
     > 사용자는 스트리밍 세션 중에 키보드 또는 마우스 입력 제공을 중지하면 유휴 상태로 간주됩니다. 파일 업로드와 다운로드, 오디오 인, 오디오 아웃, 픽셀 변경은 사용자 활성 상

태로 인정되지 않습니다. 유휴 연결 해제 제한 시간(분)의 시간 간격이 경과된 후에도 사용자가 계속 유휴 상태이면 연결이 해제됩니다.

Amazon WorkSpaces Secure Browser의 ID 제공업체 구성

다음 단계에 따라 ID 제공업체(IdP)를 구성할 수 있습니다.

주제

- Amazon WorkSpaces Secure Browser의 ID 제공업체 유형 선택
- Amazon WorkSpaces Secure Browser의 ID 제공업체 유형 변경

Amazon WorkSpaces Secure Browser의 ID 제공업체 유형 선택

WorkSpaces Secure Browser는 표준 및 AWS IAM Identity Center라는 두 가지 인증 유형을 제공합니다. ID 제공업체 구성 페이지에서 포털에 사용할 인증 유형을 선택합니다.

- 표준(기본 옵션)의 경우 타사 SAML 2.0 ID 제공업체(예: Okta 또는 Ping)를 포털과 직접 페더레이션합니다. 자세한 내용은 the section called “표준 인증 유형” 단원을 참조하십시오. 표준 유형은 SP 시작 인증과 IdP 시작 인증 플로를 모두 지원합니다.
- IAM Identity Center(고급 옵션)의 경우 IAM Identity Center를 포털과 페더레이션합니다. 이 인증 유형을 사용하려면 IAM Identity Center와 WorkSpaces Secure Browser 포털이 모두 동일한 AWS 리전에 있어야 합니다. 자세한 내용은 the section called “IAM Identity Center 인증 유형” 단원을 참조하십시오.

주제

- Amazon WorkSpaces Secure Browser의 표준 인증 유형 구성
- Amazon WorkSpaces Secure Browser의 IAM Identity Center 인증 유형 구성

Amazon WorkSpaces Secure Browser의 표준 인증 유형 구성

표준 인증 유형은 기본 인증 유형입니다. 이 유형은 SAML 2.0 준수 IdP와 함께 서비스 제공업체 시작(SP 시작) 및 ID 제공업체 시작(IdP 시작) 로그인 플로를 지원할 수 있습니다. 표준 인증 유형을 구성하려면 아래 단계에 따라 타사 SAML 2.0 IdP(예: Okta 또는 Ping)를 포털과 직접 페더레이션합니다.

주제

- Amazon WorkSpaces Secure Browser의 ID 제공업체 구성
- 자체 IdP에서 IdP 구성
- Amazon WorkSpaces Secure Browser에서 IdP 구성 완료
- Amazon WorkSpaces Secure Browser에서 특정 IdP를 사용하기 위한 지침

Amazon WorkSpaces Secure Browser의 ID 제공업체 구성

다음 단계에 따라 ID 제공업체를 구성합니다.

1. 생성 마법사의 ID 제공업체(IdP) 구성 페이지에서 표준을 선택합니다.
2. 표준 IdP로 계속 진행을 선택합니다.
3. SP 메타데이터 파일을 다운로드하고 개별 메타데이터 값에 대한 탭을 열어둡니다.
   - SP 메타데이터 파일을 사용할 수 있는 경우 메타데이터 파일 다운로드를 선택하여 서비스 제공업체(SP) 메타데이터 문서를 다운로드하고, 다음 단계에서 서비스 제공업체 메타데이터 파일을 IdP에 업로드합니다. 이렇게 하지 않으면 사용자가 로그인할 수 없습니다.
   - 제공업체에서 SP 메타데이터 파일을 업로드하지 않은 경우 메타데이터 값을 수동으로 입력합니다.
4. SAML 로그인 유형 선택에서 SP 시작 및 IdP 시작 SAML 어설션 또는 SP에서 시작한 SAML 어설션만 해당을 선택합니다.
   - SP 시작 및 IdP 시작 SAML 어설션을 사용하면 포털에서 두 가지 유형의 로그인 플로를 모두 지원할 수 있습니다. IdP 시작 플로를 지원하는 포털에서는 사용자가 포털 URL을 방문하여 세션을 시작하지 않아도 서비스 ID 페더레이션 엔드포인트에 SAML 어설션을 제공할 수 있습니다.
     - 요청하지 않은 IdP 시작 SAML 어설션을 포털에서 수락하도록 허용하려면 이 옵션을 선택합니다.
     - 이 옵션을 사용하려면 SAML 2.0 ID 제공업체에서 기본 릴레이 상태를 구성해야 합니다. 포털의 릴레이 상태 파라미터는 콘솔의 IdP 시작 SAML 로그인 아래에 있거나, `<md:IdPInitRelayState>`의 SP 메타데이터 파일에서 복사할 수 있습니다.
     - Note
       - 릴레이 상태의 형식: `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=ExIdentity-Provider`
       - SP 메타데이터 파일에서 값을 복사하여 붙여넣는 경우 `&amp;` 를 &로 변경해야 합니다. `&amp;`는 XML 이스케이프 문자입니다.

- 포털에서 SP 시작 로그인 플로만 지원하도록 하려면 SP에서 시작한 SAML 어설션만 해당을 선택합니다. 이 옵션은 IdP 시작 로그인 플로에서 요청하지 않은 SAML 어설션을 거부합니다.

> **Note**
>
> 일부 타사 IdP를 사용하면 SP 시작 플로를 활용하여 IdP 시작 인증 환경을 제공할 수 있는 사용자 지정 SAML 애플리케이션을 생성할 수 있습니다. 예를 들어 Okta 북마크 애플리케이션 추가를 참조하십시오.

5. 이 공급자에 대한 SAML 요청에 서명을 활성화할지 여부를 선택합니다. SP 시작 인증을 사용하면 IdP를 통해 인증 요청이 포털에서 발생한 것인지 확인할 수 있으므로 다른 타사 요청이 수락되지 않습니다.

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

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

> **Note**
>
> RSA-SHA256은 유일하게 지원되는 요청 및 기본 요청 서명 알고리즘입니다.

6. 암호화된 SAML 어설션 필요를 활성화할지 여부를 선택합니다. 활성화하면 IdP에서 제공하는 SAML 어설션을 암호화할 수 있습니다. 이를 통해 IdP와 WorkSpaces Secure Browser 간의 SAML 어설션에서 데이터 가로채기를 방지할 수 있습니다.

> **Note**
>
> 이 단계에서는 암호화 인증서를 사용할 수 없습니다. 포털을 시작한 후에 생성됩니다. 포털을 시작한 후 암호화 인증서를 다운로드하여 IdP에 업로드합니다. 그런 다음 IdP에서 어설션 암호화를 활성화합니다. 이름은 IdP에 따라 다를 수 있습니다.

7. 단일 로그아웃을 활성화할지 여부를 선택합니다. 단일 로그아웃을 사용하면 최종 사용자가 한 번의 작업으로 IdP와 WorkSpaces Secure Browser 세션에서 모두 로그아웃할 수 있습니다.

   a. WorkSpaces Secure Browser에서 서명 인증서를 다운로드하여 IdP에 업로드합니다. 이 인증서는 이전 단계의 요청 서명에 사용된 것과 동일한 서명 인증서입니다.

   b. 단일 로그아웃을 사용하려면 SAML 2.0 ID 제공업체에서 단일 로그아웃 URL을 구성해야 합니다. 포털의 단일 로그아웃 URL은 콘솔의 서비스 제공업체(SP) 세부 정보 - 개별 메타데이터 값 표

시에서 찾거나 <md:SingleLogoutService> 아래의 SP 메타데이터 파일에서 찾을 수 있습니다.

c. IdP에서 단일 로그아웃을 활성화합니다. IdP에 따라 이름이 다를 수 있습니다.

자체 IdP에서 IdP 구성

자체 IdP에서 IdP를 구성하려면 다음 단계를 따릅니다.

1. 브라우저에서 새 탭이 열립니다.
2. SAML IdP에 포털 메타데이터를 추가합니다.

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

   이 프로세스의 세부 사항은 제공업체마다 다를 수 있습니다. IdP 구성에 포털 세부 정보를 추가하는 방법에 대한 도움말은 the section called “특정 IdP에 대한 지침”에서 제공업체의 설명서를 참조하세요.
3. SAML 어설션의 NameID를 확인합니다.

   SAML IdP가 SAML 어설션의 NameID를 사용자 이메일 필드로 채우는지 확인합니다. NameID 및 사용자 이메일은 포털에서 SAML 페더레이션 사용자를 고유하게 식별하는 데 사용됩니다. 영구 SAML 이름 ID 형식을 사용합니다.
4. 선택 사항: IdP 시작 인증을 위한 릴레이 상태를 구성합니다.

   이전 단계에서 SP 시작 및 IdP 시작 SAML 어설션 수락을 선택한 경우 the section called “WorkSpaces Secure Browser의 IdP 구성”의 2단계에 따라 IdP 애플리케이션의 기본 릴레이 상태를 설정합니다.
5. 선택 사항: 요청 서명을 구성합니다. 이전 단계에서 이 공급자에 대한 SAML 요청에 서명을 선택한 경우 the section called “WorkSpaces Secure Browser의 IdP 구성”의 3단계에 따라 서명 인증서를 IdP에 업로드하고 요청 서명을 활성화합니다. Okta와 같은 일부 IdP의 경우 요청 서명을 사용하려면 NameID가 ‘영구’ 유형에 속해야 할 수 있습니다. 위의 단계에 따라 SAML 어설션의 NameID를 확인해야 합니다.
6. 선택 사항: 어설션 암호화를 구성합니다. 이 제공업체에서 암호화된 SAML 어설션 필요를 선택한 경우 포털 생성이 완료될 때까지 기다린 다음 아래 ‘메타데이터 업로드’의 4단계에 따라 암호화 인증서를 IdP에 업로드하고 어설션 암호화를 사용 활성화합니다.

7. 선택 사항: 단일 로그아웃을 구성합니다. 단일 로그아웃을 선택한 경우 the section called "WorkSpaces Secure Browser의 IdP 구성"의 5단계에 따라 서명 인증서를 IdP에 업로드하고 단일 로그아웃 URL을 입력한 다음 단일 로그아웃을 활성화합니다.
8. WorkSpaces Secure Browser를 사용할 수 있도록 IdP 사용자에게 액세스 권한을 부여합니다.
9. IdP에서 메타데이터 교환 파일을 다운로드합니다. 다음 단계에서 이 메타데이터를 WorkSpaces Secure Browser에 업로드합니다.

Amazon WorkSpaces Secure Browser에서 IdP 구성 완료

WorkSpaces Secure Browser에서 IdP 구성을 완료하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔로 돌아갑니다. 생성 마법사의 ID 제공업체 구성 페이지의 IdP 메타데이터에서 메타데이터 파일을 업로드하거나 IdP의 메타데이터 URL을 입력합니다. 포털에서는 IdP의 이 메타데이터를 사용하여 트러스트를 설정합니다.
2. 메타데이터 파일을 업로드하려면 IdP 메타데이터 문서에서 파일 선택을 선택합니다. 이전 단계에서 다운로드한 IdP로부터 XML 형식의 메타데이터 파일을 업로드합니다.
3. 메타데이터 URL을 사용하려면 이전 단계에서 설정한 IdP로 이동하여 메타데이터 URL을 가져옵니다. WorkSpaces Secure Browser 콘솔로 돌아가서 IdP 메타데이터 URL 아래에 IdP에서 가져온 메타데이터 URL을 입력합니다.
4. 완료되면 다음을 선택합니다.
5. 이 제공업체에서 암호화된 SAML 어설션 필요 옵션을 활성화한 포털의 경우 포털 IdP 세부 정보 섹션에서 암호화 인증서를 다운로드하여 IdP에 업로드해야 합니다. 그런 다음 거기서 옵션을 활성화할 수 있습니다.

> **Note**
>
> WorkSpaces Secure Browser를 사용하려면 IdP 설정의 SAML 어설션에 subject 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 Secure Browser를 사용하려면 SAML 응답에 다음 클레임이 있어야 합니다. *<SP Entity ID>* 및 *<SP ACS URL>*은 콘솔 또는 CLI를 통해 포털의 서비스 제공업체 세부 정보 또는 메타데이터 문서에서 찾을 수 있습니다.
>
> - 응답 대상으로 `Audience` 값이 SP Entity ID로 설정된 `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>">
```

- `Recipient` 값이 SP ACS URL이고 `InResponseTo` 값이 원래 SAML 요청 ID와 일치하는 `SubjectConfirmationData` 클레임. 예제:

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

WorkSpaces Secure Browser는 요청 파라미터와 SAML 어설션을 검증합니다. IdP 시작 SAML 어설션의 경우 요청 세부 정보가 HTTP POST 요청 본문에서 `RelayState` 파라미터로 형식화되어 있어야 합니다. 요청 본문에 SAML 어설션도 `SAMLResponse` 파라미터로 포함되어야 합니다. 이전 단계를 수행했다면 이 두 가지가 모두 있어야 합니다.
다음은 IdP 시작 SAML 제공업체에 대한 `POST` 본문 예시입니다.

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

Amazon WorkSpaces Secure Browser에서 특정 IdP를 사용하기 위한 지침

포털에 대해 SAML 페더레이션을 올바르게 구성하려면 아래 링크에서 일반적으로 사용되는 IdP의 설명서를 참조하세요.

IdP	SAML 애플리케이션 설정	사용자 관리	IdP 시작 인증	요청 서명	어설션 암호화	단일 로그아웃
Okta	SAML 앱 통합 생성	사용자 관리	애플리케이션 통합 마	애플리케이션 통합 마	애플리케이션 통합 마	애플리케이션 통합 마

IdP	SAML 애플리케이션 설정	사용자 관리	IdP 시작 인증	요청 서명	어설션 암호화	단일 로그아웃
			법사 SAML 필드 참조	법사 SAML 필드 참조	법사 SAML 필드 참조	법사 SAML 필드 참조
Entra	자체 애플리케이션 생성	빠른 시작: 사용자 계정 생성 및 할당	엔터프라이즈 애플리케이션에 대한 Single Sign-On 활성화	SAML 요청 서명 확인	Microsoft Entra SAML 토큰 암호화 구성	Single Sign-Out SAML 프로토콜
Ping	SAML 애플리케이션 추가	Users	IdP 시작 SSO 활성화	PingOne for Enterprise에서 인증 요청 서명 구성	PingOne for Enterprise에서 암호화를 지원하나요?	SAML 2.0 단일 로그아웃
One Login	SAML 사용자 지정 커넥터(고급) (4266907)	OneLogin에 수동으로 사용자 추가	SAML 사용자 지정 커넥터(고급) (4266907)	SAML 사용자 지정 커넥터(고급) (4266907)	SAML 사용자 지정 커넥터(고급) (4266907)	SAML 사용자 지정 커넥터(고급) (4266907)
IAM Identity Center	자체 SAML 2.0 애플리케이션 설정	자체 SAML 2.0 애플리케이션 설정	자체 SAML 2.0 애플리케이션 설정	해당 사항 없음	해당 사항 없음	해당 사항 없음

Amazon WorkSpaces Secure Browser의 IAM Identity Center 인증 유형 구성

IAM Identity Center 유형(고급)의 경우 IAM Identity Center를 포털과 페더레이션합니다. 다음에 해당하는 경우에만 이 옵션을 선택합니다.

- IAM Identity Center는 웹 포털 AWS 리전 과 동일한 AWS 계정 및에 구성됩니다.
- 를 사용하는 경우 관리 계정을 AWS Organizations사용합니다.

IAM Identity Center 인증 유형을 사용하여 웹 포털을 생성하기 전에 IAM Identity Center를 독립형 제공업체로 설정해야 합니다. 자세한 내용은 AM Identity Center에서 일반 작업 시작하기를 참조하세요. 또는 SAML 2.0 IdP를 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 외부 ID 제공업체에 연결을 참조하세요. 그렇지 않으면 웹 포털에 할당할 사용자나 그룹이 없게 됩니다.

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

> **Note**
>
> 이 인증 유형을 사용하려면 IAM Identity Center가 WorkSpaces Secure Browser 포털 AWS 리전 과 동일한 AWS 계정 및에 있어야 합니다. IAM Identity Center가 별도의 AWS 계정 또는에 있는 경우 표준 인증 유형에 대한 지침을 AWS 리전따릅니다. 자세한 내용은 the section called “표준 인증 유형” 단원을 참조하십시오.
> 를 사용하는 경우 관리 계정을 사용하여 IAM Identity Center와 통합된 WorkSpaces Secure Browser 포털만 생성할 AWS Organizations수 있습니다.

주제

- IAM Identity Center를 통해 웹 포털 생성
- IAM Identity Center를 통해 웹 포털 관리
- 기존 웹 포털에 사용자 및 그룹 추가
- 웹 포털의 사용자 및 그룹 보기 또는 제거

IAM Identity Center를 통해 웹 포털 생성

IAM Identity Center를 통해 웹 포털을 생성하려면 다음 단계를 따릅니다.

IAM Identity Center를 통해 웹 포털을 생성하려면

1. 4단계: ID 제공업체 구성에서 포털을 생성하는 동안 AWS IAM Identity Center를 선택합니다.
2. IAM Identity Center로 계속 진행을 선택합니다.
3. 사용자 및 그룹 할당 페이지에서 사용자 및/또는 그룹 탭을 선택합니다.
4. 포털에 추가하려는 사용자 또는 그룹 옆의 확인란을 선택합니다.
5. 포털을 생성한 후에는 연결한 사용자가 IAM Identity Center 사용자 이름과 암호를 사용하여 WorkSpaces Secure Browser에 로그인할 수 있습니다.

IAM Identity Center를 통해 웹 포털 관리

IAM Identity Center를 통해 웹 포털을 관리하려면 다음 단계를 따릅니다.

IAM Identity Center를 통해 웹 포털을 관리하려면

1. 생성한 웹 포털은 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

기존 웹 포털에 사용자와 그룹을 추가하려면 다음 단계를 따릅니다.

기존 웹 포털에 사용자 및 그룹을 추가하려면

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 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. 이 작업은 WorkSpaces Secure Browser 포털의 편집 페이지에서 수행해야 합니다.

웹 포털의 사용자 및 그룹 보기 또는 제거

웹 포털의 사용자와 그룹을 보거나 제거하려면 할당된 사용자 테이블에서 제공하는 작업을 사용합니다. 자세한 내용은 애플리케이션 액세스 관리를 참조하세요.

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

Amazon WorkSpaces Secure Browser의 ID 제공업체 유형 변경

포털의 인증 유형은 언제든지 변경할 수 있습니다. 이를 수행하려면 다음 단계를 따릅니다.

- IAM Identity Center에서 표준으로 변경하려면 the section called “표준 인증 유형”에 설명된 단계를 따릅니다.
- 표준에서 IAM Identity Center로 변경하려면 the section called “IAM Identity Center 인증 유형”에 설명된 단계를 따릅니다.

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

`UpdatePortal` 이벤트를 검사하여 AWS CloudTrail 를 통해 포털의 자격 증명 공급자 유형 변경 사항을 볼 수 있습니다. 유형은 이벤트의 요청 및 응답 페이로드에서 볼 수 있습니다.

Amazon WorkSpaces Secure Browser를 사용하여 웹 포털 시작

웹 포털 구성이 완료되면 다음 단계에 따라 웹 포털을 시작할 수 있습니다.

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.

Amazon WorkSpaces Secure Browser에서 웹 포털 테스트

웹 포털을 생성한 후 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 Amazon WorkSpaces Secure Browser에서 웹 포털 배포의 단계를 수행할 수 있습니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 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 Secure Browser 로그인 페이지에서 로그인, SAML을 선택하고 SAML 자격 증명을 입력합니다.
5. 세션 준비 중 페이지가 표시되면 WorkSpaces Secure Browser 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.

Amazon WorkSpaces Secure Browser에서 웹 포털 배포

사용자가 WorkSpaces Secure Browser를 사용할 준비가 되면 다음 옵션 중에서 선택하여 포털을 배포합니다.

- 사용자가 IdP에서 직접 세션을 시작할 수 있도록 SAML 애플리케이션 게이트웨이에 포털을 추가합니다. 이 작업은 SAML 2.0 준수 IdP를 사용하여 IdP 시작 로그인 플로를 통해 수행할 수 있습니다. 자세한 내용은 the section called “표준 인증 유형”에서 SP 시작 및 IdP 시작 SAML 어설션을 참조하세요. 또는 SP 시작 플로를 사용하여 IdP 시작 인증 환경을 제공할 수 있는 사용자 지정 SAML 애플리케이션을 생성할 수 있습니다. 자세한 내용은 북마크 앱 통합 생성을 참조하세요.
- 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.
- 사용자에게 보다 통합된 브랜딩 경험을 제공하기 위해 포털 URL 대신 포털에 대해 사용자 지정 도메인을 설정한 경우 사용자 지정 도메인을 사용합니다. 자세한 내용은 the section called “사용자 지정 도메인” 단원을 참조하십시오.

Amazon WorkSpaces Secure Browser에서 웹 포털 관리

웹 포털을 설정한 후에는 다음 작업을 수행하여 관리할 수 있습니다.

주제

- Amazon WorkSpaces Secure Browser에서 웹 포털 세부 정보 보기
- Amazon WorkSpaces Secure Browser에서 웹 포털 편집
- Amazon WorkSpaces Secure Browser에서 웹 포털 삭제
- Amazon WorkSpaces Secure Browser에서 포털의 서비스 할당량 관리
- Amazon WorkSpaces Secure Browser에서 SAML IdP 토큰 재인증 간격 제어
- Amazon WorkSpaces Secure Browser에서 사용자 활동 로깅 설정
- Amazon WorkSpaces Secure Browser에서 브라우저 정책 관리
- Amazon WorkSpaces Secure Browser용 입력 방법 편집기 구성
- Amazon WorkSpaces Secure Browser에 대한 세션 내 현지화 구성
- Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 관리
- Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램 관리
- Amazon WorkSpaces Secure Browser의 웹 콘텐츠 필터링
- Amazon WorkSpaces Secure Browser의 딥 링크
- Amazon WorkSpaces Secure Browser에서 세션 관리 대시보드 사용
- FIPS 엔드포인트 및 Amazon WorkSpaces Secure Browser를 사용하여 전송 중 데이터 보호
- Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 관리
- Amazon WorkSpaces Secure Browser의 브랜딩 사용자 지정
- Amazon WorkSpaces Secure Browser에서 WebAuthn 리디렉션 지원 활성화
- Amazon WorkSpaces Secure Browser에서 도구 모음 제어 관리
- 포털에 대한 사용자 지정 도메인 구성

Amazon WorkSpaces Secure Browser에서 웹 포털 세부 정보 보기

웹 포털 세부 정보를 보려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.

2. WorkSpaces Secure Browser, 웹 포털을 차례로 선택하고 웹 포털을 선택한 다음 세부 정보 보기를 선택합니다.

Amazon WorkSpaces Secure Browser에서 웹 포털 편집

웹 포털을 편집하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 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.

Amazon WorkSpaces Secure Browser에서 웹 포털 삭제

웹 포털을 삭제하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 선택하고 웹 포털을 선택한 다음 삭제를 선택합니다.

Amazon WorkSpaces Secure Browser에서 포털의 서비스 할당량 관리

를 생성하면 리소스 사용에 대한 기본 서비스 할당량(한도라고도 함)이 AWS 계정자동으로 설정됩니다 AWS 서비스. 관리자는 두 가지 할당량을 알고 있어야 하며, 사용 사례를 지원하기 위해 할당량을 늘려야 할 수도 있습니다. 이 두 가지 할당량은 각 리전에서 생성할 수 있는 웹 포털 수와 각 리전에서 사용

가능한 각 인스턴스 유형으로 지원할 수 있는 최대 동시 세션 수입니다. AWS 콘솔의 Service Quotas 페이지에서 이에 대한 증가를 요청할 수 있습니다.

다음 표에는 기본 서비스 할당량 한도가 나와 있습니다.

계정 AWS 리전 별 내의 기본 할당량	값
웹 포털	3
최대 동시 세션 - standard.regular	25
최대 동시 세션 - standard.large	10
최대 동시 세션 - standard.xlarge	5

각 리전의 계정에 할당된 서비스 할당량을 보려면 Service Quotas 페이지를 참조하세요.

> **Important**
>
> 서비스 할당량은 AWS 리전 한 번에 하나씩 적용됩니다. 리소스 AWS 리전 가 더 필요한 각에서 서비스 할당량 증가를 요청해야 합니다. 자세한 내용은 Amazon WorkSpaces Secure Browser 엔드포인트 및 할당량을 참조하세요.

주제

- Amazon WorkSpaces Secure Browser에서 서비스 할당량 증가 요청
- Amazon WorkSpaces Secure Browser에서 포털 증가 요청
- Amazon WorkSpaces Secure Browser에서 최대 동시 세션 증가 요청
- Amazon WorkSpaces Secure Browser의 한도 예
- Amazon WorkSpaces Secure Browser의 기타 서비스 할당량

Amazon WorkSpaces Secure Browser에서 서비스 할당량 증가 요청

서비스 할당량 증가를 요청하려면 다음 단계를 따릅니다.

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

> **Important**
>
> WorkSpaces Secure Browser 서비스 할당량은 한 번에 하나의 리전에만 영향을 줍니다. 리소스가 더 필요한 경우 각 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.

Amazon WorkSpaces Secure Browser에서 포털 증가 요청

포털은 서비스의 기본 리소스입니다. 각 포털은 SAML 2.0 ID 제공업체와 인터넷 및 비공개 웹 콘텐츠에 대한 네트워킹 연결 간의 연결고리입니다. 각 포털에는 별도의 포털 브라우저 정책과 사용자 설정이 있을 수 있으므로 관리자는 일반적으로 동일한 리전에 여러 개의 포털을 생성하여 다양한 사용 사례를 처리합니다. 예를 들어 그룹 A에는 제한적인 정책(예: 클립보드 및 파일 전송 비활성화)이 적용된 특정 웹 사이트에 대한 액세스 권한을 제공하고, 그룹 B에는 URL 필터링 없이 일반 인터넷에 대한 액세스 권한을 제공할 수 있습니다. 지원되는 모든 AWS 리전에서 포털을 생성할 수 있습니다. 현재 서비스 가용성을 확인하려면 리전별 AWS 서비스를 참조하세요.

서비스 할당량 증가 요청

1. 원하는 리전에서 Service Quotas 페이지를 엽니다.
2. 웹 포털 수를 선택합니다.
3. 계정 수준에서 증가 요청을 선택합니다.
4. 할당량 값 증가에서 원하는 총 할당량을 입력합니다.

Amazon WorkSpaces Secure Browser에서 최대 동시 세션 증가 요청

최대 동시 세션 할당량은 포털에 동시에 연결할 수 있는 최대 사용자 수입니다. 최대 동시 세션에 대한 서비스 할당량 한도가 적절하게 설정되어 있지 않으면 사용자가 로그인할 때 세션을 사용할 수 없는 경

우가 발생할 수 있습니다. 이 서비스 할당량을 늘리는 것 외에도 고객은 VPC 및 서브넷에 최대 동시 세션을 지원할 수 있는 충분한 IP 공간이 있는지 확인해야 합니다.

최대 동시 세션 증가를 요청하려면

1. 원하는 리전에서 Service Quotas 페이지를 엽니다.
2. 늘리려는 인스턴스 유형에 해당하는 포털당 최대 동시 세션 수를 선택합니다.
3. 계정 수준에서 증가 요청을 선택합니다.
4. 할당량 값 증가에서 원하는 총 할당량을 입력합니다.

> **Note**
>
> 대규모 또는 긴급 증가의 경우 서비스 할당량 기록 페이지로 이동하여 요청의 상태 열에 있는 링크를 선택하고 지원 사례로 연결한 다음 사용 사례 및/또는 긴급성에 대한 세부 정보가 포함된 회신을 추가합니다. 이 정보는 서비스 팀이 요청의 우선순위를 정하고 계정에 충분한 용량을 할당하는 데 도움이 됩니다.

Amazon WorkSpaces Secure Browser의 한도 예

예를 들어 관리자가 미국 동부(버지니아 북부)에서 총 125명의 사용자를 위해 두 개의 웹 포털을 구성하고 있다고 가정해 보겠습니다. 웹 포털을 생성하기 전에 관리자는 100명의 사용자를 지원하게 될 첫 번째 웹 포털(포털 A)을 식별합니다. 이러한 사용자의 워크플로를 테스트할 때 관리자는 세션 중에 오디오 및 비디오 스트리밍을 지원하기 위해 XL 인스턴스 유형이 필요하다고 판단합니다. 두 번째 웹 포털(포털 B)은 최대 25명의 사용자가 고객 VPC에서 호스팅되는 단일 정적 웹 페이지에 액세스할 수 있도록 지원해야 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 인스턴스 한도를 리전 기본값(즉, 5개)에서 100으로 늘려야 합니다. 완료되면 관리자는 웹 포털을 편집하여 용량을 할당할 수 있습니다. 포털 B의 경우 관리자는 할당량 증가를 요청하지 않고 진행할 수 있습니다. 즉, 해당 리전에서 표준 인스턴스 유형에 대한 기본 할당량이 25이기 때문입니다.

Amazon WorkSpaces Secure Browser의 기타 서비스 할당량

Service Quotas 페이지에 나열된 기타 할당량을 확인하고 증가를 요청할 수 있습니다. 실제로 대부분의 고객은 이러한 한도 증가를 요청할 필요가 없습니다. 이러한 할당량은 크게 수와 비율이라는 두 가지 유형으로 구분됩니다.

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

드물게 고객이 다른 리소스 할당량의 수나 비율을 늘리는 사용 사례를 찾을 수 있습니다. 예를 들어 관리자는 추가 포털 구성을 테스트하기 위해 브라우저 설정 수를 늘릴 수 있습니다. 이러한 서비스 할당량 요청은 사례별로 검토되고 이행됩니다.

비율 할당량의 경우, 계정 포털 한도에 관계없이 Service Quotas에 표시되는 비율 한도를 조정할 필요가 없습니다.

Amazon WorkSpaces Secure Browser에서 SAML IdP 토큰 재인증 간격 제어

WorkSpaces Secure Browser 포털을 방문한 사용자는 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 WorkSpaces Secure Browser에 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 기간 설정을 AWS IAM Identity Center참조하세요.
2. WorkSpaces Secure Browser 포털의 비활성 및 유휴 제한 시간 값을 설정합니다. 이 값은 사용자의 마지막 상호 작용 시점과 비활성으로 인해 WorkSpaces Secure Browser 세션이 종료되는 시점 사이의 시간을 제어합니다. 세션이 종료되면 사용자는 세션 상태(열린 탭, 저장되지 않은 웹 콘텐

츠, 기록 등)를 잃고 다음 세션이 시작될 때 새로운 상태로 돌아갑니다. 자세한 내용은 the section called “웹 포털 생성”의 5단계를 참조하십시오.

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

Amazon WorkSpaces Secure Browser에서 사용자 활동 로깅 설정

WorkSpaces Secure Browser는 사용자 활동 및 보안 관련 이벤트를 로깅하는 두 가지 옵션을 제공합니다.

- 세션 로거는 다양한 세션 이벤트를 캡처합니다. 이러한 로그는 계정의 Amazon S3 버킷으로 전송되므로 선호하는 SIEM 플랫폼과 쉽게 통합할 수 있습니다.
- 사용자 액세스 로깅은 가장 중요한 세션 이벤트를 캡처합니다. 이러한 로그는 실시간 처리 및 분석을 위해 Amazon Kinesis 스트림으로 스트리밍됩니다.

두 로깅 옵션은 모두 포털 수준에서 구성됩니다. 로깅을 활성화하려는 모든 포털에 대해 각 옵션을 개별적으로 설정해야 합니다. 각 포털의 요구 사항에 따라 옵션 또는 둘 다를 활성화할 수 있습니다.

직원 활동의 로깅 또는 모니터링을 포함하여이 기능을 사용할 때 사용자 활동의 로깅 또는 모니터링에 적용되는 요구 사항을 준수할 책임은 사용자에게 있습니다.

주제

- Amazon WorkSpaces Secure Browser용 세션 로거 설정
- Amazon WorkSpaces Secure Browser에 대한 사용자 액세스 로깅 설정

Amazon WorkSpaces Secure Browser용 세션 로거 설정

> **Warning**
>
> 세션 로거를 활성화하면 다음 Chrome 기능이 비활성화됩니다.
>
> - Incognito 모드

- 개발자 도구
- Chrome 프로파일 전환

WorkSpaces Secure Browser 포털에 대한 세션 로거를 활성화하려면 먼저 세션 이벤트가 수집될 Amazon S3 버킷을 식별해야 합니다. 유사한 로그를 이미 저장한 기존 버킷을 사용하거나이 목적을 위해 특별히 새 버킷을 생성할 수 있습니다.

Amazon S3 버킷에는 로그를 쓸 수 있는 권한을 WorkSpaces Secure Browser에 부여하는 버킷 정책이 있어야 합니다. Amazon S3 버킷을 WorkSpaces Secure Browser 포털과 동일한 AWS 계정 및 리전에 배치하는 것이 좋습니다.

Amazon S3 버킷에는 이름 지정 요구 사항이 없습니다. 새 버킷을 생성하려면 아래 단계를 따르거나 Amazon Simple Storage Service 사용 설명서의 범용 버킷 생성을 참조하세요. 권한 구성에 대한 지침은 Amazon Simple Storage Service 사용 설명서의 Amazon S3에 대한 버킷 정책을 참조하세요.

다음은 Amazon S3 버킷에 대한 정책의 예입니다. 정책을 Amazon S3 버킷 이름으로 업데이트해야 합니다. 보안 주체는 "workspaces-web.amazonaws.com"입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowSessionLogger",
          "Effect": "Allow",
          "Principal": {
              "Service": "workspaces-web.amazonaws.com"
          },
          "Action": [
              "s3:PutObject"
          ],
          "Resource": [
              "arn:aws:s3:::bucket-name/*"
          ]
      }
  ]
}
```

WorkSpaces Secure Browser 포털에서 세션 로거를 활성화하면 Amazon S3에서 요금이 발생할 수 있습니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

세션 로거가 캡처하는 세션 관련 이벤트에 대한 자세한 내용은 섹션을 참조하세요the section called "세션 로거의 세션 이벤트".

KMS 암호화를 사용하는 S3 버킷(선택 사항)

WorkSpaces Secure Browser 세션 로거는 AWS KMS 암호화가 활성화된 Amazon S3 버킷을 완전히 지원합니다. 암호화된 Amazon S3 버킷으로 적절한 로깅 기능을 보장하려면 Session Logger에 AWS KMS 키를 사용하는 데 필요한 권한을 부여해야 합니다.

AWS KMS 키 구성에 다음 정책을 추가합니다.

```
{
  "Sid": "Session Logger",
  "Effect": "Allow",
  "Principal": {
    "Service": "workspaces-web.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
```

AWS 콘솔에서 이벤트를 수집할 WorkSpaces Secure Browser 포털을 선택하고 세션 로거 탭과 편집을 선택합니다.

다음 정보를 입력하여 포털에 대한 Session Logger를 구성합니다.

- S3 위치(필수): 이벤트가 전달될 Amazon S3 버킷의 이름입니다.
- 키 접두사(선택 사항): 이벤트가 전달되는 폴더입니다. 폴더가 없으면 폴더가 생성됩니다. 필드를 비워 두면 Session Logger는 Amazon S3 버킷의 루트에 이벤트를 작성합니다.

고급에서 다음 필드를 구성할 수 있습니다.

- 이벤트 필터: 세션 로거에서 모니터링하는 이벤트 목록입니다.

  - 모두:이 옵션을 선택하면 모든 현재 및 미래 이벤트가 모니터링됩니다.
  - 포함: 이를 통해 모니터링할 특정 이벤트를 수동으로 선택할 수 있습니다. 명시적으로 선택한 이벤트만 로깅됩니다. 향후 업데이트에 도입된 새 이벤트는 선택 항목에 수동으로 추가되지 않는 한 모니터링되지 않습니다.
- 파일 형식
  - JSON(기본값): 각 로그 파일이 이벤트 배열로 표시되는 파일 형식입니다. 대부분의 사용 사례에이 형식을 사용하는 것이 좋습니다.
  - JSONLines: Amazon Athena에 최적화된 파일 형식입니다.
- 폴더 구조: 로그 파일이 저장되는 방식을 결정합니다.
  - 플랫(기본값): 모든 로그 파일은 단일 폴더에 있습니다.
  - 중첩 기준 날짜: 로그 파일은 날짜 및 시간별로 폴더로 구성됩니다. Amazon Athena용으로 분할되고 Amazon Athena 쿼리에 최적화되었습니다.

세션 로거 설정을 테스트하고 세션 로거가 올바르게 작동하는지 확인할 수 있습니다. 구성이 완료되면 시스템은 지정된 Amazon S3 버킷 및 폴더에 `_workspaces_secure_browser.tmp` 라는 테스트 파일을 쓰려고 시도합니다. 이는 로깅 기능과 권한 설정 모두에 대한 검증 역할을 합니다.

포털에서 Secure Browser 세션을 시작하고 평소와 같이 브라우저를 사용하여 테스트 세션을 실행할 수도 있습니다. 세션 로거는 활성 세션 중에 15분마다 또는 세션이 종료될 때 구성된 Amazon S3 버킷에 로그 파일을 씁니다.

세션을 종료하거나 다음 로깅 간격을 기다린 후 Amazon S3 버킷을 확인하여 세션에 대한 로그 파일이 예상대로 생성되고 저장되었는지 확인합니다.

Amazon WorkSpaces Secure Browser에 대한 사용자 액세스 로깅 설정

WorkSpaces Secure Browser 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.

WorkSpaces Secure Browser에서 로그를 수신하려면 'amazon-workspaces-web-*'로 시작하는 Amazon Kinesis Data Stream이 있어야 합니다. Amazon Kinesis 데이터 스트림에는 서버 측 암호화가 꺼져 있거나 서버 측 암호화 AWS 관리형 키 에를 사용해야 합니다.

Amazon Kinesis에서 서버 측 암호화를 설정하는 방법에 대한 자세한 내용은 서버 측 암호화를 시작하는 방법 섹션을 참조하십시오.

Amazon WorkSpaces Secure Browser에서 브라우저 정책 관리

안정적인 최신 버전에 사용할 수 있는 Chrome 정책을 사용하여 사용자 지정 브라우저 정책을 WorkSpaces Secure Browser로 설정할 수 있습니다. WorkSpaces Secure Browser 포털에서 정책을 설정하면 해당 웹 포털에서 관리하는 모든 세션에 정책이 적용됩니다.

웹 포털에 적용할 수 있는 정책은 300개가 넘습니다. Chrome 정책의 전체 목록을 포함한 자세한 내용은 Chrome Enterprise 정책 목록을 참조하세요.

Chrome 정책을 설정하는 세 가지 방법이 있습니다.

1. 웹 포털에서 시각적 편집기 사용

   콘솔 보기를 사용하여 웹 포털을 생성하면 시각적 편집기에서 가장 일반적인 정책 중 일부를 적용할 수 있습니다.

   - `StartURL`
   - 프라이빗 브라우징 설정 및 해제
   - 기록 삭제
   - 북마크 및 북마크 폴더
2. 웹 포털에서 JSON 편집기 사용

   시각적 편집기 대신 JSON 편집기를 사용하여 정책을 직접 추가하거나 편집할 수도 있습니다.

   정책의 특정 형식은 Chrome Enterprise 정책 목록을 참조하세요.
3. 웹 포털에 JSON 파일 업로드

   JSON 파일을 웹 포털에 업로드하여 조직에서 사용되는 Chrome 정책을 가져올 수도 있습니다.

   자세한 내용은 섹션을 참조하세요. the section called “자습서: 사용자 지정 브라우저 정책 설정”

WorkSpaces Secure Browser는 지정된 정책 및 모든 포털에 기본 브라우저 정책 구성을 적용합니다. 사용자 지정 JSON 파일을 사용하여 이러한 정책 중 일부를 편집할 수 있습니다. 자세한 내용은 the section called “기본 브라우저 정책 편집” 단원을 참조하십시오.

주제

- 자습서: Amazon WorkSpaces Secure Browser에서 사용자 지정 브라우저 정책 설정
- Amazon WorkSpaces Secure Browser에서 기본 브라우저 정책 편집

자습서: Amazon WorkSpaces Secure Browser에서 사용자 지정 브라우저 정책 설정

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 자습서에서는 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 Secure Browser 포털을 생성해야 합니다. 자세한 내용은 the section called “웹 포털 생성” 단원을 참조하십시오.

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 방지합니다.
   - ExtensionInstallAllowlist – 특정 확장 프로그램을 설치하도록 허용합니다.
5. 추가 정책은 나머지 요구 사항을 충족합니다.
   - ManagedBookmarks – 웹페이지에 북마크를 추가합니다.
   - RestoreOnStartupURLs - 새 브라우저 창이 시작될 때마다 열리는 웹 페이지를 구성합니다.
   - AllowDeletingBrowserHistory - 사용자가 검색 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. `RestoreOnStartup`을 `4`로 설정합니다. 이렇게 하면 URL 목록을 여는 `RestoreOnStartup` 작업이 설정됩니다. 시작 URL에서 다른 작업을 사용할 수도 있습니다. 자세한 내용은 Chrome 엔터프라이즈 정책 목록을 참조하십시오.
   b. `RestoreOnStartupURLs`를 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 ExtensionInstallAllowlist에서 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. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser을 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.

Amazon WorkSpaces Secure Browser에서 기본 브라우저 정책 편집

서비스를 제공하기 위해 WorkSpaces Secure Browser는 기본 브라우저 정책을 모든 포털에 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.

기준 URLAllowlist 및 URLBlocklist 정책은 덮어쓸 수 없습니다. 웹 포털과 연결된 JSON 브라우저 정책 파일에는 이러한 기준 정책이 포함되지 않습니다. 적용된 모든 정책 및 해당 값의 전체 목록을 보려면 원격 브라우징 세션 내에서 "chrome://policy"로 이동합니다.

고객은 웹 포털에서 다음 정책을 업데이트할 수 있습니다.

- DownloadRestrictions – 기본값은 Chrome Safe Browsing에서 악성으로 식별된 다운로드를 방지하도록 1로 설정되어 있습니다. 자세한 내용은 사용자가 유해한 파일을 다운로드하지 못하도록 방지 섹션을 참조하십시오. 이 값을 0 또는 4로 설정할 수 있습니다.

Amazon WorkSpaces Secure Browser용 입력 방법 편집기 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 Secure Browser 세션에는 기본적으로 IME 지원이 포함됩니다. 사용자는 세션의 IME 도구 모음에서 또는 키보드 단축키를 사용하여 대체 언어를 선택할 수 있습니다.

WorkSpaces Secure Browser의 IME에서 현재 지원되지 않는 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 언어

- IME를 앞쪽으로 돌리거나 오른쪽 키보드 레이아웃으로 이동하려면 Shift+Control+Left Alt 키를 누릅니다.
- 언어 및 입력 설정에 액세스하려면 상단 패널 표시줄의 언어 선택기를 사용합니다. 표시되지 않으면 도구 모음 → 기본 설정 → 일반 → 키보드 입력 방법을 통해 활성화합니다.

- 일본어
  - macOS 사용자의 경우: 미국 입력 소스를 사용하는 경우 입력 문제가 발생할 수 있습니다. 이 문제를 해결하려면:
    1. macOS에서 미국 입력 소스 대신 일본어 입력 소스(예: Japanese - Kana 또는 Japanese - Romaji)를 선택합니다.
    2. WorkSpaces Secure Browser 세션에서 도구 모음 → 기본 설정 → 키보드 → 옵션 키 설정으로 이동하고 옵션 사용("")을 원격 Alt 키(Mac)로 선택하여 키보드 바로 가기가 제대로 작동하는지 확인합니다.
  - 입력 문자 변환
    - 문자를 Hiragana로 변환하려면를 누릅니다F6.
    - 문자를 가타카나로 변환하려면를 누릅니다F7.
    - 문자를 Hankaku Katakana(하프 너비 Katakana)로 변환하려면 F8
    - 문자를 라틴어로 변환하려면를 누릅니다F10.
    - 문자를 라틴어로 변환하려면를 누릅니다F9.
  - 입력 모드 전환
    - Hiragana에서 Katakana로 전환하려면를 누릅니다Alt/Option+K.
    - Katakana에서 Hankaku Katakana로 전환하려면를 누릅니다Alt/Option+K.
    - Hankaku Katakana(하프 너비 Katakana)에서 다시 Hiragana로 전환하려면를 누릅니다Alt/Option+K.
    - 일본어 모드 또는 라틴어에서 라틴어로 전환하려면를 누릅니다Alt/Option+L.
    - 라틴어에서 라틴어로 전환하려면를 누릅니다Alt/Option+L.
    - 어떤 모드에서든 직접 입력으로 전환하려면를 누릅니다Henkaku/Zenkaku key.
    - 직접 입력에서 다시 Hiragana로 전환하려면를 누릅니다Henkaku/Zenkaku key.
- 한국어
  - 한국어를 선택하려면 Shift+Space 키를 누릅니다.
  - 한자를 선택하려면 F9 키를 누릅니다.

WorkSpaces Secure Browser 세션에서 화면 키보드를 끄려면에 문의하세요 지원.

Amazon WorkSpaces Secure Browser에 대한 세션 내 현지화 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.

세션 언어는 다음과 같은 우선 순위에 따라 결정됩니다.

1. 웹 포털 브라우저 설정의 ForcedLanguages 정책. 자세한 내용은 ForcedLanguages를 참조하십시오.
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 Secure Browser의 다음 구성 요소는 현지화를 지원합니다.

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

주제

- Amazon WorkSpaces Secure Browser에 지원되는 언어 코드
- 사용자 브라우저 설정에서 언어 선택

Amazon WorkSpaces Secure Browser에 지원되는 언어 코드

다음 목록은 WorkSpaces Secure Browser에서 현재 지원되지 않는 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)

사용자 브라우저 설정에서 언어 선택

사용자의 로컬 브라우저 설정을 설정하려면 적절한 단계를 따릅니다.

- 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.

Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 관리

> **Important**
>
> IP 액세스 제어는 IPv4만 지원합니다. IPv6-only 네트워크에서 연결하는 사용자는 차단됩니다.

WorkSpaces Secure Browser를 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 Browser를 사용하면 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 Browser에서 세션을 탐지하고 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 WorkSpaces Secure Browser 사용과 관련하여 발생할 수 있는 잠재적 법적 문제를 이해할 책임이 있고 WorkSpaces Secure Browser 사용이 모든 관련 법률 및 규정을 준수하도록 보장해야 합니다. 여기에는 애플리케이션 내에서 수행되는 활동을 포함하여 직원의 WorkSpaces Secure Browser 사용을 모니터링하는 고용주의 권한을 규제하는 법률이 포함됩니다.

주제

- Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 그룹 생성

- Amazon WorkSpaces Secure Browser에서 웹 포털과 IP 액세스 설정 연결
- Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 그룹 편집
- Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 그룹 삭제

Amazon WorkSpaces Secure Browser에서 IP 액세스 제어 그룹 생성

> **Important**
>
> IP 액세스 제어는 IPv4만 지원합니다. IPv6-only 네트워크에서 연결하는 사용자는 차단됩니다.

IP 액세스 제어 그룹을 생성하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
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.

Amazon WorkSpaces Secure Browser에서 웹 포털과 IP 액세스 설정 연결

> **Important**
>
> IP 액세스 제어는 IPv4만 지원합니다. IPv6-only 네트워크에서 연결하는 사용자는 차단됩니다.

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

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
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”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.

Amazon WorkSpaces Secure Browser에서 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. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
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.

Amazon WorkSpaces Secure Browser에서 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. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. 탐색 창에서 IP 액세스 제어 그룹을 선택합니다.
3. 그룹을 선택하고 삭제를 선택합니다.

Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램 관리

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.

기본적으로 Chrome의 시크릿 모드나 Firefox 사생활 보호 모드에서는 확장 프로그램을 사용할 수 없습니다. 사용자가 수동으로 활성화할 수 있습니다. Chrome에 대한 자세한 내용은 시크릿 모드의 확장 프로그램을 참조하세요. Firefox에 대한 자세한 내용은 사생활 보호 모드에서의 확장 기능을 참조하십시오.

사용자는 포털에 로그인할 때 확장 프로그램을 설치하라는 메시지를 받게 됩니다. 확장 프로그램의 사용자 경험에 대한 자세한 내용은 the section called “Single Sign-On 확장 프로그램” 섹션을 참조하십시오.

주제

- Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램에 대한 도메인 식별

- Amazon WorkSpaces Secure Browser에서 새 웹 포털에 Single Sign-On 확장 프로그램 추가
- Amazon WorkSpaces Secure Browser에서 기존 웹 포털에 Single Sign-On 확장 프로그램 추가
- Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램 편집 또는 제거

Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램에 대한 도메인 식별

먼저 SAML IdP 및 웹 사이트에 필요한 도메인을 결정합니다. 최대 10개의 도메인을 추가할 수 있습니다.

쿠키를 동기화할 적절한 도메인을 테스트하고 식별할 책임은 사용자에게 있습니다. SSO(Single Sign-On)가 예상대로 작동하려면 IdP 또는 웹 사이트 인증 수준에서 변경이 필요할 수 있습니다.

가장 일반적인 IdP에 사용할 도메인을 확인하려면 다음 표를 참조하세요.

IdP 및 도메인

IdP	도메인
Okta	okta.com
Entra ID	microsoftonline.com
AWS Identity Center	awsapps.com
One Login	onelogin.com
Duo	duosecurity.com

Amazon WorkSpaces Secure Browser에서 새 웹 포털에 Single Sign-On 확장 프로그램 추가

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

1. the section called “사용자 설정”에 도달할 때까지 the section called “웹 포털 생성”의 단계를 따릅니다.
2. the section called “사용자 설정”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”의 단계와 the section called “웹 포털 생성”의 나머지 섹션을 완료하여 웹 포털을 생성합니다.

Amazon WorkSpaces Secure Browser에서 기존 웹 포털에 Single Sign-On 확장 프로그램 추가

기존 웹 포털에 확장 프로그램을 추가하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home)을 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.

Amazon WorkSpaces Secure Browser에서 Single Sign-On 확장 프로그램 편집 또는 제거

도메인을 편집하거나 확장 프로그램을 제거하려면 다음 단계를 따릅니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home)을 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 세션에서 더 이상 쿠키를 동기화하지 않습니다.

Amazon WorkSpaces Secure Browser의 웹 콘텐츠 필터링

웹 콘텐츠 필터링은 조직이 WorkSpaces Secure Browser 내에서 정책을 정의하고 콘텐츠 액세스를 규제할 수 있는 보안 및 규정 준수 기능입니다. 웹 콘텐츠 필터링을 사용하면 최종 사용자가 특정 URLs

또는 도메인 범주에 액세스하거나 차단하여 액세스를 제한할 수 있는 URLs 지정하여 중요한 보안 및 규정 준수 요구 사항을 해결할 수 있습니다.

> **Note**
>
> Chrome 정책을 통해 URL 필터링 정책을 설정하여 특정 도메인을 차단하거나 허용할 수 있지만 Chrome 정책의 작업은 서비스 로깅 기능의 일부로 캡처되지 않으므로이 접근 방식을 사용하지 않는 것이 좋습니다. 포괄적인 모니터링 및 규정 준수 보고를 위해이 페이지에 설명된 웹 콘텐츠 필터링 정책을 사용합니다.

주제

- 특정 URLs로 브라우징 제한
- 특정 URLs 차단
- 차단 범주
- URLs의 예
- Chrome 정책 전송

특정 URLs로 브라우징 제한

명시적으로 승인된 웹 사이트 및 URLs 수 있습니다. 인터넷 액세스를 엄격하게 제어해야 하고 허용된 모든 사이트가 비즈니스 요구 사항 및 보안 규정 준수를 위해 심사를 받은 고보안 환경에 적합합니다.

AWS 콘솔의 URL 필터링에서 다음을 수행합니다.

- 차단 목록으로 이동하여 모든 URLs
- 허용 목록에서 URL 추가를 클릭하여 최종 사용자에게 허용할 URL을 추가합니다. URL당 하나의 항목을 추가합니다.
- 저장을 클릭합니다.

특정 URLs 차단

알려진 문제가 있는 사이트를 차단하면서 개방형 인터넷 액세스를 유지하여 보안과 생산성의 균형을 맞출 수 있습니다. 사용자를 신뢰하지만 합법적인 비즈니스 활동을 지나치게 제한하지 않고 특정 위협 또는 부적절한 콘텐츠에 대한 액세스를 방지하려는 조직에 적합합니다.

AWS 콘솔의 URL 필터링에서 다음을 수행합니다.

- 차단된 URLs로 이동
- URL 추가를 선택하고 차단할 URL을 입력합니다. 차단하려는 URL당 하나의 항목 추가
- 저장을 클릭합니다.

차단 범주

특정 URLs 차단하는 것 외에도 콘텐츠 범주를 기반으로 URLs 그룹을 자동으로 차단할 수도 있습니다. 이는 개별 사이트를 수동으로 식별하고 차단할 필요 없이 다양한 유형의 부적절하거나 위험한 콘텐츠에 대한 포괄적인 적용 범위가 필요한 조직에 유용합니다.

AWS 콘솔의 URL 필터링에서 다음을 수행합니다.

- 차단된 범주로 이동하여 범주 추가를 클릭합니다.
- 차단하려는 범주 선택
- 허용 목록에 URLs를 적용할 수 있습니다. 이렇게 하려면 URL 추가를 클릭하고 허용하려는 URLs의 항목을 입력합니다. 범주에 포함되더라도 최종 사용자는 URLs을 방문할 수 있습니다.
- 저장을 클릭합니다.

다음 범주를 선택할 수 있습니다. 하나, 여러 개 또는 모든 범주를 선택할 수 있습니다.

사용 가능한 필터링 범주

테마	범주	설명
성인 및 부적절한 콘텐츠	나체	성적이지 않은 누드 이미지 또는 아트워크가 포함된 사이트.
성인 및 부적절한 콘텐츠	포르노	명시적인 성적 콘텐츠 또는 도발적인 누드 자료가 있는 사이트.
성인 및 부적절한 콘텐츠	성교육	연령에 적합하고 의학적 검토를 거친 건강 및 성욕 리소스.
성인 및 부적절한 콘텐츠	테이스트리스	다른 범주에서 다루지 않는 어린이에게 부적절한 콘텐츠.
커뮤니케이션 및 소셜	Chat	실시간 그룹 및 프라이빗 메시징 플랫폼.

테마	범주	설명
커뮤니케이션 및 소셜	인스턴트 메시징	프라이빗 메시징 서비스.
커뮤니케이션 및 소셜	전문 네트워크	비즈니스 중심 관계 구축 플랫폼.
커뮤니케이션 및 소셜	소셜 네트워킹	개인 콘텐츠 및 경험을 공유하기 위한 사용자 상호 작용 플랫폼입니다.
커뮤니케이션 및 소셜	웹 기반 이메일	e-카드 및 인사말 시스템을 포함하여 브라우저에서 액세스할 수 있는 메시징 서비스입니다.
엔터테인먼트	게임	비디오 게임, 퍼즐, 도박 외 활동을 포함한 레크리에이션 게임 리소스.
엔터테인먼트	이미지 공유	호스팅, 검색 및 공유 기능을 제공하는 시각적 콘텐츠 플랫폼입니다.
엔터테인먼트	피어 투 피어	파일 공유 애플리케이션 공급자 및 관련 소프트웨어 도구.
유해 및 불법 콘텐츠	범죄 활동	불법 행위를 홍보하는 지침 또는 자료.
유해 및 불법 콘텐츠	해킹	무단 시스템 액세스 도구 및 네트워크 악용 리소스.
유해 및 불법 콘텐츠	불법 약물	기분 전환용 약물 사용 또는 약물 남용을 홍보하는 콘텐츠.
유해 및 불법 콘텐츠	잘못된 소프트웨어	무단 저작권이 있는 자료 및 악성 소프트웨어 배포.
유해 및 불법 콘텐츠	폭력	물리적 피해를 촉진하거나 그래픽 재료를 표시하는 콘텐츠입니다.
유해 및 불법 콘텐츠	무기	합법적인 스포츠 및 레크리에이션 총기 사용 리소스.

테마	범주	설명
고위험 행동	컬트	메인스트림이 아닌 영적 및 메타물리적 콘텐츠.
고위험 행동	도박	베팅 관련 활동 및 정보.
고위험 행동	증오 및 무관용	콘텐츠는 보호 대상 특성에 대한 편향을 촉진합니다.
고위험 행동	학교 부정 행위	무단 학업 지원 및 숙제 완료 서비스.
고위험 행동	자해	자기 파괴적 행동을 홍보하거나 논의하는 콘텐츠입니다.
기술 및 AI	사이트 다운로드	소프트웨어, 애플리케이션 및 디지털 자산 호스팅 플랫폼.
기술 및 AI	생성형 AI	AI 및 기계 학습 기술 리소스.
기술 및 AI	주차된 도메인	광고 또는 도메인 판매에 사용되는 최소 콘텐츠 도메인.
기술 및 AI	스트리밍 미디어 및 다운로드	음악, 비디오 및 인터넷 라디오를 포함한 오디오/비디오 콘텐츠 플랫폼.

URLs의 예

AllowedUrls 또는 BlockedUrls에서 다음과 같은 유형의 URLs을 제공할 수 있습니다. BlockedUrls

Type	예제
도메인	example.com
하위 도메인	login.example.com
경로	example.com/myvideos
쿼리 파라미터	example.com/?parameter=123

Chrome 정책 전송

특정 도메인을 허용하거나 차단하도록 설정된 Chrome 정책이 이미 있는 경우 웹 콘텐츠 필터링 기능으로 이전하는 것이 좋습니다.

웹 콘텐츠 필터링 기능은 WorkSpaces Secure Browser 세션에 적용되는 URLAllow 또는 URLBlock 정책을 감지하고 AWS 콘솔에서 이를 알립니다.

URLAllowlist 및/또는 URLBlocklist에 대한 Chrome 정책을 전송하려면

- AWS 콘솔의 URL 필터링에서 Chrome 정책 검토를 클릭합니다(Chrome 정책 검토 버튼이 표시되지 않으면 현재 URL 허용 또는 URL URLBlock에 Chrome 정책이 적용되지 않음).
- 오버레이에서 Chrome 정책을 검토합니다.
- 전송을 클릭합니다.

Chrome 정책은 정책 설정에서 JSON 편집기에서 제거되고 새 URLs은 웹 콘텐츠 필터링 기능에 자동으로 추가됩니다.

Amazon WorkSpaces Secure Browser의 딥 링크

사용자가 WorkSpaces Secure Browser에 로그인하면 관리자가 설정한 홈 페이지에서 세션이 시작됩니다. 세션 중에 사용자를 특정 웹사이트로 연결하는 딥링크를 포털에서 수신하도록 허용할 수도 있습니다. 딥링크를 선택하면 딥링크에 지정된 URL이 포털에 표시됩니다. 링크는 세션 시작을 위해 구성된 홈 페이지와 함께 표시되거나 세션이 이미 진행 중인 경우 단독으로 표시됩니다. 이 기능을 통해 관리자는 WorkSpaces Secure Browser로 더욱 동적인 사용자 환경을 생성할 수 있습니다.

딥 링크를 클릭하면 WorkSpaces Secure Browser 세션에서 페이지가 열립니다. 세션이 이미 실행 중인 경우 딥 링크가 새 탭에서 열립니다. 세션이 아직 실행 중이지 않은 경우 새 탭에서 딥링크 URL이 열리고 별도의 탭에서 포털 기본 홈 페이지가 열립니다. 딥 링크에 둘 이상의 URL이 포함된 경우 먼저 나열된 딥 링크 URL이 포커스 상태로 표시되고 그 이후의 각 URL(기본 홈페이지 포함)은 별도의 탭에서 열립니다.

주제

- Amazon WorkSpaces Secure Browser에서 딥 링크 설정
- Amazon WorkSpaces Secure Browser에서 딥 링크에 URL 필터링 사용

Amazon WorkSpaces Secure Browser에서 딥 링크 설정

딥 링크에 대한 권한을 허용하려면 사용자 설정을 생성할 때 허용을 선택합니다. 딥링크로 연결하려는 사이트는 URL 인코딩 사이트여야 합니다. 예를 들어 사용자를 “https://www.example.com/?query=true”에 연결하려면 링크를 https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue로 업데이트합니다.

딥링크에는 최대 10개의 URL을 쉼표로 구분하여 포함할 수 있습니다. 예제:

https://<uuid>.workspaces-web.com/?deepLinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue,https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue2,https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue3,https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue4.

딥링크 허용에 대한 자세한 내용은 the section called “사용자 설정” 단원을 참조하세요.

Amazon WorkSpaces Secure Browser에서 딥 링크에 URL 필터링 사용

이 포털 링크를 공유하는 사용자는 해당 도메인이 포털에서 접근 가능하고 URL 차단 목록에 없으면 딥 링크 값을 조작하여 웹 사이트를 방문할 수 있습니다. 사용자가 포털에서 의도하지 않은 도메인을 방문하지 못하도록 제한적인 허용 목록 또는 차단 목록을 생성하려면 URL 필터링을 사용합니다.

포털의 허용 목록 및 차단 목록은 포털의 브라우저 설정에서 URL 필터링을 사용하여 편집할 수 있습니다. 이렇게 하려면 허용 목록에 있는 포털 URL에 URL을 다음 형식으로 추가합니다. 여기서 UUID는 포털 ID입니다. https://<uuid>.workspaces-web.com/?deepLinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue

자세한 내용은 the section called “웹 콘텐츠 필터링” 및 웹사이트 액세스 허용 또는 차단하기를 참조하세요.

Amazon WorkSpaces Secure Browser에서 세션 관리 대시보드 사용

WorkSpaces Secure Browser 콘솔의 세션 관리 대시보드를 사용하여 활성 세션과 완료된 세션을 모니터링하고 관리할 수 있습니다.

대시보드 액세스

대시보드에 액세스하려면 다음 단계를 따릅니다.

대시보드에 액세스하려면

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 선택하고 웹 포털을 선택합니다.
3. 세션 탭을 선택하거나 세션 보기를 선택하여 아래의 분할 패널에서 대시보드를 엽니다.

대시보드 필터

세션 패널에서 다음 속성 또는 값을 기준으로 세션을 필터링할 수 있습니다.

- 상태
  - 활성 - 세션이 현재 실행 중임을 나타냅니다. 세션을 종료하려면 아래를 참조하세요.
  - 종료됨 - 세션이 더 이상 활성 상태가 아님을 나타냅니다.
- 세션 ID
- 사용자 이름
- 세션 시작 작업

세션 종료

세션을 종료하려면 다음 단계를 따릅니다.

세션을 종료하려면

1. 세션 대시보드에서 중지할 세션을 선택합니다.
2. 종료를 선택합니다.
3. 연결이 끊긴 사용자는 세션의 모든 상태를 잃습니다. 열려 있는 모든 탭, 브라우저 기록 및 보안 브라우저에 다운로드된 파일은 재활용됩니다.

세션 기록

대시보드에는 지난 35일 동안의 세션이 포함되어 있습니다. CLI를 사용하여 필터를 사용하거나 사용하지 않고 세션을 나열할 수 있습니다. 세션 기록은 JSON으로 제공되며, 관리자는 이를 처리, 관리하고 별도의 저장소에 저장할 수 있습니다.

다음은 미국 서부 2(오리건) 리전의 세션을 관리하기 위한 샘플 CLI 명령입니다.

웹 포털의 모든 세션을 나열하려면 다음 명령을 실행합니다.

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>

웹 포털의 특정 사용자에 대한 세션을 모두 나열하려면 다음 명령을 실행합니다.

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>

FIPS 엔드포인트 및 Amazon WorkSpaces Secure Browser를 사용하여 전송 중 데이터 보호

기본적으로 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDK를 사용하여 관리자로 WorkSpaces Secure Browser 서비스와 통신하거나 사용자 세션 중에 전송 중인 모든 데이터는 TLS 1.2를 사용하여 암호화됩니다.

명령줄 인터페이스 또는 API를 통해 AWS 에 액세스할 때 FIPS 140-3 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. FIPS 엔드포인트를 사용하면 모든 전송 중 데이터가 FIPS(미 연방 정부 정보 처리 표준) 140-3을 준수하는 암호화 표준을 사용하여 암호화됩니다. WorkSpaces Secure Browser 엔드포인트 목록을 포함한 FIPS 엔드포인트에 대한 자세한 내용은 https://aws.amazon.com/compliance/fips 단원을 참조하세요.

FIPS 엔드포인트로 포털을 생성한 후에는 모든 사용자 세션 및 관리 변경이 FIPS 140-3 엔드포인트를 사용하여 자동으로 수행됩니다. `AWS_USE_FIPS_ENDPOINT=true` 환경 변수를 사용하여 FIPS 엔드포인트를 찾고 SDK를 사용하여 요청을 보낼 수 있습니다. 다음은 예입니다.

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

`–endpoint-url` 옵션을 사용하여 FIPS 엔드포인트로 직접 요청을 보낼 수도 있습니다. 다음은 미국 서부 2(오리건) 리전에서 포털 목록을 직접 호출하는 예시입니다.

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-west-2.amazonaws.com
```

Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 관리

데이터 보호 설정은 세션 중에 데이터가 공유되지 않도록 보호하는 데 사용됩니다. 설정을 생성하여 여러 포털에 적용할 수 있습니다.

주제

- Amazon WorkSpaces Secure Browser의 인라인 데이터 수정
- Amazon WorkSpaces Secure Browser의 기본 수정 구성
- Amazon WorkSpaces Secure Browser의 기본 인라인 수정
- Amazon WorkSpaces Secure Browser에서 사용자 지정 인라인 수정
- Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 생성
- Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 연결
- Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 편집
- Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 삭제

Amazon WorkSpaces Secure Browser의 인라인 데이터 수정

포털에 인라인 데이터 수정을 추가하면 웹 페이지에 표시된 텍스트 문자열에서 특정 데이터를 자동으로 예측하고 수정할 수 있습니다. 기본 제공 패턴(예: 주민등록번호 또는 신용 카드 번호) 중에서 선택하여 수정 정책을 생성하거나 정규 표현식 및 키워드를 사용하여 고유한 사용자 지정 데이터 유형을 생성할 수 있습니다. 정책에는 수정을 적용해야 하는 URLs에 대해 구성 가능한 수준의 적용 및 제어가 포함됩니다.

다음 구성 요소는 데이터가 수정되는 시기를 결정합니다.

- 데이터 보호 설정 - 데이터 보호 설정은 데이터 유형 및 적용 기준을 포함하는 리소스의 이름입니다. 이 리소스를 사용하려면 먼저 설정을 생성한 다음 포털에 연결합니다. 사용자가 세션을 시작하면 세션 중에 설정이 적용됩니다.
- 세션 내 브라우저 확장 - 편집 설정을 포털과 연결하면 설정을 적용하는 시스템 적용 브라우저 확장으로 세션 브라우저가 시작됩니다. 데이터 보호 설정은 신뢰도 수준 및 URL 적용 구성에 따라 패턴 일치(정규 표현식) 및 키워드 검색을 통해 수정을 적용합니다. 콘텐츠는 텍스트 문자열에서 예측되며 화면에 표시되기 전에 수정됩니다. 또한 확장은 수정을 우회하는 사용자의 기능(예: 비활성화된 프라이빗 브라우징, 개발자 도구에 대한 액세스, 네트워크 검사)을 제어하는 관련 브라우저 정책을 설정합니다.

세션 내 브라우저 확장에 따라 다음 Chrome 브라우저 정책 변경 사항이 적용됩니다. 자세한 내용은 Chrome 엔터프라이즈 정책 목록을 참조하십시오.

- 브라우저 정책을 적용하여 사용자가 수정 없이 세션을 볼 수 없도록 합니다.
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2

  - BrowserAddPersonEnabled = false
  - BrowserGuestModeEnabled = false
- 또한 확장은 다운로드 이벤트를 취소하여 사용자가 데이터 보호 설정을 적용하는 URLs에서 HTML 파일을 다운로드하지 못하도록 합니다.

일반적으로 구조화되지 않은 퍼블릭 브라우징(예: Facebook 또는 Google)이 아닌 구조화된 프라이빗 웹 사이트(예: 고객 관리 도구, 티켓팅 시스템 또는 Wiki)에서 수정을 사용해야 합니다. 기본 제공 데이터 유형(전체 목록은 아래 참조) 중에서 선택하거나 자체 정규식 값과 키워드를 사용하여 사용자 지정 데이터 유형을 정의할 수 있습니다. 관리자는 각 데이터 유형, 신뢰도 수준 및 URL 적용이 예상대로 작동하는지 테스트하고 검증할 책임이 있습니다.는 타사에서 제공하는 사용자 지정 웹 사이트 또는 애플리케이션과의 호환성을 보장할 AWS 수 없습니다.

WorkSpaces Secure Browser는 현재 다음 형식의 텍스트를 포함하여 텍스트가 아닌 형식의 지원되는 또는 사용자 지정 데이터 형식 수정을 지원하지 않습니다.

- JPEG, PNG 또는 GIF와 같은 이미지
- 사용자가 Google Docs 또는 Sheets와 같은 동적 단어 처리 또는 편집을 사용할 수 있는 웹 페이지
- YouTube 비디오와 같이 브라우저에서 액세스하는 오디오 또는 비디오 스트림
- Chrome 브라우저에서 보는 PDFs

지원되지 않는 형식의 콘텐츠에는 수정을 사용하지 마세요. 관리자는 사용자에게 수정하려는 콘텐츠에 대한 액세스 권한을 부여하기 전에 사이트 및 콘텐츠 호환성을 검증할 책임이 있습니다.

Amazon WorkSpaces Secure Browser의 기본 수정 구성

기본 수정 구성은 데이터 보호 설정의 모든 기본 제공 데이터 유형에 대해 신뢰 수준 및 URL 적용을 자동으로 적용합니다. 기본 제공 데이터 유형을 추가할 때 기본 구성을 재정의할 수 있습니다.

신뢰도 수준을 사용하면 형식, 키워드 및 형식이 지정되지 않은 텍스트의 조합을 사용하여 기본 제공 데이터 유형에 대한 수정 로직을 미세 조정할 수 있습니다. 높음, 중간 또는 낮음을 포함하여 수정이 적용되는 방법에 대한 엄격성 수준을 선택합니다. 기본값은 데이터 형식 수준에서 재정의가 적용되지 않는 한 모든 데이터 형식에 적용됩니다. 일반적으로 Medium의 기본 구성으로 시작하고 수정이 사이트에 예상대로 적용되었는지 확인하여 구체화합니다.

신뢰도 수준	설명	예제
높음	콘텐츠를 수정하려면 형식이 지정된 텍스트 패턴 일치가 필요합니다.	123-45-6798의 SSN은 수정되지만 123456789은 수정되지 않습니다.
중간	수정은 형식이 지정된 텍스트와 형식이 지정되지 않은 텍스트를 모두 고려하고 키워드 연결을 로직에 추가합니다.	SSN 123-45-6798가 수정됩니다. 키워드(예: "사회보장번호") 근처에서 탐지되면 123456789가 수정됩니다.
낮음	형식이 지정된 패턴과 키워드가 없는 형식이 지정되지 않은 패턴 모두에 적용되는 수정입니다.	및 123-45-6798 형식의 SSN123456789은 키워드 없이 수정됩니다.

모든 데이터 유형에 대해 기본 수정 구성을 설정해야 합니다. 다음 옵션 중에서 선택할 수 있습니다.

- 모든 URLs
- 특정 URLs
- 고급 구성

기본값은 데이터 형식 수준에서 재정의가 적용되지 않는 한 모든 데이터 형식에 적용됩니다. URL 적용은 허용 및 차단 목록을 관리하기 위해 Chrome 정책과 유사한 로직을 사용합니다. 차단 및 허용 URLs 사용에 대한 지침은 웹 사이트에 대한 액세스 허용 또는 차단을 참조하세요. 최상의 결과를 얻으려면 Chrome의 차단 목록 필터 형식에 따라 이러한 목록에 URLs을 추가합니다. 자세한 내용은 URL 차단 목록 필터 형식을 참조하세요.

Amazon WorkSpaces Secure Browser의 기본 인라인 수정

인라인 데이터 수정은 기본 인라인 수정 아래에 나열된 기본 제공 패턴(예: 주민등록번호 및 신용 카드 번호)을 지원합니다. 드롭다운 메뉴에서 데이터 형식(들)을 선택하고 각 데이터 형식에 대한 대체 값을 지정합니다. 모든 데이터 형식은 위의 기본 구성 적용 패턴을 따르지만 신뢰도 수준을 재정의하고 각 데이터 형식에 대해 도메인 적용 패턴을 미세 조정할 수 있습니다.

기본 구성에서 대체 값을 입력하려면 신뢰도 수준 재정의를 선택합니다. 예를 들어 기본 구성이 중간으로 설정된 경우 테스트 중에 데이터 유형 중 하나가 안정적으로 수정되지 않는 것을 확인할 수 있습니

다. 재정의를 낮음으로 설정하여 다른 데이터 유형에 사용되는 로직을 조정하지 않고도 수정 가능성을 높일 수 있습니다.

기본 구성을 변경하지 않고 URLs 간에 수정이 적용되는 방식을 미세 조정하려면 URL 적용 재정의를 적용합니다. 예를 들어 URL 재정의 사용을 설정하여 회사 디렉터리 웹 사이트 또는 웹 기반 이메일의 이메일 주소에 대한 사용자 액세스를 중단하지 않고 고객 관계 관리 시스템에서 이메일 주소 수정을 적용할 수 있습니다.

다음은 데이터 유형 및 해당 기본 제공 패턴 IDs

builtInPatternId	데이터 유형
awsAccessKey:	AWS 액세스 키
awsSecretKey:	AWS 보안 키
cardNumbers:	신용 카드 번호
암호화:	암호화폐 주소
cusipNum:	CUSIP 번호
날짜:	Date
deaNum:	미국 DEA 번호
dob:	생년월일
driversLicense:	미국 운전면허증
emailAddress:	이메일 주소
ein:	미국 고용주 식별 번호
expDate:	신용 카드 만료 날짜
healthInsuranceNum:	메디케어 건강 보험 클레임 번호
hipaaCode:	HIPAA ICD-10 코드
indivTaxId:	미국 개인 세금 ID

builtInPatternId	데이터 유형
ipAddr:	IP 주소
isin:	국제 증권 식별 번호
jwt:	JSON 웹 토큰
locationCoord:	위치 좌표
macAddr:	MAC 주소
medicareBeneficiaryId:	메디케어 수혜자 번호
npi:	국가 공급자 식별 번호
ndc:	국가 의약품 코드(NDC)
passportNum:	미국 여권 번호
phoneNum:	전화번호
routingNumber:	ABA 라우팅 번호
ssn:	미국 사회보장번호
swiftCode:	SWIFT 코드
시간:	Time
vin:	미국 차량 식별 번호

Amazon WorkSpaces Secure Browser에서 사용자 지정 인라인 수정

고객은 사용자 지정 내부 애플리케이션 IDs. 사용자 지정 인라인 수정 패턴을 생성하려면 다음 단계를 따르세요.

1. 데이터 보호 설정으로 이동합니다.
2. 사용자 지정 인라인 수정을 선택하고 추가합니다.
3. 사용자 지정 데이터 형식의 이름을 입력합니다.

4. 정규식 값을 입력합니다.
   - 정규식 값은 JavaScript 정규식 리터럴 구문과 일치해야 합니다. 자세한 내용은 Regular expressions를 참조하세요. 정규식의 예는 입니다`/ex[am]+ple/i`.
   - 지원하려는 웹 사이트에서 사용자 지정 패턴을 테스트해야 합니다. 사용자 지정 패턴에 오류가 있는 경우 의도하지 않은 성능 문제가 발생할 수 있습니다.
5. 대체 값을 지정합니다.
6. 다음을 포함한 선택적 사용자 지정에 대한 추가 옵션을 선택합니다.
   - 키워드를 추가하여 수정 로직을 미세 조정합니다. 키워드는 적용 정확도를 높일 수 있습니다. Javascript 정규 표현식 리터럴 구문에 키워드를 추가합니다. 자세한 내용은 Regular expressions를 참조하세요.

     예를 들어 내부 시스템에서 사용되는 클라이언트 IDs에 대한 사용자 지정 수정 패턴을 생성하는 경우 키워드 필드에 `/client name/i`를 추가하여 스캔 및 감지 로직에 알릴 수 있습니다.
   - URL 적용 재정의를 적용하여 기본 구성을 변경하지 않고 URLs 간에 수정이 적용되는 방식을 미세 조정합니다.

     예를 들어 URL 재정의 사용을 설정하여 회사 디렉터리 웹 사이트 또는 웹 기반 이메일의 이메일 주소에 대한 사용자 액세스를 중단하지 않고 고객 관계 관리 시스템에서 이메일 주소 수정을 적용할 수 있습니다.
   - 데이터 유형에 대한 설명(선택 사항)을 입력합니다.

Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 생성

WorkSpaces Secure Browser에서 데이터 보호 설정을 생성할 수 있습니다.

데이터 보호 설정을 생성하려면

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. 왼쪽 탐색 창에서 데이터 보호 설정을 선택합니다.
3. 데이터 보호 설정 생성을 선택합니다.
4. 설정에 대한 표시 이름(필수)과 설명(선택 사항)을 입력합니다.
5. 인라인 수정을 위한 기본 설정을 선택합니다. 다음을 설정할 수 있습니다.
   - 모든 데이터 유형의 엄격성 수준
   - 수정을 적용해야 하는 도메인

6. 지원되는 유형에서 기본 인라인 수정 데이터 유형을 선택하거나 사용자 지정 데이터 유형을 생성합니다. 엄격한 수준 및 도메인 예외를 포함하여 각 데이터 유형에 대해 재정의를 설정할 수 있습니다.
7. 보고를 위해 태그(선택 사항)를 추가합니다.
8. 마치면 [Save]를 선택합니다.

Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 연결

WorkSpaces Secure Browser에서 데이터 보호 설정을 연결할 수 있습니다.

데이터 보호 설정을 기존 포털과 연결하려면

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. 왼쪽 탐색 창에서 웹 포털을 선택합니다.
3. 웹 포털을 선택하고 편집을 선택합니다.
4. 데이터 보호 설정에서 포털의 설정을 선택합니다.
5. 저장을 선택합니다.

새 포털을 생성할 때 데이터 보호 설정을 연결하려면 다음 단계를 따르세요.

새 포털을 생성할 때 데이터 보호 설정을 연결하려면

1. 데이터 보호 설정에 도달할 때까지의 지침에 따라 포털을 the section called “웹 포털 생성” 생성합니다.
2. 드롭다운 메뉴에서 데이터 보호 설정을 선택합니다.
3. 의 단계를 완료the section called “웹 포털 생성”하여 포털 생성을 완료합니다.

새 포털을 생성할 때 데이터 보호 설정을 생성하려면 다음 단계를 따르세요.

새 포털을 생성할 때 데이터 보호 설정을 생성하려면

1. 데이터 보호 설정에 도달할 때까지의 지침에 따라 포털을 the section called “웹 포털 생성” 생성합니다.
2. 드롭다운 메뉴에서 데이터 보호 설정을 선택합니다.
3. 설정에 대한 표시 이름(필수)과 설명(선택 사항)을 입력합니다.

4. 인라인 수정을 위한 기본 설정을 선택합니다. 다음을 설정할 수 있습니다.
   - 모든 데이터 유형의 엄격성 수준
   - 수정을 적용해야 하는 도메인
5. 지원되는 유형에서 기본 인라인 수정 데이터 유형을 선택하거나 사용자 지정 데이터 유형을 생성합니다. 엄격한 수준 및 도메인 예외를 포함하여 각 데이터 유형에 대해 재정의를 설정할 수 있습니다.
6. 보고할 태그(선택 사항)를 추가합니다.
7. 마치면 [Save]를 선택합니다.
8. 데이터 보호 설정에서 새로 고침 버튼을 선택한 다음 드롭다운 메뉴에서 데이터 보호 설정을 선택합니다.
9. 포털 생성 지침에 따라 포털 생성을 완료합니다.

Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 편집

WorkSpaces Secure Browser에서 데이터 보호 설정을 편집할 수 있습니다.

데이터 보호 설정을 편집하려면

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. 목록 보기에서 편집하려는 데이터 보호 설정과 데이터 보호 설정을 선택합니다.
3. 이름, 설명, 기본 설정, 데이터 유형(지원 또는 사용자 지정)을 업데이트하고 신뢰도 수준 또는 도메인 재정의를 적용할 수 있습니다.
4. 저장을 선택합니다.

Amazon WorkSpaces Secure Browser에서 데이터 보호 설정 삭제

WorkSpaces Secure Browser에서 데이터 보호 설정을 삭제할 수 있습니다.

데이터 보호 설정을 삭제하려면

1. 데이터 보호 설정과 연결된 포털이 있는 경우 데이터 보호 설정을 삭제하기 전에 먼저 연결을 제거해야 합니다.
2. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.

3. 목록 보기에서 삭제할 데이터 보호 설정과 데이터 보호 설정을 선택합니다.
4. 삭제를 선택합니다.

Amazon WorkSpaces Secure Browser의 브랜딩 사용자 지정

시각적 요소, 텍스트 콘텐츠 및 서비스 약관을 수정하여 최종 사용자에게 표시되는 로그인 및 로드 화면을 사용자 지정할 수 있습니다. 브랜딩 사용자 지정은 조직의 자격 증명에 맞는 일관된 경험을 만드는 데 도움이 됩니다.

개요

브랜딩 사용자 지정을 사용하면 사용자 경험의 다음 측면을 개인화할 수 있습니다.

- 시각적 요소 - 로고, 파비콘 및 월페이퍼를 업로드하고 브랜드 아이덴티티와 일치하는 색상 테마를 선택합니다.
- 텍스트 콘텐츠 - 로그인 흐름 전체에서 브랜드 음성을 유지하도록 환영 메시지, 브라우저 탭 제목 및 기타 선택적 텍스트 필드를 사용자 지정합니다. 특정 필드에 사용자 지정 텍스트를 지정하지 않으면 기본 텍스트가 사용됩니다. 자세한 내용은 the section called “사용자 지정 지침”을 참조하세요.
- 서비스 약관(선택 사항) - 사용자가 세션을 시작하기 전에 승인해야 하는 조직의 서비스 약관을 추가합니다.

> **Note**
>
> 포털의 도메인 이름을 사용자 지정할 수도 있습니다. 자세한 내용은 the section called “사용자 지정 도메인”을 참조하세요.

주제

- 포털에 대한 브랜딩 사용자 지정 구성
- 사용자 지정 지침

포털에 대한 브랜딩 사용자 지정 구성

작동 방식

브랜딩 사용자 지정을 구성하는 경우:

- 시각적 요소와 텍스트 요소는 로그인 화면과 로드 화면 모두에 적용됩니다.
- 브라우저 탭에는 사용자 지정 파비콘과 제목이 표시됩니다.
- 최종 사용자는 새 세션을 시작할 때 사용자 지정 변경 사항을 볼 수 있습니다. 경우에 따라 변경 사항이 표시되기까지 몇 분 정도 걸릴 수 있습니다.
- 서비스 약관이 구성된 경우 최종 사용자는 스트리밍 세션을 시작하기 전에 서비스 약관에 동의해야 합니다. 모든 세션이 시작될 때 질문을 받게 됩니다.

사전 조건

시작하기 전:

- 포털 설정을 수정하는 데 필요한 권한이 있는지 확인합니다. 섹션을 참조하세요the section called “AWS 관리형 정책”.
- 의 사양에 따라 브랜딩 자산(로고, 파비콘, 월페이퍼)을 준비합니다the section called “사용자 지정 지침”.

시작하기

브랜딩 사용자 지정을 구성하려면 다음 단계를 따르세요.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 선택하고 웹 포털을 선택합니다.
3. 포털을 선택하고 사용자 설정 탭을 선택합니다.
4. 브랜딩 사용자 지정 섹션에서 편집을 선택합니다.
5. 필요에 따라 다음 섹션을 구성합니다.
   - 콘텐츠 편집기 - 모든 시각적 요소(회사 로고, 파비콘 및 선택적 월페이퍼)를 업로드하고 색상 테마를 선택합니다. 로컬 컴퓨터 또는 S3 버킷에서 파일을 업로드할 수 있습니다. S3 버킷 권한 설정에 대한 자세한 내용은 섹션을 참조하세요the section called “S3 버킷 권한 설정”.
   - 텍스트 편집기 - 로그인 화면에 나타나는 텍스트 사용자 지정.
   - 서비스 약관 편집기 - 선택적으로 사용자가 승인해야 하는 용어를 추가합니다.
6. 변경 사항 저장을 선택합니다.

각 사용자 지정 옵션에 대한 자세한 지침은 섹션을 참조하세요the section called “사용자 지정 지침”.

S3 버킷 권한 설정

컴퓨터에서 직접 브랜딩 파일을 업로드하거나 S3 버킷에서 기존 객체를 선택할 수 있습니다. S3 버킷에서 시각적 요소(회사 로고, 파비콘 및 월페이퍼)에 대한 파일을 업로드하도록 선택한 경우 S3 버킷에 대한 적절한 권한을 설정해야 합니다.

동일한 계정에서 S3 객체 선택

IAM 사용자 또는 역할에 브랜딩 자산이 포함된 버킷에 대한 `s3:GetObject` 권한이 이미 있는 경우 추가 구성이 필요하지 않습니다.

다른 계정에서 S3 객체 선택

다른 AWS 계정에서 S3 버킷을 선택하려면 소스 계정의 버킷 정책과 관리자 계정의 IAM 정책을 모두 구성해야 합니다.

버킷 정책 예제(소스 계정에서):

소스 계정의 S3 버킷에이 정책을 적용합니다. *123456789012*을 관리자 계정 ID로 바꾸고 *source-account-bucket-name*을 실제 버킷 이름으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

IAM 정책 예제(관리자 계정):

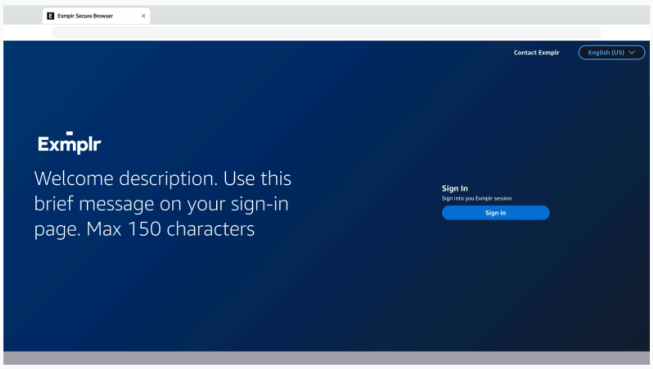
관리자 계정의 IAM 사용자 또는 역할에이 정책을 연결합니다. *source-account-bucket-name*을 소스 계정의 실제 버킷 이름으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

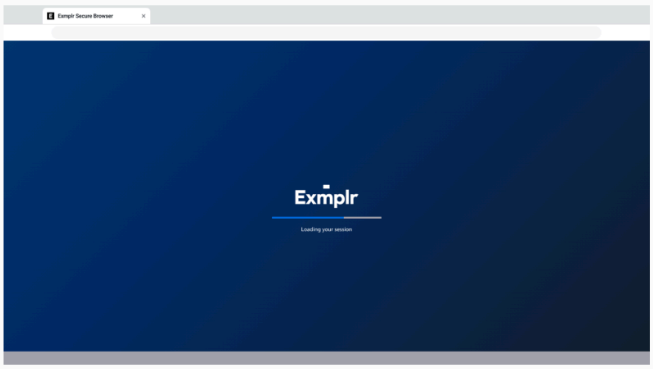
교차 계정 액세스에 대한 자세한 내용은 S3 Access Grants 교차 계정 액세스를 참조하세요.

사용자 지정 지침

로그인 및 로드 페이지에서 브랜딩 요소와 텍스트를 업데이트하여 최종 사용자의 로그인 및 로드 환경을 사용자 지정합니다. 로고 및 월페이퍼와 같은 시각적 요소를 수정하고, 환영 메시지 및 헤더와 같은 텍스트 요소를 편집하고, 선택적으로 사용자가 세션을 시작하기 전에 수락해야 하는 서비스 약관 계약을 구성할 수 있습니다.



Sign in Page



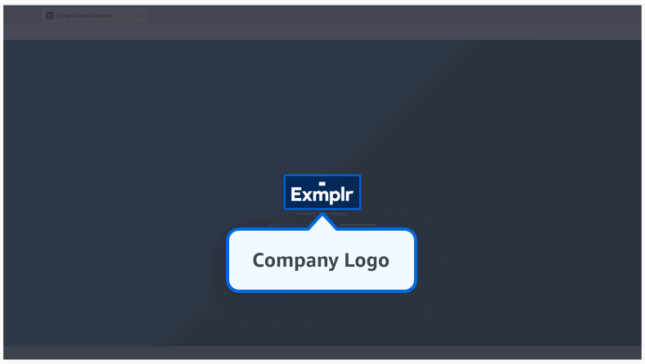
Loading Page

콘텐츠 편집기

회사 로고

로고는 로그인 화면과 로딩 화면에 표시되어 사용자 경험 전반에서 일관된 브랜딩을 제공합니다.

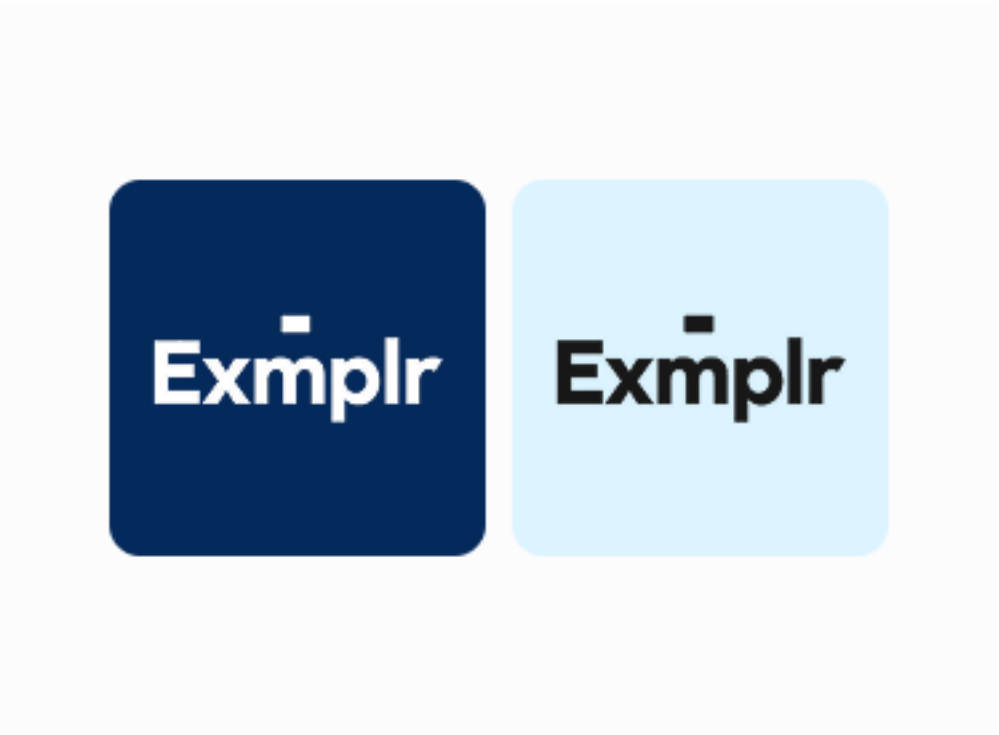
Sign in page



Loading page

- 지원되는 형식: JPG, ICO 또는 PNG
- 최대 파일 크기: 100KB

수행



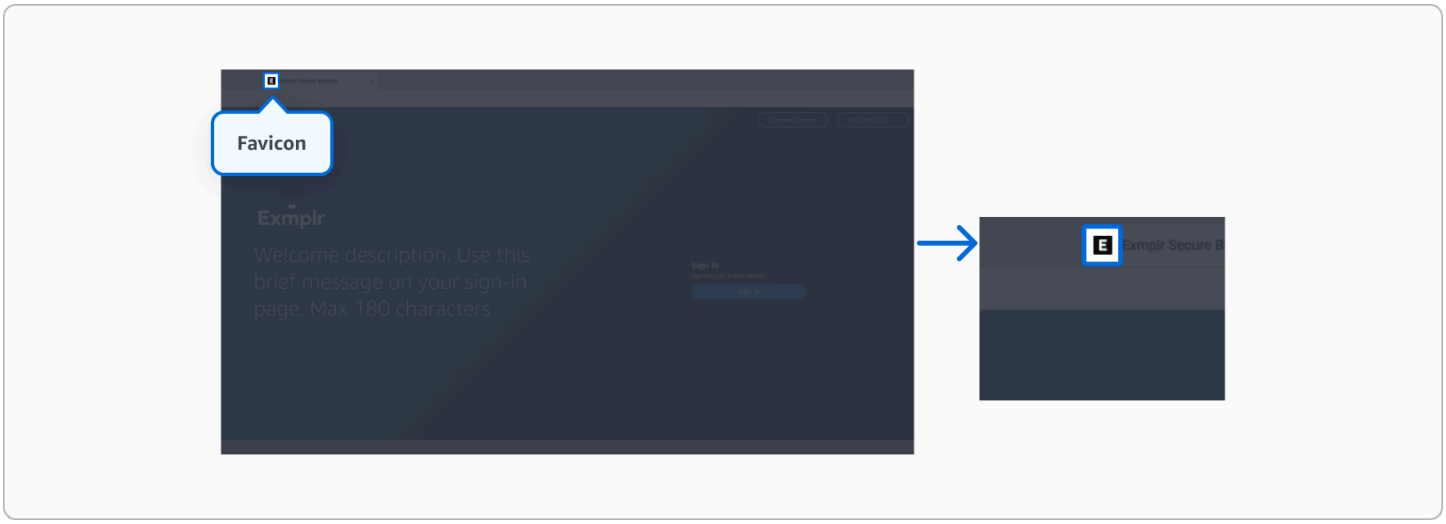
- 로고 변형이 다른 경우(예: 다른 색상 또는 스타일) 선택한 월페이퍼 배경과 가장 잘 대비되는 것을 선택합니다.

하지 말 것

- 로고 크기를 조정할 때 종횡비를 무시하지 마세요.
- 로고 크기가 올바르게 지정되지 않은 로고는 왜곡된 것처럼 보일 수 있으므로 사용하지 마세요.

파비콘

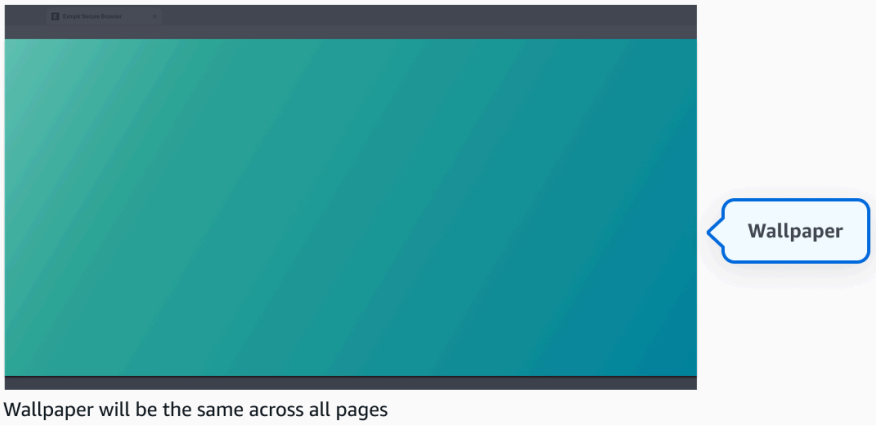
파비콘은 브라우저 탭에 나타나는 작은 아이콘으로, 사용자가 여러 열린 탭에서 애플리케이션을 식별할 수 있도록 도와줍니다.



- 지원되는 형식: JPG, ICO 또는 PNG
- 최대 파일 크기: 100KB
- 권장 가로 세로 비율: 1:1

월페이퍼 - 선택 사항

월페이퍼는 모든 화면의 배경 이미지로 사용되어 통일된 시각적 경험을 제공합니다. 사용자 지정 월페이퍼를 업로드하지 않으면 아래 표시된 기본 월페이퍼가 사용됩니다. 콘텐츠 가독성을 방해하지 않으면서 브랜딩을 보완하는 이미지를 선택하세요.



Wallpaper will be the same across all pages

- 지원되는 형식: JPG 또는 PNG
- 최대 파일 크기: 5MB
- 권장 가로 세로 비율: 16:9
- 권장 최소 해상도: 1920 x 1080

수행

- 전경 콘텐츠를 방해하지 않는 미세하고 대비가 낮은 배경화면 또는 흐린 이미지를 사용합니다.
- 텍스트 뒤의 바쁜 영역을 방지하려면 사전 설정된 텍스트 배치를 고려하세요.
- 브랜드 색상을 활용하고 오버레이를 사용하여 대비와 가독성을 높입니다.

하지 말 것

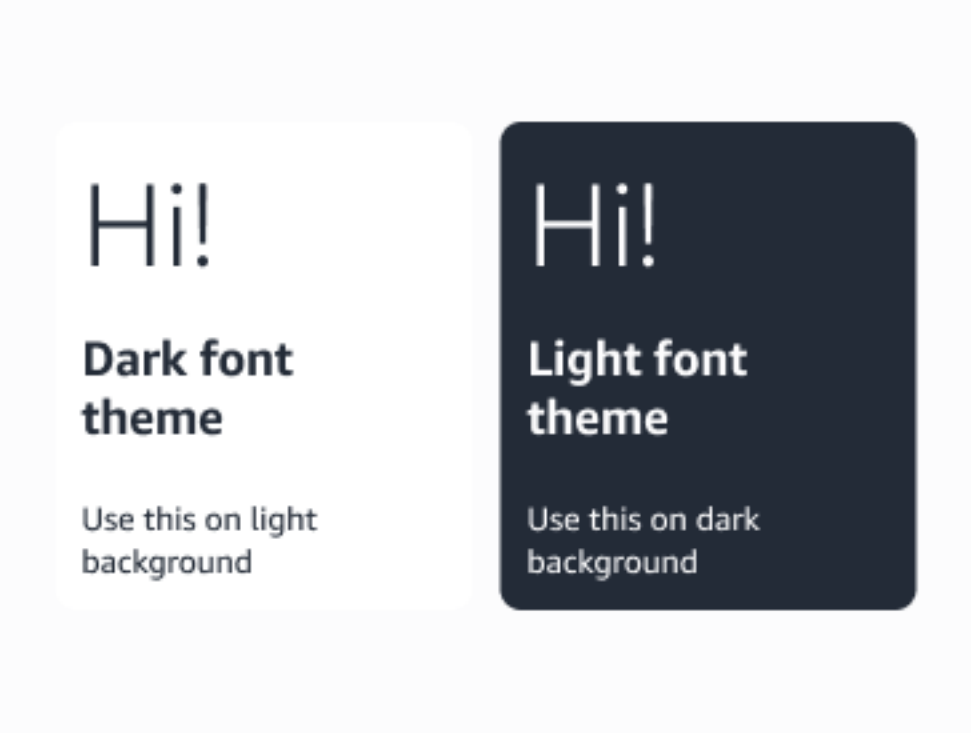
- 중요한 텍스트 바로 뒤에 사용 중이거나 포화되었거나 세부 정보가 많은 이미지를 사용하지 마세요.
- 시각적으로 복잡한 이미지 또는 사전 설정된 텍스트 위치에 가독성 제한이 발생하는 급격한 전환이 있는 이미지를 사용하지 마세요.
- 충분한 대비 없이 배경에서 텍스트를 분리하기 위해 색상에만 의존하지 마세요.

색상 테마

글꼴, 버튼 및 모달을 반영하는 밝거나 어두운 테마 중에서 선택합니다.

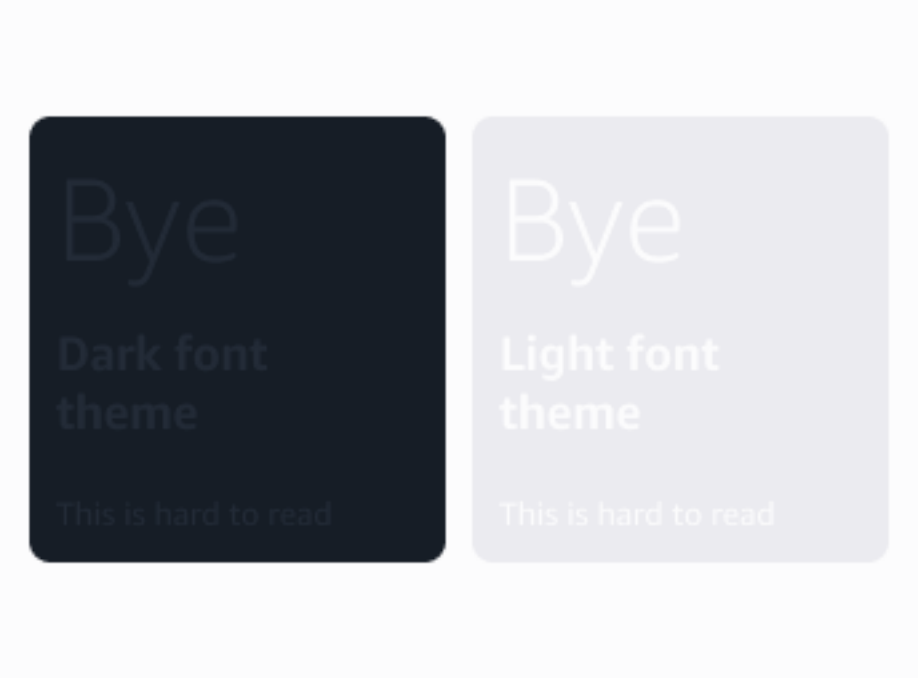
- 라이트 테마 - 어두운 배경에 적합하며, 저조도 환경에서 작업할 때 선명한 대비를 제공하고 눈의 피로를 줄입니다.
- 다크 테마 - 밝은 배경에 최적화되어, 주변이 밝을 때 눈부심을 줄이고 편안하게 볼 수 있도록 합니다.

수행



- 배경 요소/벽지와 강력한 대조를 이룹니다.
- 밝은 배경에서 어두운 색상 테마를 사용합니다.
- 어두운 배경에서 밝은 색상 테마를 사용합니다.

하지 말 것



- 이미지나 복잡한 배경화면 위에 밝거나 어두운 글꼴을 배치하지 마세요.

텍스트 편집기

텍스트 편집기를 사용하여 최종 사용자의 로그인 화면에 표시되는 텍스트를 사용자 지정할 수 있습니다. 브랜딩 사용자 지정을 활성화하려면 하나 이상의 언어를 추가해야 합니다.

새 사용자의 경우: 브라우저 언어 기본 설정이 감지되며 브랜딩 언어로 구성된 경우 해당 언어로 포털 페이지가 표시됩니다. 브라우저 언어가 구성된 언어가 아니라면 사용 가능한 경우 영어(en-US)로 기본 설정됩니다. 영어를 구성하지 않은 경우 구성된 언어에서 알파벳순으로 첫 번째 언어가 사용됩니다.

재방문 사용자: 이전 세션의 언어 기본 설정이 브라우저 쿠키에 저장됩니다. 해당 언어가 구성된 브랜딩 언어인 경우 해당 언어가 사용됩니다. 그렇지 않으면 동일한 대체 로직을 따라 사용 가능한 경우 영어(en-US), 아니면 알파벳순으로 구성된 첫 번째 언어가 사용됩니다.

다음 로캘(언어 코드)이 지원됩니다.

- 독일어(de-DE)
- 영어(en-US)
- 스페인어(es-ES)
- 프랑스어(fr-FR)
- 인도네시아어(id-ID)

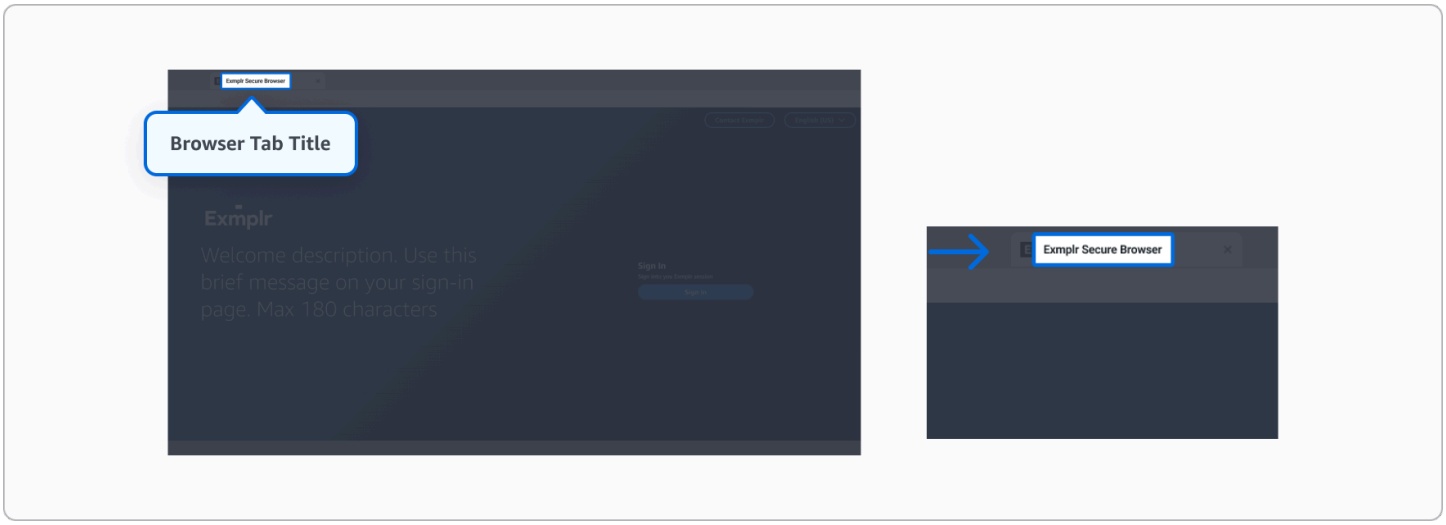
- 이탈리아어(it-IT)
- 일본어(ja-JP)
- 한국어(ko-KR)
- 포르투갈어(pt-BR)
- 중국어 간체(zh-CN)
- 중국어 번체(zh-TW)

보안상의 이유로 모든 텍스트 필드에서 다음 문자가 차단됩니다.

- 미만
- >(초과)
- &(앰퍼샌드)
- '(곧은 아포스트로피)
- `(백틱/그레이브 악센트)
- ~ (물결표)
- \(백슬래시)

브라우저 탭 제목

브라우저 탭에 표시되는 텍스트입니다. 최대 25자입니다.

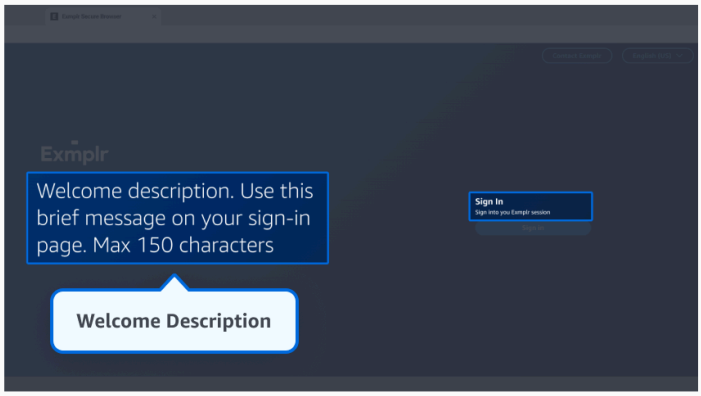


권장 사항

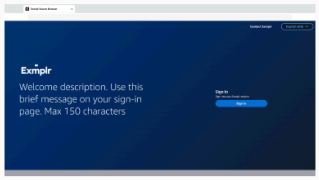
여러 탭이 열려 있더라도 읽을 수 있도록 짧고 명확한 제목을 사용하는 것이 좋습니다.

환영 설명

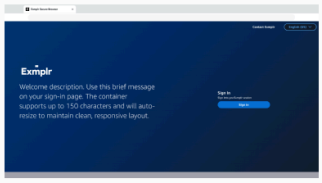
로그인 화면에서 회사 로고와 함께 표시되는 간략한 설명입니다. 최대 150자입니다.



Welcome description



Starting font sizing



Adapted sizing to Max characters

권장 사항

가독성을 높이기 위해 텍스트를 간결하게 유지합니다. 더 긴 텍스트는 자동으로 더 작은 글꼴 크기로 조정되는 반면, 더 짧은 메시지는 더 두드러지게 표시됩니다.

연락처 섹션

문의 버튼 - 선택 사항

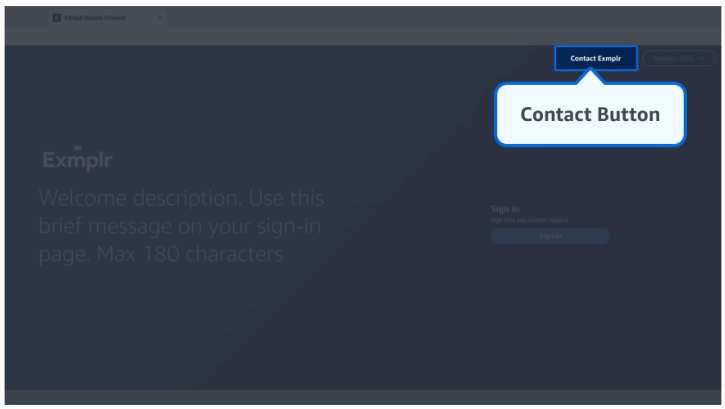
로그인 화면의 문의 버튼 텍스트입니다. 비워 두면 “문의하기”가 표시됩니다. 최대 30자입니다.

문의 링크 - 선택 사항

로그인 화면의 문의 버튼 링크입니다. 다음을 사용할 수 있습니다.

- 사용자를 웹 페이지로 안내하는 HTTPS URL
- mailto: 사용자의 이메일 클라이언트를 여는 링크

비워 두면 문의 버튼이 화면에서 숨겨집니다.



권장 사항

텍스트를 짧게, 이상적으로는 2~3단어로 유지합니다.

로그인 섹션

로그인 헤더 - 선택 사항

로그인 페이지의 로그인 섹션에 대한 헤더입니다. 비워 두면 "로그인"이 표시됩니다. 최대 100자입니다.

로그인 설명 - 선택 사항

로그인 섹션에 대한 설명 텍스트입니다. 비워 두면 "WorkSpaces Secure Browser 세션에 로그인하세요"가 표시됩니다. 최대 250자.

로그인 버튼 - 선택 사항

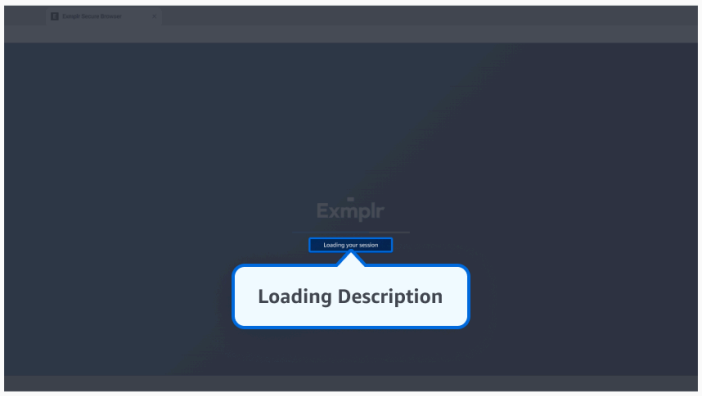
로그인 버튼에 표시되는 텍스트입니다. 비워 두면 "로그인"이 표시됩니다. 최대 30자입니다.

권장 사항

- 텍스트를 짧게 유지합니다.
- 로그인 버튼을 누르면 사용자가 포털에 대해 구성된 자격 증명 공급자로 이동합니다. 특정 자격 증명 공급자를 반영하도록 버튼 텍스트를 사용자 지정할 수 있습니다.

설명 로드

연결 중 로딩 화면에 표시되는 텍스트입니다. 비워 두면 "연결 중..."이 표시됩니다. 최대 300자.



Loading screen

권장 사항

이 메시지는 세션이 로드되는 동안에만 표시되므로 최종 사용자가 읽을 시간이 없을 수 있습니다. 너무 길게 만들지 않도록 하세요.

서비스 약관 - 선택 사항

최종 사용자가 스트리밍 세션을 시작하기 전에 검토하고 수락해야 하는 서비스 약관을 사용자 지정할 수 있습니다. 이 콘텐츠는 마크다운 파일을 업로드하거나 내장 마크다운 편집기를 사용하여 추가할 수 있습니다.

성공적으로 로그인하면 사용자에게 서비스 약관이 표시됩니다. 사용자는 문서 전체를 스크롤하고 "수락" 버튼을 클릭해야 Secure Browser 세션으로 이동할 수 있습니다. 사용자가 "거절"을 클릭하면 로그인 페이지로 다시 리디렉션됩니다.

참고로 이는 선택적 설정입니다. 서비스 약관을 추가하지 않으면 사용자가 로그인한 후 세션으로 바로 이동하게 됩니다.

지원되는 형식:

- 기본 텍스트 스타일(굵게, 기울임꼴)
- 제목
- 순서가 지정된 목록과 순서가 지정되지 않은 목록
- 인용구
- 가로선
- 간단한 단락 및 줄 바꿈

보안을 위해 다음 요소가 차단됩니다.

- 스크립트 및 코드 실행
- 양식 및 iframe과 같은 대화형 요소
- 안전하지 않은 프로토콜 및 파일 경로
- HTML 속성 및 스타일
- 외부 링크 및 테이블

서비스 약관 파일은 크기가 150KB를 초과해서는 안 됩니다.

Amazon WorkSpaces Secure Browser에서 WebAuthn 리디렉션 지원 활성화

> **Warning**
>
> WebAuthn 리디렉션은 인터넷 액세스가 활성화된 브라우저 세션에서만 작동합니다. 포털의 네트워크 설정이 WebAuthn 기능이 제대로 작동하도록 인터넷 액세스를 허용하는지 확인합니다.

WorkSpaces Secure Browser는 원격 브라우저 세션 내에서 액세스하는 웹 사이트에 대해 WebAuthn(웹 인증)을 지원합니다. 이를 통해 사용자는 WorkSpaces Secure Browser 세션을 탐색하는 동안 로컬 FIDO2 보안 키, 생체 인식 인증자 및 플랫폼 인증자를 사용하여 웹 사이트에 인증할 수 있습니다.

> **Note**
>
> WebAuthn 리디렉션은 Google Chrome 136(이상) 또는 Microsoft Edge 137(이상)을 사용하는 최종 사용자가 사용할 수 있습니다. 이 기능은 Safari 또는 Firefox와 같은 비Chromium 브라우저에서는 사용할 수 없습니다.
> WebAuthn 리디렉션 기능을 활성화하려면 관리자가 다음 두 가지를 모두 구성해야 합니다.
>
> 1. 포털 사용자 설정 - 포털 설정에서 WebAuthn 리디렉션 활성화
> 2. 최종 사용자 로컬 브라우저 정책 - WebAuthn 리디렉션을 허용하도록 사용자 디바이스에서 WebAuthenticationRemoteDesktopAllowedOrigins 브라우저 정책을 구성합니다.

주제

- 포털 설정에서 WebAuthn 리디렉션 활성화
- WebAuthn에 대한 로컬 브라우저 정책 구성
- 원격 브라우저 세션에서 WebAuthn 리디렉션 사용
- WebAuthn 리디렉션 문제 해결

포털 설정에서 WebAuthn 리디렉션 활성화

원격 브라우저 세션 내에서 액세스하는 웹 사이트에 대해 WebAuthn 리디렉션을 활성화하려면 다음 단계를 따르세요.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)을 엽니다.
2. WorkSpaces Secure Browser, 웹 포털을 차례로 선택하고 웹 포털을 선택한 다음 편집을 선택합니다.
3. 사용자 설정 섹션으로 이동합니다.
4. 사용자 권한에서 사용자가 포털 세션에서 로컬 인증을 사용하도록 허용을 허용으로 설정합니다.
5. 저장을 선택하여 구성을 적용합니다.

WebAuthn에 대한 로컬 브라우저 정책 구성

포털 설정에서 WebAuthn 리디렉션을 활성화하는 것 외에도 사용자의 로컬 디바이스와 원격 브라우저 세션 간의 WebAuthn 리디렉션을 허용하도록 로컬 브라우저 정책을 구성해야 하며 그 반대의 경우도 마찬가지입니다. 이 구성은 일반적으로 엔터프라이즈 환경의 경우 IT 관리자가, BYOD 시나리오의 경우 개별 사용자가 관리합니다.

브라우저 정책에는 해당 리전의 WorkSpaces Secure Browser 콘텐츠 도메인이 포함되어야 합니다. 리전에 따라 `WebAuthenticationRemoteDesktopAllowedOrigins` 정책에 다음 오리진을 추가합니다.

`https://<region>.content.workspaces-web.com`

예를 들어 us-west-2에서는 다음과 같습니다. `https://us-west-2.content.workspaces-web.com`

특정 구성 방법은 엔터프라이즈 환경에서 브라우저를 관리하는지 아니면 BYOD 사용자를 위한 개별 디바이스를 구성하는지에 따라 달라집니다. 브라우저 정책에 대한 자세한 내용은 Chrome Enterprise 정책 설명서 및 Microsoft Edge 정책 설명서를 참조하세요.

> **Note**
>
> 정책을 적용하려면 브라우저를 다시 시작해야 할 수 있습니다.

원격 브라우저 세션에서 WebAuthn 리디렉션 사용

포털 설정에서 WebAuthn 리디렉션이 활성화되고 로컬 브라우저 정책이 구성되면 사용자는 WorkSpaces Secure Browser 원격 브라우저 세션 내의 웹 사이트에서 WebAuthn 인증을 사용할 수 있습니다.

사용자는 다음을 사용하여 웹 사이트에 인증할 수 있습니다.

- 로컬 디바이스에 연결된 FIDO2 보안 키
- 패스키
- Windows Hello 또는 Touch ID와 같은 플랫폼 인증자

WebAuthn 인증 프로세스는 원격 브라우저 세션에서 사용자의 로컬 디바이스로 원활하게 전달되어 원격 브라우징 환경의 보안 이점을 유지하면서 암호 없는 보안 인증을 제공합니다.

WebAuthn 리디렉션 문제 해결

사용자가 원격 브라우저 세션에서 WebAuthn 리디렉션 문제를 경험하는 경우 다음 문제 해결 단계를 사용하여 일반적인 문제를 식별하고 해결합니다.

주제

- WebAuthn 리디렉션이 작동하지 않음
- 일반적인 오류 메시지

WebAuthn 리디렉션이 작동하지 않음

WebAuthn 인증 프롬프트가 표시되지 않거나 작동하지 않는 경우:

1. 사용자 권한 아래의 포털 설정에서 WebAuthn이 활성화되어 있는지 확인합니다.
2. `chrome://policy` 또는 로 이동하여에 리전의 콘텐츠 URL이 `WebAuthenticationRemoteDesktopAllowedOrigins` 포함되어 있는지 `edge://policy` 확인하여 로컬 브라우저 정책이 올바르게 구성되어 있는지 확인합니다.
3. 브라우저 버전이 Chrome 136 이상 또는 Edge 137 이상의 요구 사항을 충족하는지 확인합니다.
4. 다른 인증자(보안 키와 플랫폼 인증자 비교)로 테스트합니다.

일반적인 오류 메시지

다음은 일반적인 오류 메시지와 해결 방법입니다.

WebAuthn 오류 메시지 및 해결 방법

오류 메시지	해결 방법
Amazon DCV WebAuthn 리디렉션이 등록 요청을 완료하지 못함: 클라이언트에서 Webauthn 리디렉션을 지원하지 않음	지원되는 브라우저 및 버전(Chrome 136 이상 또는 Edge 137 이상)을 사용하고 있는지 확인합니다.
프롬프트가 표시되지만 로컬 인증자와 상호 작용할 수 없음	원격 브라우저에 Amazon DCV WebAuthn 리디렉션 확장이 설치되어 활성화되어 있는지 확인합니다.
Amazon DCV WebAuthn 리디렉션이 등록 요청을 완료하지 못했습니다. 신뢰 당사자 ID가 현재 도메인의 등록 가능한 도메인 접미사이거나 같지 않습니다. 이후 클레임된 RP ID의 .well-known/webauthn 리소스를 가져오려는 시도가 실패했습니다.	즉, WebAuthenticationRemoteDesktopAllowedOrigins 로컬 브라우저 정책이 적용되지 않습니다. 정책을 확인하고 콘텐츠 도메인을 허용하도록 업데이트합니다. 브라우저가 다시 시작되었는지 확인합니다. 변경 사항을 적용하려면 새 세션을 시작해야 할 수 있습니다.
작업이 시간 초과되었거나 허용되지 않았습니다. 참조: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client.	이 오류는 (1) DCV WebAuthn 리디렉션 확장이 설치 또는 활성화되지 않았거나, (2) 사용자가 인증 프롬프트를 취소하거나, (3) 사용자가 보안 키에 잘못된 PIN을 입력하거나, (4) 사용자가 프롬프트와 상호 작용하지 않고 요청 시간이 초과된 경우 발생할 수 있습니다.

Amazon WorkSpaces Secure Browser에서 도구 모음 제어 관리

도구 모음 제어를 사용하면 다음 옵션을 포함하여 최종 사용자 세션에 대한 도구 모음 프레젠테이션을 구성할 수 있습니다.

- Features
  - 클립보드: 활성화되면 세분화된 컨트롤(복사 전용, 붙여넣기 전용 또는 둘 다)을 사용하여 복사/붙여넣기를 허용합니다. 비활성화하면가 아이콘을 숨기고 도구 모음에서 사용을 방지합니다.
  - 파일 전송: 활성화하면 세분화된 제어(업로드만, 다운로드만 또는 둘 다)를 사용하여 파일 작업을 허용합니다. 비활성화하면 아이콘을 숨기고 전송을 방지합니다.
  - 마이크: 활성화되면 마이크 사용을 허용합니다. 비활성화하면 아이콘을 숩깁니다.

  - 웹캠: 활성화되면 카메라 사용을 허용합니다. 비활성화하면 아이콘을 숨깁니다.
  - 듀얼 모니터: 활성화되면 듀얼 모니터 사용을 허용합니다. 비활성화하면 아이콘을 숨깁니다.
  - 전체 화면: 활성화하면 전체 화면 모드를 허용합니다. 비활성화하면 아이콘을 숨깁니다.
  - Windows: 활성화되면 창 간 이동을 허용합니다. 비활성화하면 아이콘을 숨깁니다.
- 설정
  - 도구 모음 테마: 밝거나 어두운 모드 표시를 제어합니다. 구성은 최종 사용자 테마 제어를 제거합니다.
  - 도구 모음 상태: 도구 모음의 도킹 또는 분리 상태를 설정합니다. 구성은 도구 모음 상태에 대한 최종 사용자 제어를 제거합니다.
  - 최대 해상도: 허용되는 가장 높은 디스플레이 해상도를 정의합니다. 사용자는이 정의된 한도까지만 해상도를 선택할 수 있습니다.

포털에 대한 사용자 지정 도메인 구성

기본 포털 URL 대신 자체 도메인 이름을 통해 액세스할 수 있도록 WorkSpaces Secure Browser 포털에 대한 사용자 지정 도메인을 구성할 수 있습니다. 이 기능을 사용하면 조직의 브랜딩에 맞는 도메인을 사용하여 사용자에게 보다 통합된 환경을 제공할 수 있습니다.

개요

사용자 지정 도메인을 사용하면 사용자 경험의 다음 측면을 개인화할 수 있습니다.

- 브랜드 포털 액세스 - 사용자는 기본 AWS 엔드포인트 대신 조직의 도메인을 통해 포털에 액세스합니다.
- 일관된 사용자 경험 - 조직에 맞는 친숙한 도메인 이름을 사용하여 브랜드 일관성을 유지합니다.

> **Note**
>
> 포털의 시각적 모양 및 브랜딩 요소를 사용자 지정하려면 섹션을 참조하세요the section called “브랜딩 사용자 지정”.

주제

- 포털에 대한 사용자 지정 도메인 구성
- 사용자 지정 도메인 문제 해결

포털에 대한 사용자 지정 도메인 구성

작동 방식

사용자 지정 도메인을 구성하는 경우:

- 사용자 지정 도메인을 사용하여 역방향 프록시를 생성하고 구성하여 트래픽을 포털 엔드포인트로 라우팅합니다.
- 사용자는 기본 포털 엔드포인트 대신 사용자 지정 도메인을 통해 포털에 액세스합니다.
- SSL 인증서는 프로세스 전반에 걸쳐 보안 연결을 보장합니다.

사전 조건

사용자 지정 도메인을 설정하기 전에 다음이 있는지 확인합니다.

- Amazon Route53과 같은 DNS 서비스 공급자를 통해 관리하는 도메인 이름입니다.
- WorkSpaces Secure Browser 포털. 포털 생성에 대한 자세한 내용은 섹션을 참조하세요the section called “웹 포털 생성”.
- AWS Certificate Manager, CloudFront 및 DNS 구성을 관리하는 데 필요한 권한이 있는지 확인합니다.

Important

사용자는 적절한 포털 기능을 보장하려면 브라우저에서 사용자 지정 도메인에 대해 타사 쿠키를 활성화해야 합니다.
포털의 보안 및 기능을 유지하려면 사용자 지정 도메인과 DNS 레코드를 소유하고 올바르게 관리해야 합니다.

Note

사용자 지정 도메인에 대해 Single Sign-On 확장을 활성화하려면 사용자가 1.0.2505.6608 이상의 버전으로 브라우저에 확장을 설치해야 합니다.
사용자는 포털에 로그인할 때 확장 프로그램을 설치하라는 메시지를 받게 됩니다. 확장 프로그램의 사용자 경험에 대한 자세한 내용은 the section called “Single Sign-On 확장 프로그램” 섹션을 참조하십시오.

시작하기

새 포털을 생성하거나 기존 포털을 편집할 때 사용자 지정 도메인을 포털 설정 속성으로 구성할 수 있습니다. 콘솔 AWS , SDK, CloudFormation 또는 AWS CLI 명령을 사용하여이 작업을 수행할 수 있습니다.

Amazon CloudFront 배포를 사용자 지정 도메인에서 WorkSpaces Secure Browser 포털 엔드포인트로 트래픽을 라우팅하는 역방향 프록시로 설정하는 것이 좋습니다.

> **Note**
>
> Amazon CloudFront가 역방향 프록시 솔루션으로 권장되지만 대체 역방향 프록시 구성을 사용할 수 있습니다. Amazon CloudFront 설정 단계에 설명된 대로 필요한 오리진 및 캐시 구성 설정을 충족하는지 확인합니다.

CloudFront를 역방향 프록시로 설정

역방향 프록시 설정을 완료하려면 다음이 필요합니다.

- 를 통한 SSL 인증서 AWS Certificate Manager (ACM)
- Amazon CloudFront 배포
- DNS 레코드
- 사용자 지정 도메인으로 구성된 포털

SSL 인증서

아직 없는 경우 다음 단계에 따라 ACM을 통해 요청합니다.

1. 에서 ACM 콘솔로 이동합니다https://console.aws.amazon.com/acm.

   > **Important**
   >
   > CloudFront에서 인증서를 저장해야 하므로 미국 동부(버지니아 북부) 리전을 사용합니다.

2. 인증서 요청:

   - 새 ACM 사용자의 경우: 인증서 프로비저닝에서 시작하기를 선택합니다.
   - 기존 ACM 사용자의 경우: 인증서 요청을 선택합니다.

3. 퍼블릭 인증서 요청을 선택한 다음 인증서 요청을 선택합니다.

> **Note**
>
> 기존 인증서를 가져올 수도 있습니다. 자세한 내용은 ACM 사용 설명서의 ACM으로 인증서 가져오기를 참조하세요.

4. 기본 도메인 이름(예: **myportal.example.com**)을 입력합니다.
5. 검증 방법을 선택합니다.
   - DNS 검증(Route 53 사용자에게 권장) - 호스팅 영역에서 자동 레코드 세트 생성을 허용합니다. 자세한 내용은 ACM 사용 설명서의 DNS 검증을 참조하세요.
   - 이메일 검증 - 자세한 내용은 ACM 사용 설명서의 이메일 검증을 참조하세요.
6. 설정을 검토하고 확인 및 요청을 선택합니다.

CloudFront 배포

CloudFront 배포를 생성하여 사용자 지정 도메인의 요청을 포털 엔드포인트로 프록시합니다.

1. 에서 CloudFront 콘솔로 이동합니다https://console.aws.amazon.com/cloudfront.
2. 배포 생성(Create Distribution)을 선택합니다.
   - 배포 이름: 배포의 이름을 입력합니다.
   - 배포 유형: 단일 웹 사이트 또는 앱

> **Note**
>
> 사용자 지정 도메인이 동일한 AWS 계정의 Route 53에서 관리되는 경우 CloudFront에서 자동으로 DNS를 관리할 수 있습니다. 사용자 지정 도메인을 입력하고 “도메인 확인”을 클릭합니다. 다른 DNS 공급자의 도메인이 있는 경우이 단계를 건너뛰고 나중에 도메인을 구성합니다.

3. 오리진 설정을 구성합니다.
   - 오리진 유형: 기타
   - 사용자 지정 오리진: 포털 엔드포인트 *<portalId>*.workspaces-web.com 입력합니다.
   - 오리진 경로: 비워 둡니다(기본값).

4. 오리진 설정 사용자 지정:

   - 사용자 지정 헤더 추가

     > **Important**
     >
     > 사용자 지정 도메인을 통한 포털 액세스는이 헤더가 프록시 요청에 있는 경우에만 작동합니다. 헤더 이름과 값이 언급된 대로 정확히 지정되었는지 확인합니다.

     - 헤더 이름: workspacessecurebrowser-custom-domain
     - 값: 사용자 지정 도메인(예: **`myportal.example.com`**)
   - 프로토콜: HTTPS 전용
   - HTTPS 포트: 443(기본값 유지)
   - 최소 원래 SSL 프로토콜: TLSv1.2(기본값)
   - 오리진 IP 주소 유형: IPv4 전용(Amazon WorkSpaces Secure Browser는이 관리 안내서 작성 시 IPv6를 지원하지 않습니다.)
5. 캐시 설정 사용자 지정:

   - 최종 사용자 프로토콜 정책: HTTP를 HTTPS로 리디렉션
   - 허용된 HTTP 메서드: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - 캐시 정책: CachingDisabled
   - 오리진 요청 정책: AllViewerExceptHostHeader

     > **Important**
     >
     > 사용자 지정 도메인을 통한 포털 액세스는 오리진 요청 정책이 AllViewerExceptHostHeader로 설정된 경우에만 작동합니다. 이름에서 알 수 있듯이이 정책은 요청 헤더에서 호스트 헤더만 필터링하고 나머지 모든 헤더를 오리진으로 전달합니다.
6. 원하는 경우 WAF를 구성할 수 있지만이 설정을 위해 필요하지는 않습니다.
7. TLS 인증서 가져오기에서 1단계에서 생성한 TLS 인증서를 선택합니다.
8. 설정을 검토하고 배포 생성을 선택합니다.

DNS 레코드

호스팅 영역이 동일한 AWS 계정에 있는 경우 Cloudfront는 Route 53의 DNS 레코드를 업데이트하여 지정된 도메인에서 2단계에서 생성된 배포로 트래픽을 라우팅할 수 있습니다.

1. CloudFront 설정으로 이동
2. “도메인을 CloudFront로 라우팅”을 클릭합니다.
3. "라우팅 자동 설정"을 클릭합니다.

다른 서비스 공급자 또는 다른 AWS 계정에서 사용자 지정 도메인에 대한 DNS를 구성한 경우 도메인의 트래픽을 배포로 라우팅하도록 DNS 공급자를 구성합니다. 다음 단계에서는 Route 53을 사용하여 이를 수행하는 방법을 설명합니다.

1. 에서 Amazon Route 53 콘솔을 엽니다https://console.aws.amazon.com/route53.
2. 액세스 DNS 관리:
   - 이 AWS 계정에서 Route 53를 처음 사용하는 경우 Amazon Route 53 개요 페이지가 열립니다. DNS 관리에서 지금 시작하기를 선택합니다.
   - 이 AWS 계정으로 이전에 Route 53를 사용한 경우 다음 단계로 진행합니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 호스팅 영역이 아직 없는 경우 호스팅 영역을 생성합니다.
   - 인터넷 트래픽을 리소스로 라우팅하려면 Amazon Route 53 개발자 안내서의 퍼블릭 호스팅 영역 생성을 참조하세요.
   - VPC에서 트래픽을 라우팅하려면 Amazon Route 53 개발자 안내서의 프라이빗 호스팅 영역 생성을 참조하세요.
5. 호스팅 영역 페이지에서 관리하려는 호스팅 영역의 이름을 선택합니다.
6. [Create Record Set]를 선택합니다.
7. 도메인에 대한 항목을 생성합니다(예: **`myportal.example.com`**).
   - 유형: A – IPv4 주소
   - 별칭]: 예
   - 별칭 대상: CloudFront 배포 URL

   기타 모든 설정은 기본값을 유지합니다.

> **Note**
>
> Route 53을 사용하여 도메인의 DNS를 관리하지 않는 경우 DNS 서비스 공급자를 사용하고 도메인을 가리키는 DNS 항목을 CloudFront 배포의 URL에 추가합니다.

또는 다음 CloudFormation 템플릿을 사용하여 CloudFront 배포를 생성할 수 있습니다.

이 CloudFormation 템플릿은 CloudFront 배포를 자동으로 생성하고, 역방향 프록시 설정을 구성하고, 선택적으로 Route53 DNS 레코드를 생성합니다.

Example workspaces-web-custom-domain-template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'CloudFront Distribution for custom domain configuration with existing AWS
 WorkSpaces Secure Browser Portal'

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'

  CustomDomainName:
    Type: String
    Description: 'Custom domain name for the portal (e.g., myportal.example.com)'
    AllowedPattern: '^([a-zA-Z0-9]?((?!-)([A-Za-z0-9-]*[A-Za-z0-9])\.)+[a-zA-Z0-9]+)$'
    ConstraintDescription: 'Must be a valid domain name'

  CertificateArn:
    Type: String
    Description: 'ARN of the validated SSL certificate in ACM (must be in us-east-1
 region for CloudFront)'
    AllowedPattern: 'arn:aws:acm:us-east-1:[0-9]{12}:certificate/[a-f0-9]{8}-[a-f0-9]
{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}'
    ConstraintDescription: 'Must be a valid ACM certificate ARN in us-east-1 region'

  CreateRoute53Record:
    Type: String
```

```
    Description: 'Create Route53 record for custom domain (requires existing hosted
 zone)'
    Default: 'No'
    AllowedValues:
      - 'Yes'
      - 'No'

  HostedZoneId:
    Type: String
    Description: 'Route53 Hosted Zone ID for the custom domain (required if creating
 Route53 record)'
    Default: ''

Conditions:
  ShouldCreateRoute53Record: !And
    - !Equals [!Ref CreateRoute53Record, 'Yes']
    - !Not [!Equals [!Ref HostedZoneId, '']]

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
 ${CustomDomainName}'
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

        # Origin Configuration
        Origins:
          - Id: WorkSpacesWebOrigin
            DomainName: !Ref PortalEndpoint
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
              - HeaderName: workspacessecurebrowser-custom-domain
```

```
                HeaderValue: !Ref CustomDomainName

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
          MinimumProtocolVersion: TLSv1.2_2021

      Tags:
        - Key: Name
          Value: !Sub '${AWS::StackName}-cloudfront'

  # Route 53 Record (optional - requires hosted zone to exist)
  Route53Record:
    Type: AWS::Route53::RecordSet
    Condition: ShouldCreateRoute53Record
    Properties:
      HostedZoneId: !Ref HostedZoneId
      Name: !Ref CustomDomainName
      Type: A
      AliasTarget:
        DNSName: !GetAtt CloudFrontDistribution.DomainName
        HostedZoneId: Z2FDTNDATAQYW2  # CloudFront Hosted Zone ID
        EvaluateTargetHealth: false
```

```
Outputs:
  PortalEndpoint:
    Description: 'WorkSpaces Web Portal endpoint used as origin'
    Value: !Ref PortalEndpoint
    Export:
      Name: !Sub '${AWS::StackName}-PortalEndpoint'

  CustomDomainEndpoint:
    Description: 'Custom domain endpoint for the portal'
    Value: !Sub 'https://${CustomDomainName}'
    Export:
      Name: !Sub '${AWS::StackName}-CustomDomainEndpoint'

  CloudFrontDistributionId:
    Description: 'CloudFront Distribution ID'
    Value: !Ref CloudFrontDistribution
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDistributionId'

  CloudFrontDomainName:
    Description: 'CloudFront Distribution Domain Name'
    Value: !GetAtt CloudFrontDistribution.DomainName
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDomainName'

  CertificateArn:
    Description: 'SSL Certificate ARN used by CloudFront'
    Value: !Ref CertificateArn
    Export:
      Name: !Sub '${AWS::StackName}-CertificateArn'

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: "Existing Portal Configuration"
        Parameters:
          - PortalEndpoint
      - Label:
          default: "Custom Domain Configuration"
        Parameters:
          - CustomDomainName
          - CertificateArn
          - CreateRoute53Record
```

```
        - HostedZoneId
    ParameterLabels:
      PortalEndpoint:
        default: "Portal Endpoint"
      CustomDomainName:
        default: "Custom Domain Name"
      CertificateArn:
        default: "SSL Certificate ARN"
      CreateRoute53Record:
        default: "Create Route53 Record"
      HostedZoneId:
        default: "Hosted Zone ID"
```

이 템플릿을 사용하려면:

1. 위의 템플릿을 로 저장 `workspaces-web-custom-domain-template.yaml`
2. 특정 파라미터 값과 함께 AWS 콘솔, AWS CLI 또는 AWS SDK를 사용하여 배포
3. 배포 후 아래 4단계에 설명된 대로 사용자 지정 도메인으로 포털을 구성합니다.

포털 구성

AWS 콘솔, UpdatePortal API 또는 update-portal AWS CLI 명령을 사용하여 사용자 지정 도메인을 포털 설정 속성으로 등록합니다.

1. WorkSpaces Secure Browser 콘솔(https://console.aws.amazon.com/workspaces-web/home)을 엽니다.
2. 탐색 창에서 웹 포털을 선택합니다.
3. 구성할 웹 포털을 선택하고 편집을 선택합니다.
4. 포털 설정에서 사용자 지정 도메인을 추가합니다.
5. 포털 구성을 저장합니다.

구성 테스트

구성을 테스트하려면 다음 단계를 따릅니다.

1. 웹 브라우저를 열고 사용자 지정 도메인의 URL(예: **`https://myportal.example.com`**)로 이동합니다.

2. 모든 것이 올바르게 설정된 경우 포털의 로그인 페이지가 표시됩니다.
3. 그런 다음 브라우저에 포털 URL을 입력합니다. IdP에 로그인한 후 사용자 지정 도메인으로 리디렉션되어야 합니다.
4. 마지막으로 IdP에 로그인하고 포털의 애플리케이션 타일을 클릭합니다. 사용자 지정 도메인으로 리디렉션되어야 합니다.

사용자 지정 도메인 문제 해결

사용자가 원격 브라우저 세션에서 사용자 지정 도메인을 통한 포털 액세스에 문제가 있는 경우 다음 문제 해결 단계를 사용하여 일반적인 문제를 식별하고 해결합니다.

주제

- 일반적인 오류 메시지

일반적인 오류 메시지

다음은 사용자 지정 도메인을 설정할 때 발생하는 일반적인 오류 메시지와 해결 방법입니다.

잘못된 CSRF 토큰 오류

이 오류는 Secure Browser가 CloudFront 설정을 통해 요청을 제대로 수신하지 못할 때 발생합니다.

이 문제를 해결하려면:

- CloudFront 배포에서 사용자 지정 오리진 설정을 확인합니다.
- 사용자 지정 헤더의 이름이 사용자 지정 도메인(https:// 또는 쿼리 파라미터 제외)`workspacessecurebrowser-custom-domain`과 정확히 일치하는지 확인합니다.
- 로컬 브라우저에서 캐시를 지웁니다.
- CloudFront에서 캐시를 무효화합니다.

502 잘못된 게이트웨이 오류

이 오류는 일반적으로 캐시 구성 문제를 나타냅니다.

이 문제를 해결하려면:

- CloudFront 배포의 캐시 설정을 확인합니다.

- 캐시 정책이 로 설정되어 있는지 확인합니다`CachingDisabled`.
- 오리진 요청 정책이 로 설정되어 있는지 확인합니다`AllViewerExceptHostHeader`.
- 로컬 브라우저에서 캐시를 지웁니다.
- CloudFront에서 캐시를 무효화합니다.

액세스 거부 오류

사용자 지정 도메인이 잘못 구성된 경우이 오류가 발생할 수 있습니다.

이 문제를 해결하려면:

- CloudFront 배포의 오리진 설정을 확인합니다.
- 오리진이 올바른 포털 URL로 설정되어 있는지 확인합니다.
- 포털이 올바른 사용자 지정 도메인으로 구성되어 있는지 확인합니다.
- 로컬 브라우저에서 캐시를 지웁니다.
- CloudFront에서 캐시를 무효화합니다.

Amazon WorkSpaces Secure Browser의 보안

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

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

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon WorkSpaces Secure Browser에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 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 목표에 맞게 Amazon WorkSpaces Secure Browser를 구성하는 방법을 보여줍니다. 또한 Amazon WorkSpaces Secure Browser 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

내용

- Amazon WorkSpaces Secure Browser의 데이터 보호
- Amazon WorkSpaces Secure Browser용 Identity and Access Management
- Amazon WorkSpaces Secure Browser의 인시던트 대응
- Amazon WorkSpaces Secure Browser에 대한 규정 준수 확인
- Amazon WorkSpaces Secure Browser의 복원력
- Amazon WorkSpaces Secure Browser의 인프라 보안
- Amazon WorkSpaces Secure Browser의 구성 및 취약성 분석
- 인터페이스 VPC 엔드포인트APIs에 액세스(AWS PrivateLink)
- Amazon WorkSpaces Secure Browser의 보안 모범 사례

Amazon WorkSpaces Secure Browser의 데이터 보호

AWS 공동 책임 모델 Amazon WorkSpaces Secure Browser의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 관한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

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

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 WorkSpaces Secure Browser 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

주제

- Amazon WorkSpaces Secure Browser의 데이터 암호화

- Amazon WorkSpaces Secure Browser의 네트워크 간 트래픽 개인 정보 보호
- Amazon WorkSpaces Secure Browser의 사용자 액세스 로깅

Amazon WorkSpaces Secure Browser의 데이터 암호화

Amazon WorkSpaces Secure Browser는 브라우저 설정, 사용자 설정, 네트워크 설정, ID 제공업체 정보, 트러스트 스토어 데이터, 트러스트 스토어 인증서 데이터와 같은 포털 사용자 지정 데이터를 수집합니다. 또한 WorkSpaces Secure Browser는 브라우저 정책 데이터, 사용자 기본 설정(브라우저 설정용), 세션 로그도 수집합니다. 수집된 데이터는 Amazon DynamoDB 및 Amazon S3에 저장됩니다. WorkSpaces Secure Browser는 암호화 AWS Key Management Service 에를 사용합니다.

콘텐츠를 보호하려면 다음 지침을 따릅니다.

- 최소 권한 액세스를 구현하고 WorkSpaces Secure Browser 작업에 사용할 특정 역할을 생성합니다. IAM 템플릿을 사용하여 전체 액세스 역할 또는 읽기 전용 역할을 생성합니다. 자세한 내용은 AWS WorkSpaces Secure Browser에 대한 관리형 정책 단원을 참조하십시오.
- 제공된 키로 WorkSpaces Secure Browser가 저장 데이터를 암호화할 수 있도록 고객 관리형 키를 제공하여 데이터를 처음부터 끝까지 보호합니다.
- 포털 도메인과 사용자 보안 인증 정보를 공유할 때는 주의해야 합니다.
  - 관리자는 Amazon WorkSpaces 콘솔에 로그인해야 하고, 사용자는 WorkSpaces Secure Browser 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 암호화하여 콘텐츠와 메타데이터를 보호합니다 AWS KMS. 또한 브라우저 정책 및 사용자 기본 설정을 수집하여 WorkSpaces Secure Browser 세션 중에 정책과 설정을 적용합니다. 기존 설정을 적용하는 중 오류가 발생하는 경우 사용자는 새 세션에 액세스할 수 없으며 회사 내부 사이트 및 SaaS 애플리케이션에도 액세스할 수 없습니다.

Amazon WorkSpaces Secure Browser의 저장 중 암호화

유휴 시 암호화는 기본적으로 구성되며 WorkSpaces Secure Browser에 사용되는 모든 고객 데이터(예: 브라우저 정책 설명, 사용자 이름, 로깅 또는 IP 주소)는를 사용하여 암호화됩니다 AWS KMS. 기본적으로 WorkSpaces Secure Browser는 AWS소유 키를 사용하여 암호화를 활성화합니다. 리소스 생

성 시 고객 관리형 키(CMK)를 지정하여 CMK를 사용할 수도 있습니다. 이 기능은 현재 CLI를 통해서만 지원됩니다.

CMK를 전달하기로 선택한 경우 제공된 키는 대칭 암호화 AWS KMS 키여야 하며 관리자로서 다음 권한이 있어야 합니다.

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

CMK를 사용하는 경우 키에 액세스할 수 있도록 WorkSpaces Secure Browser 외부 서비스 보안 주체를 허용 목록에 추가해야 합니다.
자세한 내용은 aws:SourceAccount가 포함된 범위 지정 CMK 키 정책 예시를 참조하세요.

가능하면 WorkSpaces Secure Browser는 전달 액세스 세션(FAS) 자격 증명을 사용하여 키에 액세스합니다. FAS에 대한 자세한 내용은 전달 액세스 세션을 참조하세요.
WorkSpaces Secure Browser에서 비동기적으로 키에 액세스해야 하는 경우가 있습니다. 키 정책에서 WorkSpaces Secure Browser 외부 서비스 보안 주체를 허용 목록에 추가하면 WorkSpaces Secure Browser는 키를 사용하여 허용 목록의 암호화 작업 세트를 수행할 수 있습니다.

리소스가 생성된 후에는 키를 더 이상 제거하거나 변경할 수 없습니다. CMK를 사용한 경우 리소스에 액세스하는 관리자에게는 다음 권한이 있어야 합니다.

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

콘솔을 사용할 때 액세스 거부됨 오류가 표시되면 사용 중인 키의 CMK를 사용하는 데 필요한 권한이 콘솔에 액세스하는 사용자에게 없는 것일 수 있습니다.

WorkSpaces Secure Browser의 키 정책 및 범위 지정 예시

CMK에는 다음과 같은 키 정책이 필요합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      }
    ]
}
```

WorkSpaces Secure Browser에는 다음 권한이 필요합니다.

- `kms:DescribeKey` - 제공된 AWS KMS 키가 올바르게 구성되었는지 확인합니다.
- `kms:GenerateDataKeyWithoutPlaintext` 및 `kms:GenerateDataKey`- 객체를 암호화하는 데 사용되는 데이터 키를 생성하도록 AWS KMS 키를 요청합니다.
- `kms:Decrypt` - 암호화된 데이터 AWS KMS 키를 해독하도록 키를 요청합니다. 이러한 데이터 키는 데이터를 암호화하는 데 사용됩니다.
- `kms:ReEncryptTo` 및 `kms:ReEncryptFrom`- KMS AWS KMS 키에서 또는 KMS 키로의 재암호화를 허용하는 키를 요청합니다.

AWS KMS 키에 대한 WorkSpaces Secure Browser 권한 범위 지정

키 정책 문의 보안 주체가 AWS 서비스 보안 주체인 경우, 암호화 컨텍스트 외에 aws:SourceArn 또는 aws:SourceAccount 전역 조건 키를 사용하는 것이 좋습니다.

리소스에 사용되는 암호화 컨텍스트에는 항상 `aws:workspaces-web:RESOURCE_TYPE:id` 형식의 항목과 해당 리소스 ID가 포함됩니다.

소스 ARN 및 소스 계정 값은 요청이 다른 AWS 서비스 AWS KMS 에서 로 오는 경우에만 권한 부여 컨텍스트에 포함됩니다. 이러한 조건 조합은 최소 권한을 구현하고 잠재적 혼동된 대리자 시나리오를 방지합니다. 자세한 내용은 키 정책의 AWS 서비스에 대한 권한을 참조하세요.

```
   "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "AccountId",
          "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
          ]
        },
      }
```

> **Note**
>
> 리소스 생성 전에는 전체 리소스 ARN이 아직 존재하지 않으므로 키 정책에는 `aws:SourceAccount` 조건만 사용해야 합니다. 리소스 생성 후에는 `aws:SourceArn` 및 `kms:EncryptionContext` 조건을 포함하도록 키 정책을 업데이트할 수 있습니다.

`aws:SourceAccount`가 포함된 범위 지정 CMK 키 정책 예시

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

aws:SourceArn 및 리소스 와일드카드가 포함된 범위 지정 CMK 키 정책 예시

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
```

```
}
```

`aws:SourceArn`이 포함된 범위 지정 CMK 키 정책 예시

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> 리소스를 생성한 후 해당 리소스에 대한 와일드카드를 SourceArn에서 업데이트할 수 있습니다. WorkSpaces Secure Browser를 사용하여 CMK 액세스가 필요한 새 리소스를 생성하는 경우 그에 따라 키 정책도 업데이트해야 합니다.

aws:SourceArn 및 리소스 와일드카드 **EncryptionContext**가 포함된 범위 지정 CMK 키 정책 예시

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
```

```
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
"<userSetttingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
"<browserSettingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
```

```
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
 "<ipAccessSettingsId>"
         }
      }
    },
  ]
}
```

> **Note**
>
> 동일한 키 정책에 특정 리소스별 `EncryptionContext`가 포함된 경우 별도의 문을 생성해야 합니다. 자세한 내용은 kms:EncryptionContext:context-key 아래의 여러 암호화 컨텍스트 페어 사용 단원을 참조하세요.

Amazon WorkSpaces Secure Browser의 전송 중 암호화

WorkSpaces Secure Browser는 HTTPS 및 TLS 1.2를 통해 전송 중 데이터를 암호화합니다. 콘솔이나 API 직접 호출을 사용하여 WorkSpaces에 요청을 보낼 수 있습니다. 전송 중인 요청 데이터는 HTTPS 또는 TLS 연결을 통해 모든 데이터를 전송하여 암호화됩니다. 요청 데이터는 AWS 콘솔 AWS Command Line Interface또는 AWS SDK에서 WorkSpaces Secure Browser로 전송할 수 있습니다.

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

Amazon WorkSpaces Secure Browser의 키 관리

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

Amazon WorkSpaces Secure Browser의 네트워크 간 트래픽 개인 정보 보호

WorkSpaces Secure Browser와 온프레미스 애플리케이션 간의 연결을 보호하려면 WorkSpaces Secure Browser를 사용하여 자체 VPC 내에서 브라우저 세션을 시작해야 합니다. 온프레미스 애플리케이션에 대한 연결은 자체 VPC에서 구성되며 WorkSpaces Secure Browser에서 제어되지 않습니다.

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

Amazon WorkSpaces Secure Browser의 사용자 액세스 로깅

관리자는 시작, 중지, URL 방문을 비롯한 WorkSpaces Secure Browser 세션 이벤트를 기록할 수 있습니다. 이러한 로그는 암호화되어 Amazon Kinesis 데이터 스트림을 통해 고객에게 안전하게 전달됩니다. 사용자 액세스 로깅에서 정보를 검색하는 것은 로깅이 구성되지 않은 세션에 저장 AWS되거나 세션에서 사용할 수 없습니다. 시크릿 모드에서의 URL 방문 또는 브라우저 기록에서 삭제된 URL은 사용자 액세스 로깅에 기록되지 않습니다.

Amazon WorkSpaces Secure Browser용 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 인증(로그인) 및 권한 부여(권한 보유)를 통해 WorkSpaces Secure Browser 리소스를 사용할 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- Amazon WorkSpaces Secure Browser와 IAM의 연동 방식
- Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시
- AWS WorkSpaces Secure Browser에 대한 관리형 정책
- Amazon WorkSpaces Secure Browser ID 및 액세스 문제 해결
- Amazon WorkSpaces Secure Browser에 서비스 연결 역할 사용

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조Amazon WorkSpaces Secure Browser ID 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(Amazon WorkSpaces Secure Browser와 IAM의 연동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

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

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

Amazon WorkSpaces Secure Browser와 IAM의 연동 방식

IAM을 사용하여 WorkSpaces Secure Browser에 대한 액세스를 관리하기 전에 WorkSpaces Secure Browser에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

Amazon WorkSpaces Secure Browser에서 사용할 수 있는 IAM 기능

IAM 특성	WorkSpaces Secure Browser 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACL	아니요
ABAC(정책 내 태그)	부분적
임시 자격 증명	예
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	예

WorkSpaces Secure Browser 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

주제

- WorkSpaces Secure Browser용 ID 기반 정책
- WorkSpaces Secure Browser 내 리소스 기반 정책
- WorkSpaces Secure Browser에 대한 정책 작업
- WorkSpaces Secure Browser에 대한 정책 리소스
- WorkSpaces Secure Browser용 정책 조건 키
- WorkSpaces Secure Browser의 액세스 제어 목록(ACL)
- WorkSpaces Secure Browser의 속성 기반 액세스 제어(ABAC)

- WorkSpaces Secure Browser에서 임시 자격 증명 사용
- WorkSpaces Secure Browser의 교차 서비스 보안 주체 권한
- WorkSpaces Secure Browser의 서비스 역할
- WorkSpaces Secure Browser용 서비스 연결 역할

WorkSpaces Secure Browser용 ID 기반 정책

ID 기반 정책 지원: 예

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

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

WorkSpaces Secure Browser용 ID 기반 정책 예시

WorkSpaces Secure Browser ID 기반 정책의 예시를 보려면 Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시 단원을 참조하세요.

WorkSpaces Secure Browser 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

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

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

WorkSpaces Secure Browser에 대한 정책 작업

정책 작업 지원: 예

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

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

WorkSpaces Secure Browser 작업 목록을 보려면 서비스 권한 부여 참조에서 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하세요.

WorkSpaces Secure Browser의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
workspaces-web
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

WorkSpaces Secure Browser ID 기반 정책의 예시를 보려면 Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시 단원을 참조하세요.

WorkSpaces Secure Browser에 대한 정책 리소스

정책 리소스 지원: 예

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

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

WorkSpaces Secure Browser 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조에서 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하세요.

WorkSpaces Secure Browser ID 기반 정책의 예시를 보려면 Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시 단원을 참조하세요.

WorkSpaces Secure Browser용 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` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

WorkSpaces Secure Browser 조건 키 목록을 보려면 서비스 권한 부여 참조에서 Amazon WorkSpaces Secure Browser에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon WorkSpaces Secure Browser에서 정의한 작업을 참조하세요.

WorkSpaces Secure Browser ID 기반 정책의 예시를 보려면 Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시 단원을 참조하세요.

WorkSpaces Secure Browser의 액세스 제어 목록(ACL)

ACL 지원: 아니요

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

WorkSpaces Secure Browser의 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

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

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

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

WorkSpaces Secure Browser에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

WorkSpaces Secure Browser의 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

WorkSpaces Secure Browser의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 WorkSpaces Secure Browser의 기능이 중단될 수 있습니다. WorkSpaces Secure Browser에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

WorkSpaces Secure Browser용 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

Amazon WorkSpaces Secure Browser용 ID 기반 정책 예시

기본적으로 사용자 및 역할에는 WorkSpaces Secure Browser 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 WorkSpaces Secure Browser에 정의된 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조에서 Amazon WorkSpaces Secure Browser에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

- Amazon WorkSpaces Secure Browser에 대한 ID 기반 정책 모범 사례
- Amazon WorkSpaces Secure Browser 콘솔 사용
- 사용자가 Amazon WorkSpaces Secure Browser에 대한 자신의 권한을 볼 수 있도록 허용

Amazon WorkSpaces Secure Browser에 대한 ID 기반 정책 모범 사례

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

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수

있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

Amazon WorkSpaces Secure Browser 콘솔 사용

Amazon WorkSpaces Secure Browser 콘솔에 액세스하려면 최소한의 권한 세트가 필요합니다. 이러한 권한이 있어야 AWS 계정에서 WorkSpaces Secure Browser 리소스에 대한 세부 정보를 나열하고 볼 수 있습니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

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

사용자와 역할이 여전히 WorkSpaces Secure Browser 콘솔을 사용할 수 있도록 하려면 WorkSpaces Secure Browser `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 Amazon WorkSpaces Secure Browser에 대한 자신의 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

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

AWS WorkSpaces Secure Browser에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 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 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스는 새로운 기능을 지원하기 위해 AWS 관리형 정책에 권한을 추가할 수 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. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한는 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 관리ReadOnlyAccess AWS 형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책: AmazonWorkSpacesWebServiceRolePolicy
- AWS 관리형 정책: AmazonWorkSpacesSecureBrowserReadOnly
- AWS 관리형 정책: AmazonWorkSpacesWebReadOnly
- AWS 관리형 정책에 대한 WorkSpaces Secure Browser 업데이트

AWS 관리형 정책: AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 WorkSpaces Secure Browser에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 the section called “서비스 연결 역할 사용” 단원을 참조하십시오.

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 대한 액세스를 허용합니다.
- `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 내용은 the section called “사용자 활동 로깅 설정” 단원을 참조하십시오.

```
{
    "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 ID에 연결할 수 있습니다.

이 정책은 AWS Management Console, SDK 및 CLI를 통해 WorkSpaces Secure Browser 및 해당 종속 항목에 대한 액세스를 허용하는 읽기 전용 권한을 부여합니다. 인증 유형으로 `IAM_Identity_Center`를 사용하여 포털과 상호 작용하는 데 필요한 권한은 이 정책에 포함되지 않습니다. 이러한 권한을 얻으려면 이 정책을 `AWSSSOReadOnly`와 결합합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `workspaces-web` - AWS Management Console, SDK 및 CLI를 통해 WorkSpaces Secure Browser 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.
- `ec2` - 보안 주체가 VPC, 서브넷, 보안 그룹을 설명하도록 허용합니다. WorkSpaces Secure Browser의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 VPCs, 서브넷 및 보안 그룹을 표시하는 데 사용됩니다.
- `Kinesis` - 보안 주체가 Kinesis 데이터 스트림을 나열할 수 있도록 허용합니다. 이는 WorkSpaces Secure Browser의 AWS 관리 콘솔에서 서비스와 함께 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 ID에 연결할 수 있습니다.

이 정책은 AWS Management Console, SDK 및 CLI를 통해 WorkSpaces Secure Browser 및 해당 종속 항목에 대한 액세스를 허용하는 읽기 전용 권한을 부여합니다. 인증 유형으로 `IAM_Identity_Center`를 사용하여 포털과 상호 작용하는 데 필요한 권한은 이 정책에 포함되지 않습니다. 이러한 권한을 얻으려면 이 정책을 `AWSSSOReadOnly`와 결합합니다.

> **Note**
>
> 현재 이 정책을 사용하고 있는 경우 새 `AmazonWorkSpacesSecureBrowserReadOnly` 정책으로 전환합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `workspaces-web` - AWS Management Console, SDK 및 CLI를 통해 WorkSpaces Secure Browser 및 해당 종속성에 대한 읽기 전용 액세스를 제공합니다.
- `ec2` - 보안 주체가 VPC, 서브넷, 보안 그룹을 설명하도록 허용합니다. WorkSpaces Secure Browser의 AWS 관리 콘솔에서 서비스에 사용할 수 있는 VPCs, 서브넷 및 보안 그룹을 표시하는 데 사용됩니다.

- `Kinesis` - 보안 주체가 Kinesis 데이터 스트림을 나열할 수 있도록 허용합니다. 이는 WorkSpaces Secure Browser의 AWS 관리 콘솔에서 서비스와 함께 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 정책에 대한 WorkSpaces Secure Browser 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 WorkSpaces Secure Browser의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 이력 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AmazonWorkSpacesSecureBrowserReadOnly – 새 정책	WorkSpaces Secure Browser는 AWS Management Console, SDK, CLI를 통해 WorkSpaces Secure Browser 및 해당 종속 요소에 대한 읽기 전용 액세스 권한을 제공하도록 새 정책을 추가했습니다.	2024년 6월 24일
AmazonWorkSpacesWebServiceRolePolicy – 업데이트된 정책	CreateNetworkInterface가 aws:RequestTag/WorkSpacesWebManaged: true로 태그를 지정하고 서브넷 및 보안 그룹 리소스에서 작동하도록 제한하고, DeleteNetworkInterface가 aws:ResourceTag/WorkSpacesWebManaged: true로 태그가 지정된 ENI로 제한하도록 WorkSpaces Secure Browser에서 정책을 업데이트했습니다.	2022년 12월 15일
AmazonWorkSpacesWebReadOnly – 업데이트된 정책	사용자 액세스 로깅 및 Kinesis 데이터 스트림 목록에 대한 읽기 권한을 포함하도록	2022년 11월 2일

변경	설명	Date
	WorkSpaces Secure Browser에서 정책을 업데이트했습니다. 자세한 내용은 the section called “사용자 활동 로깅 설정” 단원을 참조하십시오.	
AmazonWorkSpacesWebServiceRolePolicy – 업데이트된 정책	Kinesis 데이터 스트림의 요약을 설명하고 사용자 액세스 로깅을 위해 Kinesis 데이터 스트림에 레코드를 넣을 수 있도록 WorkSpaces Secure Browser에서 정책을 업데이트했습니다. 자세한 내용은 the section called “사용자 활동 로깅 설정” 단원을 참조하십시오.	2022년 10월 17일
AmazonWorkSpacesWebServiceRolePolicy – 업데이트된 정책	ENI 생성 중에 태그를 생성하도록 WorkSpaces Secure Browser에서 정책을 업데이트했습니다.	2022년 9월 6일
AmazonWorkSpacesWebServiceRolePolicy – 업데이트된 정책	PutMetricData API 권한에 AWS/Usage 네임스페이스를 추가하도록 WorkSpaces Secure Browser에서 정책을 업데이트했습니다.	2022년 4월 6일
AmazonWorkSpacesWebReadOnly – 새 정책	WorkSpaces Secure Browser는 AWS Management Console, SDK, CLI를 통해 WorkSpaces Secure Browser 및 해당 종속 요소에 대한 읽기 전용 액세스 권한을 제공하도록 새 정책을 추가했습니다.	2021년 11월 30일

변경	설명	Date
AmazonWorkSpacesWebServiceRolePolicy – 새 정책	WorkSpaces Secure Browser에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 허용하는 새 정책을 WorkSpaces Secure Browser에서 추가했습니다.	2021년 11월 30일
WorkSpaces Secure Browser, 변경 사항 추적 시작	WorkSpaces Secure Browser가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 11월 30일

Amazon WorkSpaces Secure Browser ID 및 액세스 문제 해결

다음 정보를 사용하여 WorkSpaces Secure Browser 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- WorkSpaces Secure Browser에서 작업을 수행할 권한이 없어요.
- iam:PassRole을 수행하도록 인증되지 않음
- 내 AWS 계정 외부의 사람이 내 WorkSpaces Secure Browser 리소스에 액세스하도록 허용하고 싶습니다.

WorkSpaces Secure Browser에서 작업을 수행할 권한이 없어요.

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `workspaces-web:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
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 `mateojackson` 사용자 정책을 업데이트해야 합니다.

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

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 WorkSpaces Secure Browser에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 WorkSpaces Secure Browser에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
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 사람이 내 WorkSpaces Secure Browser 리소스에 액세스하도록 허용하고 싶습니다.

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

자세한 내용은 다음을 참조하세요.

- WorkSpaces Secure Browser에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon WorkSpaces Secure Browser와 IAM의 연동 방식 단원을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.

- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Amazon WorkSpaces Secure Browser에 서비스 연결 역할 사용

Amazon WorkSpaces Secure Browser는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 WorkSpaces Secure Browser에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 WorkSpaces Secure Browser에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 WorkSpaces Secure Browser를 더 쉽게 설정할 수 있습니다. WorkSpaces Secure Browser에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, WorkSpaces Secure Browser만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 WorkSpaces Secure Browser 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조해 서비스 연결 역할 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

주제

- WorkSpaces Secure Browser용 서비스 연결 역할 권한
- WorkSpaces Secure Browser용 서비스 연결 역할 생성
- WorkSpaces Secure Browser용 서비스 연결 역할 편집
- WorkSpaces Secure Browser용 서비스 연결 역할 삭제
- WorkSpaces Secure Browser 서비스 연결 역할에 지원되는 리전

WorkSpaces Secure Browser용 서비스 연결 역할 권한

WorkSpaces Secure Browser는 `AWSServiceRoleForAmazonWorkSpacesWeb`이라는 서비스 연결 역할을 사용합니다. WorkSpaces Secure Browser는 이 서비스 연결 역할을 통해 고객 계정의 Amazon EC2 리소스에 액세스하여 스트리밍 인스턴스 및 CloudWatch 지표를 제공합니다.

AWSServiceRoleForAmazonWorkSpacesWeb 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- workspaces-web.amazonaws.com

AmazonWorkSpacesWebServiceRolePolicy라는 역할 권한 정책은 WorkSpaces Secure Browser가 지정된 리소스에 대해 다음 작업을 완료하도록 허용합니다. 자세한 내용은 the section called "AmazonWorkSpacesWebServiceRolePolicy" 단원을 참조하십시오.

- 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 resources에 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 연결 역할 권한 섹션을 참조하세요.

WorkSpaces Secure Browser용 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI또는 AWS API에서 첫 번째 포털을 생성하면 WorkSpaces Secure Browser가 서비스 연결 역할을 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 Browser에서 서비스 연결 역할을 다시 생성합니다.

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

WorkSpaces Secure Browser용 서비스 연결 역할 편집

WorkSpaces Secure Browser에서는 `AWSServiceRoleForAmazonWorkSpacesWeb` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

WorkSpaces Secure Browser용 서비스 연결 역할 삭제

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 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 WorkSpaces Secure Browser 서비스에서 해당 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForAmazonWorkSpacesWeb에서 사용하는 WorkSpaces Secure Browser 리소스를 삭제하려면

- 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 다음을 수행하세요.

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

WorkSpaces Secure Browser 서비스 연결 역할에 지원되는 리전

WorkSpaces Secure Browser는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하십시오.

Amazon WorkSpaces Secure Browser의 인시던트 대응

`SessionFailure` Amazon CloudWatch 지표를 모니터링하여 인시던트를 탐지할 수 있습니다. 인시던트 알림을 받으려면 `SessionFailure` 지표에 CloudWatch 경보를 사용합니다. 자세한 내용은 Amazon CloudWatch를 사용한 Amazon WorkSpaces Secure Browser 모니터링 단원을 참조하십시오.

Amazon WorkSpaces Secure Browser에 대한 규정 준수 확인

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 범위 내 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

Amazon WorkSpaces Secure Browser의 복원력

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

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

다음은 현재 WorkSpaces Secure Browser에서 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 WorkSpaces Secure Browser의 인프라 보안

관리형 서비스인 Amazon WorkSpaces Secure Browser는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Amazon WorkSpaces Secure Browser에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.

- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

WorkSpaces Secure Browser는 모든 서비스에 Standard AWS SigV4 인증 및 권한 부여를 적용하여 서비스 트래픽을 격리합니다. 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. 멀티테넌시 및 VPC 엔드포인트(PrivateLink)는 현재 지원되지 않습니다.

Amazon WorkSpaces Secure Browser의 구성 및 취약성 분석

WorkSpaces Secure Browser는 필요에 따라 Chrome 및 Linux를 비롯한 애플리케이션 및 플랫폼을 업데이트하고 패치합니다. 패치하거나 다시 빌드할 필요는 없습니다. 하지만 사양 및 지침에 따라 WorkSpaces Secure Browser를 구성하고 사용자의 WorkSpaces Secure Browser 사용량을 모니터링할 책임은 사용자에게 있습니다. 모든 서비스 관련 구성 및 취약성 분석에 대한 책임은 WorkSpaces Secure Browser에 있습니다.

WorkSpaces Secure Browser용 리소스(예: 웹 포털 수, 사용자 수)에 대한 한도 증가를 요청할 수 있습니다. WorkSpaces Secure Browser는 서비스 및 SLA의 가용성을 보장합니다.

인터페이스 VPC 엔드포인트APIs에 액세스(AWS PrivateLink)

인터넷을 통해 연결하는 대신 프라이빗 클라우드(VPC) 내에서 Amazon WorkSpaces Secure Browser API 엔드포인트를 직접 호출할 수 있습니다. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 Direct Connect 연결을 사용하지 않고도이 작업을 수행할 수 있습니다.

로 구동되는 인터페이스 VPC 엔드포인트를 생성하여이 프라이빗 연결을 설정합니다AWS PrivateLink. VPC에서 지정하는 각 서브넷에 대해 서브넷에 엔드포인트 네트워크 인터페이스를 생성합니다. 엔드포인트 네트워크 인터페이스는 Amazon WorkSpaces Secure Browser API 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

자세한 내용은 를 통한 AWS 서비스 액세스를 AWS PrivateLink 참조하세요.

주제

- Amazon WorkSpaces Secure Browser에 대한 고려 사항

- Amazon WorkSpaces Secure Browser용 인터페이스 VPC 엔드포인트 생성
- 인터페이스 VPC 엔드포인트에 대한 엔드포인트 정책 생성
- 문제 해결

Amazon WorkSpaces Secure Browser에 대한 고려 사항

Amazon WorkSpaces Secure Browser APIs에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에를 통한 액세스 AWS 서비스 AWS PrivateLink에서 "사전 조건"을 검토해야 합니다. Amazon WorkSpaces Secure Browser는 인터페이스 VPC 엔드포인트를 통해 모든 API 작업을 호출할 수 있도록 지원합니다.

기본적으로 엔드포인트를 통해 Amazon WorkSpaces Secure Browser에 대한 전체 액세스가 허용됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

Amazon WorkSpaces Secure Browser용 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 ()를 사용하여 Amazon WorkSpaces Secure Browser 서비스에 대한 인터페이스 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. AWS Command Line Interface 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Amazon WorkSpaces Secure Browser용 인터페이스 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.workspaces-web

FIPS 지원 리전의 경우 다음 서비스 이름을 사용하여 Amazon WorkSpaces Secure Browser용 인터페이스 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.workspaces-web-fips

인터페이스 VPC 엔드포인트에 대한 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 VPC 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 VPC 엔드포인트를 통해 Amazon WorkSpaces Secure Browser APIs에 대한 전체 액세스 권한을 제공합니다. VPC에서 Amazon WorkSpaces Secure Browser에 부여된 액세스를 제어하려면 인터페이스 VPC 엔드포인트에 사용자 지정 엔드포인트 정책을 연결합니다.

엔드포인트 정책은 다음 정보를 지정합니다.

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

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

예: Amazon WorkSpaces Secure Browser 작업에 대한 VPC 엔드포인트 정책

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

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

문제 해결

Amazon WorkSpaces Secure Browser APIs에 대한 호출이 중단되는 경우 VPC 엔드포인트 서비스 보안 그룹 또는 IAM 역할 설정에 잘못된 구성이 있을 수 있습니다. 이 문제를 해결하려면 다음을 시도하세요.

- 인터페이스 VPC 엔드포인트를 생성하는 동안 인터페이스 VPC 엔드포인트가 AWS 계정의 기본 보안 그룹에 자동으로 연결되었을 수 있습니다. 다른 보안 그룹을 사용해 보고 인바운드 및 아웃바운드 권한을 통해 데이터를 적절하게 전송할 수 있는지 확인합니다.
- Amazon WorkSpaces Secure Browser APIs를 호출할 수 있는 IAM 역할을 사용하고 있는지 확인합니다.

자세한 내용은 Amazon VPC 사용 설명서의 What is AWS PrivateLink?를 참조하세요.

Amazon WorkSpaces Secure Browser의 보안 모범 사례

Amazon WorkSpaces Secure Browser는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

Amazon WorkSpaces Secure Browser의 모범 사례는 다음과 같습니다.

- WorkSpaces Secure Browser 사용과 관련된 잠재적 보안 이벤트를 탐지하려면 AWS CloudTrail 또는 Amazon CloudWatch를 사용하여 액세스 기록을 탐지 및 추적하고 로그를 처리합니다. 자세한 내용은 Amazon CloudWatch를 사용한 Amazon WorkSpaces Secure Browser 모니터링 및 를 사용하여 WorkSpaces Secure Browser API 호출 로깅 AWS CloudTrail 단원을 참조하세요.
- 탐지 제어를 구현하고 이상 징후를 식별하려면 CloudTrail 로그 및 CloudWatch 지표를 사용합니다. 자세한 내용은 Amazon CloudWatch를 사용한 Amazon WorkSpaces Secure Browser 모니터링 및 를 사용하여 WorkSpaces Secure Browser API 호출 로깅 AWS CloudTrail 단원을 참조하세요.
- 사용자 액세스 로깅을 설정하여 사용자 이벤트를 기록할 수 있습니다. 자세한 내용은 the section called “사용자 활동 로깅 설정” 단원을 참조하십시오.

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

- 최소 권한 액세스를 구현하고 WorkSpaces Secure Browser 작업에 사용할 특정 역할을 생성합니다. IAM 템플릿을 사용하여 전체 액세스 또는 읽기 전용 역할을 생성합니다. 자세한 내용은 AWS WorkSpaces Secure Browser에 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 Secure Browser 모니터링

모니터링은 Amazon WorkSpaces Secure Browser 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 WorkSpaces Secure Browser 포털 및 리소스를 모니터링하고, 이상이 있을 때 보고하고, 적절한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 AWS 제공합니다.

- Amazon CloudWatch는 AWS 리소스와 AWS 실행 중인 애플리케이션을 실시간으로 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 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 정보는 Amazon CloudWatch 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs로 Amazon EC2 인스턴스, CloudTrail, 기타 소스의 로그 파일을 모니터링, 저장, 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임곗값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.
- AWS CloudTrail는 AWS 계정에 의해 또는 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 호출한 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

주제

- Amazon CloudWatch를 사용한 Amazon WorkSpaces Secure Browser 모니터링
- 를 사용하여 WorkSpaces Secure Browser API 호출 로깅 AWS CloudTrail
- Amazon WorkSpaces Secure Browser의 사용자 활동 로깅

Amazon CloudWatch를 사용한 Amazon WorkSpaces Secure Browser 모니터링

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 CloudWatch를 사용하여 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 임곗값을 주시하다가 해당 임곗값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

AWS/WorkSpacesWeb 네임스페이스에는 다음과 같은 지표가 포함됩니다.

Amazon WorkSpaces Secure Browser의 CloudWatch 지표

지표	설명	Dimensions	Statistics	단위
SessionAttempt	Amazon WorkSpaces Secure Browser 세션 시도 횟수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionSuccess	성공한 Amazon WorkSpaces Secure Browser 세션 시작 횟수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionFailure	실패한 Amazon WorkSpaces Secure Browser 세션 시작 횟수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionIdleDisconnect	사용자 비활성으로 인해 종료된 연결 수입니다.	[PortalId]	평균	개수
ActiveSession	포털의 활성 세션 수입니다.	[PortalId]	평균	개수
GlobalCpuPercent	Amazon WorkSpaces Secure Browser 세션 인스턴스의	[PortalId] [PortalId, UserName]	Average, Sum, Maximum, Minimum	%

지표	설명	Dimensions	Statistics	단위
	CPU 사용량입니다.			
GlobalMemoryPercent	Amazon WorkSpaces Secure Browser 세션 인스턴스의 메모리(RAM) 사용량입니다.	[PortalId] [PortalId, UserName]	Average, Sum, Maximum, Minimum	%
DisplayLatency	프레임 캡처와 프레젠테이션 사이의 평균 밀리초 단위 시간입니다.	[PortalId] [PortalId, UserName]	Average, Maximum, Minimum	밀리초
InputLatency	클라이언트와 서버 간의 입력 지연 시간입니다. 예를 들어 클라이언트 마우스 클릭과 서버 마우스 클릭 사이의 지연 시간입니다.	[PortalId] [PortalId, UserName]	Average, Maximum, Minimum	밀리초
SessionLoggerEventDelivered	전달된 각 세션 로거 파일에 있는 이벤트 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionLoggerTargetNotFoundError	버킷을 찾을 수 없는 로그 파일 전송 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수

지표	설명	Dimensions	Statistics	단위
SessionLoggerAccessDeniedError	권한이 거부된 로그 파일 전송 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수

> **Note**
>
> 지표 데이터 포인트는 각 세션에서 분당 한 번씩 수집되어 5분마다 한 번씩 CloudWatch에 게시됩니다. 세션 로거 지표는 각 로그 파일 전송에 대해 즉시 내보내집니다.

Amazon WorkSpaces Secure Browser 지표의 차원

차원	설명
PortalId	지정된 포털에 대한 Amazon WorkSpaces Secure Browser의 지표 데이터를 필터링합니다.
UserName	지정된 포털 및 사용자에 대한 Amazon WorkSpaces Secure Browser의 지표 데이터를 필터링합니다.

SessionLoggerEventDelivered 지표를 사용하여 포털에서 집계된 이벤트 수를 모니터링하거나 값을 합산하는 대신 데이터 포인트 수를 계산하여 전송된 로그 파일 수를 확인할 수 있습니다. 실수로 인한 리소스 또는 권한 삭제를 감지하려면 SessionLoggerTargetNotFoundError 및 SessionLoggerAccessDeniedError 지표에 대한 경보를 구성하는 것이 좋습니다.

를 사용하여 WorkSpaces Secure Browser API 호출 로깅 AWS CloudTrail

WorkSpaces Secure Browser는 Amazon WorkSpaces Secure Browser에서 사용자, 역할 또는 AWS CloudTrail서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Amazon WorkSpaces Secure Browser에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 여기에

는 Amazon WorkSpaces Secure Browser 콘솔로부터의 직접 호출과 Amazon WorkSpaces Secure Browser API 작업에 대한 코드 직접 호출이 포함됩니다. 추적을 생성하면 Amazon WorkSpaces Secure Browser 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon WorkSpaces Secure Browser에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간, 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- CloudTrail의 WorkSpaces Secure Browser 정보
- WorkSpaces Secure Browser 로그 파일 항목 이해

CloudTrail의 WorkSpaces Secure Browser 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Amazon WorkSpaces Secure Browser에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 이벤트 기록에서 AWS 계정의 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amazon WorkSpaces Secure Browser에 대한 이벤트를 포함하여 AWS 계정의 이벤트를 지속적으로 기록하려면 추적을 생성할 수 있습니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS지역에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Amazon WorkSpaces Secure Browser 작업은 CloudTrail에서 로깅되며 Amazon WorkSpaces API 참조에 설명되어 있습니다. 예를 들어 `CreatePortal`, `DeleteUserSettings`, `ListBrowserSettings` 작업을 직접 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 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 서비스에서 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

WorkSpaces Secure Browser 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 및 기타 세부 사항에 관한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 `ListBrowserSettings` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.


```
{
   "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"
    }]
}
```

Amazon WorkSpaces Secure Browser의 사용자 활동 로깅

Amazon WorkSpaces Secure Browser를 사용하면 고객이 보안 브라우저 세션에서 사용자 활동과 관련된 세션 이벤트를 로깅할 수 있습니다.

WorkSpaces Secure Browser는 사용자 활동 및 보안 관련 이벤트를 로깅하는 두 가지 옵션을 제공합니다.

- 세션 로거는 다양한 세션 이벤트를 캡처합니다. 이러한 로그는 계정의 Amazon S3 버킷으로 전송되므로 선호하는 SIEM 플랫폼과 쉽게 통합할 수 있습니다.
- 사용자 액세스 로깅은 가장 중요한 세션 이벤트를 캡처합니다. 이러한 로그는 실시간 처리 및 분석을 위해 Amazon Kinesis 스트림으로 스트리밍됩니다.

이러한 옵션을 설정하는 방법에 대한 자세한 내용은 the section called “세션 로거 설정” 및 섹션을 참조하세요the section called “사용자 액세스 로깅 설정”.

주제

- Amazon WorkSpaces Secure Browser용 세션 로거의 세션 이벤트
- Amazon WorkSpaces Secure Browser에 대한 사용자 액세스 로깅의 세션 이벤트

Amazon WorkSpaces Secure Browser용 세션 로거의 세션 이벤트

세션 로거는 모니터링 및 감사 목적으로 다양한 세션 관련 이벤트를 캡처합니다.

WorkSpaces Secure Browser 포털의 요구 사항에 따라 모든 세션 이벤트 또는 선택한 하위 집합을 수집하도록 세션 로거를 구성할 수 있습니다. 구성에 대한 자세한 내용은 단원을 참조하십시오the section called “세션 로거 설정”.

사용자 개인 정보를 유지하기 위해 Session Logger는 클립보드 데이터 또는 업로드되거나 다운로드된 파일의 콘텐츠와 같은 민감한 콘텐츠를 기록하지 않습니다.

모든 이벤트에는 다음 필드가 포함됩니다.

- Time
- 사용자 이름
- 포털 ID
- 포털 IP

- 클라이언트 IP
- 세션 ID

명칭	설명	이벤트에 포함된 추가 필드
SessionStart	보안 브라우저 세션이 시작되었지만 사용자가 아직 연결되지 않았습니다.	
SessionConnect	사용자가 보안 브라우저 세션에 연결되어 있습니다.	
TabOpen	보안 브라우저 세션에서 사용자가 새 탭을 열거나 새 탭에서 링크를 열었습니다.	호스트 이름, 경로, URL(사용자가 새 탭에서 링크를 여는 경우), 없음(사용자가 새 탭을 여는 경우)
UrlVisit	브라우저 세션에서 사용자는 URL로 이동했습니다.	호스트 이름, 경로, URL
WebsiteInteract	사용자가 웹 사이트에서 표준 HTML 요소를 변경했습니다(예: 확인란, 라디오 버튼 또는 버튼을 클릭하거나 드롭다운에서 항목을 선택).	호스트 이름, 경로, URL
TabClose	브라우저 세션에서 사용자가 탭을 닫았습니다.	호스트 이름, 경로, URL(사용자가 탐색한 탭을 닫는 경우), 없음(사용자가 새 탭을 닫는 경우)
ContentTransferFromLocalToRemoteClipboard	사용자가 로컬 브라우저의 콘텐츠를 사용하여 보안 브라우저 내에서 클립보드를 업데이트했습니다(보안 환경 외부). 이 업데이트는 세션 내 도구 모음을 통해 콘텐츠를 복사하거	

명칭	설명	이벤트에 포함된 추가 필드
	나 키보드 바로 가기(Ctrl+C / Ctrl+V)를 통해 데이터를 전송하여 발생할 수 있습니다.	
ContentCopyFromWebsite	사용자가 보안 브라우저(보안 환경 내부)의 콘텐츠를 사용하여 보안 브라우저 내에서 클립보드를 업데이트했습니다.	호스트 이름, 경로, URL
ContentPasteToWebsite	클립보드 콘텐츠가 브라우저 내의 웹 페이지에 붙여넣어졌습니다. (이 이벤트는 클립보드 콘텐츠가 브라우저의 URL 표시줄에 붙여넣는 인스턴스를 캡처하지 않습니다.)	호스트 이름, 경로, URL
PrintJobSubmit	사용자가 브라우저의 가상 프린터(“DCV 프린터”)에 요청 작업을 제출했습니다. 콘텐츠는 사용자의 로컬 시스템에 PDF로 저장됩니다.	파일 이름, 크기, 확장명
FileDownloadFromSecureBrowserToRemoteDisk	세션에서 원격 인스턴스의 로컬 디스크로 파일이 저장되었습니다.	호스트 이름, 경로, URLfilename, 크기, 확장
FileTransferFromRemoteToLocalDisk	원격 인스턴스의 디스크에서 사용자의 로컬 디바이스로 파일이 다운로드되었습니다.	파일 이름, 크기, 확장명
FileUploadFromRemoteDiskToSecureBrowser	원격 인스턴스의 로컬 디스크에 저장된 파일이 브라우저 세션을 통해 파일 공유 SaaS 플랫폼(예: Google Drive, Box 또는 File.io)에 업로드되었습니다.	

명칭	설명	이벤트에 포함된 추가 필드
FileTransferFromLocalToRemoteDisk	파일이 사용자 디바이스에서 보안 브라우저 세션으로 업로드되었습니다.	파일 이름, 크기 및 확장명
SessionDisconnection	사용자가 보안 브라우저 세션에서 연결 해제되었습니다.	
SessionEnd	보안 브라우저 세션이 종료되었습니다. 종료는 관리자가 콘솔의 사용자 세션 관리자를 통해 세션을 종료하거나, 사용자가 도구 모음의 세션 종료를 사용하여 세션을 수동으로 종료하거나, 관리자가 설정한 기간을 초과한 후 세션 시간이 초과되는 세 가지 방법 중 하나로 발생할 수 있습니다.	

각 이벤트는 OCSF 표준을 따르며 모든 이벤트에 공통적인 속성 목록을 포함합니다.

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
    activity_id : Integer | OCSF standard value 99 for 'others'
    category_name : "WorkSpacesSecureBrowser" | The category name where the event
 belongs to.
    category_id : 2 | Numerical identifier for category,
    metadata : link | Required {
        product : link {
            vendor_name : "wsb",
            name : "WorkSpacesSecureBrowser"
        }
        version : String | Version of the schema | eg. 1.0.0
    },
    severity_id : 1 | The severity of the event. All events will have a severity of 1,
 meaning 'Informational',
    type_id : class_uid * 100 + activity_id
```

```
    time : The time the event happened (RFC3339 format),
    observables : link [
        {
            name : "session_detail.portal_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.session_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.client_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.portal_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.username",
            type_id : 10 //Resource UID
            value : //Generated value
        }
    ],

    // New Events
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
        username : String | The logged-in username | eg. bobross
    }
}
```

다음은 URLVisit 이벤트의 예입니다.

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

다음은 PrintJobSubmit 이벤트의 예입니다.

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
```

```
}
```

Amazon WorkSpaces Secure Browser에 대한 세션 로거 지표

세션 로거는 다음 Amazon CloudWatch 지표를 내보냅니다.

SessionLoggerEventDelivered 지표를 사용하여 포털에서 집계된 이벤트 수를 모니터링하거나 값을 합산하는 대신 데이터 포인트 수를 계산하여 전송된 로그 파일 수를 확인할 수 있습니다. 실수로 인한 리소스 또는 권한 삭제를 감지하려면 SessionLoggerTargetNotFoundError 및 SessionLoggerAccessDeniedError 지표에 대한 경보를 구성하는 것이 좋습니다.

> **Note**
>
> 지표 데이터 포인트는 각 세션에서 분당 한 번씩 수집되고 5분마다 Amazon CloudWatch 한 번씩에 게시됩니다. 세션 로거 지표는 각 로그 파일 전송에 대해 즉시 내보내집니다.

세션 로거 지표

지표	설명	차원	Statistics	단위
SessionLoggerEventDelivered	전달된 각 세션 로거 파일에 있는 이벤트 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionLoggerTargetNotFoundError	버킷을 찾을 수 없는 로그 파일 전송 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수
SessionLoggerAccessDeniedError	권한이 거부된 로그 파일 전송 수입니다.	[PortalId]	Average, Sum, Maximum, Minimum	개수

Amazon WorkSpaces Secure Browser에 대한 사용자 액세스 로깅의 세션 이벤트

사용자 액세스 로깅에 사용할 수 있는 세션 이벤트는 다음과 같습니다.

- 검증: 이벤트가 Kinesis 데이터 스트림에 성공적으로 배치되었습니다.
- StartSession: 사용자가 세션을 시작했으며 보안 브라우저 세션에 연결되어 있습니다.
- VisitPage: 사용자가 세션의 페이지를 방문하고 있습니다.
- EndSession: 사용자가 세션을 종료했습니다.

URL 탐색 로그는 브라우저 기록에서 기록됩니다. 브라우저 기록에 기록되지 않은 URLs(인식 불가 모드에서 방문하거나 브라우저 기록에서 삭제됨)은 로그에 기록되지 않습니다. 브라우저 정책을 사용하여 비인식 모드 또는 기록 삭제를 해제할지 여부를 결정하는 것은 고객의 몫입니다.

다음은 사용 가능한 각 이벤트의 예입니다. 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"
}
```

Amazon WorkSpaces Secure Browser 사용자를 위한 지침

관리자는 WorkSpaces Secure Browser를 사용하여 내부 웹 사이트, 서비스형 소프트웨어(SAAS) 웹 애플리케이션 또는 인터넷과 같은 회사 웹 사이트에 연결하는 웹 포털을 생성합니다. 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 사용자에게 도움이 됩니다.

주제

- Amazon WorkSpaces Secure Browser의 브라우저 및 디바이스 호환성
- Amazon WorkSpaces Secure Browser용 웹 포털 액세스
- Amazon WorkSpaces Secure Browser에 대한 세션 지침
- Amazon WorkSpaces Secure Browser의 사용자 문제 해결
- Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램

Amazon WorkSpaces Secure Browser의 브라우저 및 디바이스 호환성

Amazon WorkSpaces Secure Browser는 웹 브라우저 내에서 실행되는 Amazon DCV 웹 브라우저 클라이언트를 통해 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 최신 세부 정보는 Web browser client(웹 브라우저 클라이언트)를 참조하십시오.

> **Note**
>
> 웹캠은 현재 Google Chrome 및 Microsoft Edge와 같은 Chromium 기반 브라우저에서만 지원됩니다. 현재 Apple Safari 및 Mozilla FireFox는 웹캠을 지원하지 않습니다.

Amazon WorkSpaces Secure Browser용 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.

Amazon WorkSpaces Secure Browser에 대한 세션 지침

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

주제

- Amazon WorkSpaces Secure Browser에서 세션 시작
- Amazon WorkSpaces Secure Browser에서 도구 모음 사용
- Amazon WorkSpaces Secure Browser에서 브라우저 사용
- Amazon WorkSpaces Secure Browser에서 세션 종료

Amazon WorkSpaces Secure Browser에서 세션 시작

로그인하여 세션을 시작하면 세션 실행 중 메시지와 진행률 표시줄이 표시됩니다. 이는 Amazon WorkSpaces Secure Browser에서 사용자를 위한 세션을 생성하고 있음을 나타냅니다. Amazon WorkSpaces Secure Browser은 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 팝업 항상 허용으로 설정하여 Amazon WorkSpaces Secure Browser에서 추가 모니터 창을 실행할 수 있도록 설정합니다.

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

Amazon WorkSpaces Secure Browser에서 도구 모음 사용

도구 모음 사용법에 대해 알아보려면 다음 단계를 따릅니다.

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

도구 모음을 축소하려면 도구 모음 위에 커서를 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 디바이스를 확대하거나 축소하려면 다음 단계를 따릅니다.

1. 도구 모음 또는 웹 콘텐츠를 선택합니다.
2. Ctrl + +를 눌러 확대하거나 Ctrl + -를 눌러 축소합니다.

Mac 디바이스를 확대하거나 축소하려면 다음 단계를 따릅니다.

1. 도구 모음 또는 웹 콘텐츠를 선택합니다.
2. Cmd + +를 눌러 확대하거나 Cmd + -를 눌러 축소합니다.

도구 모음을 화면 상단에 고정하려면 도구 모음 모드에서 기본 설정, 일반, 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. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**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.

Amazon WorkSpaces Secure Browser에서 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.

Amazon WorkSpaces Secure Browser에서 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.

Amazon WorkSpaces Secure Browser의 사용자 문제 해결

WorkSpaces Secure Browser 사용 중에 다음과 같은 문제가 발생하면 다음 해결 방법을 시도해 보세요.

Amazon WorkSpaces Secure Browser 포털에 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 모

음에서 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.

어떤 마이크 및/또는 웹캠이 사용되고 있는지 어떻게 알 수 있으며 어떻게 변경할 수 있습니까?

마이크 또는 카메라 옆에 있는 아래쪽 화살표 아이콘을 클릭합니다. 메뉴에는 현재 디바이스를 나타내는 확인 표시와 함께 사용 가능한 디바이스가 표시됩니다. 다른 디바이스를 선택하여 세션에 사용할 디바이스를 변경합니다.

회사의 사용자 지정 도메인에서 직접 액세스하면 웹 포털이 시작되지 않습니다.

와 같은 비 workspaces-web.com 도메인 이름을 사용하여 세션을 시작하려는 경우 브라우저에 액세스 중인 회사 도메인에 대해 타사 쿠키가 활성화되어 있는지 `acme.secureportal.mycompany.com`확인합니다.

Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램

Amazon WorkSpaces Secure Browser는 데스크톱 컴퓨터의 Chrome 및 Firefox 브라우저에서 Single Sign-On을 위한 확장 기능을 제공합니다. 관리자가 확장 프로그램을 활성화한 경우 로그인할 때 웹 포털에서 확장 프로그램을 설치하라는 메시지를 표시합니다.

Amazon WorkSpaces Secure Browser는 세션 중에 웹사이트에 Single Sign-On할 수 있도록 확장 기능을 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.

주제

- Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 호환성
- Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 설치
- Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 문제 해결

Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 호환성

Single Sign-On 확장 프로그램은 다음 디바이스 및 브라우저에서 작동합니다.

- Devices
  - 랩톱
  - 데스크톱
- 브라우저
  - Google Chrome
  - Mozilla Firefox

Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 설치

Single Sign-On 확장 프로그램을 설치하려면 다음 단계를 따릅니다.

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 작동하게 하려면 시크릿 모드(Chrome) 또는 사생활 보호 모드(Firefox) 대신 일반 브라우징 창에서 확장 프로그램을 사용합니다.

Amazon WorkSpaces Secure Browser용 Single Sign-On 확장 프로그램 문제 해결

Single Sign-On 확장 프로그램을 사용하는 동안 다음과 같은 문제가 발생할 수 있습니다.

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

1. 브라우저에 Amazon WorkSpaces Secure Browser 확장 프로그램이 설치되어 있는지 확인합니다. 브라우저 데이터를 삭제한 경우 확장 프로그램이 실수로 제거되었을 수 있습니다.
2. 시크릿 모드(Chrome)나 사생활 보호 모드(Firefox)가 아닌지 확인합니다. 이러한 모드는 확장 프로그램에 문제를 일으킬 수 있습니다.
3. 문제가 지속되면 포털 관리자에게 문의하여 추가 지원을 받으십시오.

Amazon WorkSpaces Secure Browser 관리 안내서의 문서 기록

다음 표에서는 Amazon WorkSpaces Secure Browser 릴리스 관련 문서를 소개합니다.

변경 사항	설명	날짜
세션 로거	다양한 세션 이벤트를 캡처하도록 세션 로거를 설정합니다.	2025년 8월 1일
CloudWatch 지표	CloudWatch 지표를 업데이트했습니다.	2025년 7월 21일
도구 모음 제어	도구 모음 컨트롤을 사용하면 최종 사용자 세션에 대한 도구 모음 프레젠테이션을 구성할 수 있습니다.	2025년 2월 21일
인터페이스 VPC 엔드포인트 APIs에 액세스(AWS PrivateLink)	인터넷을 통해 연결하는 대신 프라이빗 클라우드(VPC) 내에서 Amazon WorkSpaces Secure Browser API 엔드포인트를 직접 호출합니다.	2025년 1월 10일
데이터 보호 설정	데이터 보호 설정을 추가하여 세션 중에 데이터가 공유되지 않도록 보호합니다.	2024년 11월 20일
FIPS 엔드포인트	FIPS 엔드포인트로 전송 중 데이터 보호	2024년 10월 7일
세션 관리 대시보드	세션 관리 대시보드를 사용하여 활성 세션과 완료된 세션을 모니터링하고 관리할 수 있습니다.	2024년 9월 19일
딥 링크 허용	세션 중에 사용자를 특정 웹 사이트에 연결하는 딥 링크를 포	2024년 6월 25일

	털에서 수신하도록 허용합니다.	
관리형 정책 업데이트	AmazonWorkSpacesSecureBrowserReadOnly 관리형 정책 추가	2024년 6월 24일
도구 모음을 사용하여 확대/축소	도구 모음을 사용하여 디스플레이, 아이콘 및 텍스트의 크기를 늘릴 수 있습니다.	2024년 5월 1일
새 웹 포털 설정	이제 웹 포털의 인스턴스 유형과 최대 동시 사용자 한도를 지정할 수 있습니다.	2024년 4월 22일
CloudWatch 지표	GlobalCpuPercent 및 GlobalMemoryPercent 지표가 추가되었습니다.	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 Identity Center 인증 유형 중에서 선택할 수 있습니다.	2024년 2월 5일
Single Sign-On용 확장 프로그램 활성화	최종 사용자가 더 나은 포털 로그인을 경험할 수 있도록 확장 프로그램을 활성화할 수 있습니다.	2023년 8월 28일
Amazon WorkSpaces Secure Browser 사용자 지침	Amazon WorkSpaces Secure Browser 액세스, 세션 시작 및 구성, 도구 모음 및 웹 브라우저 사용에 대해 자세히 알아보려는 최종 사용자에게 도움이 되는 콘텐츠를 추가했습니다.	2023년 7월 17일

IP 액세스 제어	WorkSpaces Secure Browser를 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 Secure Browser는 표준 및 AWS IAM Identity Center라는 두 가지 인증 유형을 제공합니다.	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	PutMetricData API 권한에 AWS/Usage 네임스페이스를 추가하도록 업데이트된 AmazonWorkSpacesWebServiceRolePolicy 관리형 정책	2022년 4월 6일
서비스 연결 역할	새 AWSServiceRoleForAmazonWorkSpacesWeb 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 Secure Browser 관리 안내서의 최초 릴리스	2021년 11월 30일

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