aws

시작 안내서

AWS Management Console

버전 1.0

AWS Management Console: 시작 안내서

Table of Contents

란 무엇입니까 AWS Management Console?

AWS Management Console는 모든 개별 AWS 서비스 콘솔에 대한 중앙 집중식 액세스를 포함하고 제공하는 웹 기반 애플리케이션입니다. 에서 통합 탐색 AWS Management Console 을 사용하여 서비스를 검색하고, 알림을 보고, AWS CloudShell에 액세스하고, 계정 및 결제 정보에 액세스하고, 일반 콘솔 설정을 사용자 지정할 수 있습니다. 의 홈 페이지가 호출 AWS Management Console 됩니다 AWS Console Home. 에서 AWS 애플리케이션을 관리하고 다른 모든 개별 서비스 콘솔에 액세스할 AWS Console Home수 있습니다. 위젯을 사용하여 AWS 및 리소스에 대한 기타 유용한 정보를 표시 AWS Console Home 하도록를 사용자 지정할 수도 있습니다. 최근에 방문한 서비스, AWS Health 등과 같은 위젯을 추가, 제거 및 재정렬할 수 있습니다.

주제

의 기능 AWS Management Console

의 중요한 기능은 다음과 AWS Management Console 같습니다.

- AWS 서비스 콘솔로 이동 - 통합 탐색을 사용하여 최근에 방문한 서비스 콘솔에 액세스하고, 즐겨찾기 목록에 서비스를 보고 추가하고, 콘솔 설정에 액세스하고, 액세스할 수 있습니다 AWS 사용자 알림.
- AWS 서비스 및 기타 AWS 정보 검색 - 통합 검색을 사용하여 AWS 서비스 및 기능과 AWS 마켓플레이스 제품을 검색합니다.
- 콘솔 사용자 지정 - 통합 설정을 사용하여 AWS Management Console의 다양한 측면을 사용자 지정할 수 있습니다. 여기에는 언어, 기본 리전 등이 포함됩니다.
- CLI 명령 실행 - 콘솔에서 직접 AWS CloudShell 액세스할 수 있습니다. CloudShell을 사용하여 선호하는 서비스에 대해 AWS CLI 명령을 실행할 수 있습니다.
- 모든 AWS 이벤트 알림에 액세스 -를 사용하여 AWS 사용자 알림 및의 알림 AWS Management Console 에 액세스할 수 있습니다 AWS Health.
- 사용자 지정 AWS Console Home - 위젯을 사용하여 AWS Console Home 경험을 완전히 사용자 지정할 수 있습니다.

- AWS 애플리케이션 생성 및 관리 -에서 myApplications를 사용하여 애플리케이션의 비용, 상태, 보안 태세 및 성능을 관리하고 모니터링합니다 AWS Console Home.
- Amazon Q와 채팅 - 콘솔에서 직접 AWS 서비스 질문에 대한 생성형 인공 지능(AI) 어시스턴트 기반 답변을 얻을 수 있습니다. 추가 지원을 위해 라이브 에이전트와 연결할 수도 있습니다.
- 네트워크에서 AWS 계정 액세스 제어 - 트래픽이 네트워크 내에서 시작될 때 AWS Management Console 프라이빗 액세스를 사용하여에 대한 액세스를 지정된 알려진 AWS 계정 집합 AWS Management Console 으로 제한할 수 있습니다.

의 개별 AWS 서비스 콘솔 AWS Management Console

각 AWS 서비스에는 내에서 액세스할 수 있는 고유한 개별 서비스 콘솔이 있습니다 AWS Management Console. 시각적 모드 및 기본 언어 AWS Management Console와 같이에 대한 통합 설정에서 선택한 설정은 모든 개별 AWS 콘솔에 적용됩니다. AWS 서비스 콘솔은 클라우드 컴퓨팅을 위한 다양한 도구와 계정 및 결제에 대한 정보를 제공합니다. Amazon Elastic Compute Cloud와 같은 특정 서비스 및 콘솔에 대해 자세히 알아보려면 AWS Management Console 탐색 모음에서 통합 검색을 사용하여 콘솔로 이동하고 AWS 설명서 웹 사이트에서 Amazon EC2 설명서에 액세스합니다.

개별 AWS 서비스의 콘솔로 이동하더라도 콘솔 상단의 통합 탐색을 AWS Management Console 사용하여의 기능에 계속 액세스할 수 있습니다. 해당 콘솔로 이동해 페이지 바닥글에서 피드백을 선택하여 개별 서비스의 콘솔에 대한 피드백을 남길 수 있습니다.

에 액세스 AWS Management Console

https://console.aws.amazon.com/ AWS Management Console 에 액세스할 수 있습니다.

모바일 디바이스에서 AWS Management Console 액세스

AWS Management Console은 태블릿뿐만 아니라 다른 종류의 모바일 디바이스에서도 작동하도록 설계되었습니다.

- 화면에 더 많은 정보를 표시하도록 가로 및 세로 공간이 최대화되었습니다.
- 더 나은 터치 경험을 위해 버튼과 선택기가 더 커집니다.

모바일 디바이스에서 AWS Management Console에 액세스하려면 AWS Console Mobile Application을 사용해야 합니다. 이 앱은 Android 및 iOS에서 사용할 수 있습니다. Console 모바일 애플리케이션은 전체 웹 경험에서 유용한 모바일 관련 태스크를 제공합니다. 예를 들어 휴대폰에서 기존 Amazon

EC2 인스턴스와 Amazon CloudWatch 경보를 손쉽게 보고 관리할 수 있습니다. 자세한 내용은 AWS Console Mobile Application 사용 설명서의 AWS Console Mobile Application란 무엇입니까?를 참조하세요.

Console 모바일 애플리케이션은 Amazon Appstore, Google Play, iOS App Store에서 다운로드할 수 있습니다.

AWS Management Console에서 서비스 시작하기

AWS Management Console에서는 여러 가지 방법으로 개별 서비스 콘솔로 이동할 수 있습니다.

특정 서비스의 콘솔을 열려면

다음 중 하나를 수행합니다.

- 탐색 모음의 검색 상자에 서비스 이름의 전체 또는 일부를 입력합니다. [서비스(Services)]의 검색 결과 목록에서 원하는 서비스를 선택합니다. 자세한 내용은 에서 통합 검색을 사용하여 제품, 서비스, 기능 등 검색 AWS Management Console 섹션을 참조하세요.
- 최근 방문한 서비스(Recently visited services) 위젯에서 서비스 이름을 선택합니다.
- 최근 방문한 서비스 위젯에서 모든 AWS 서비스 보기를 선택합니다. 그런 다음 모든 AWS 서비스 페이지에서 서비스 이름을 선택합니다.
- 탐색 모음에서 [서비스(Services)]를 선택하여 서비스의 전체 목록을 엽니다. 그런 다음 [최근 방문(Recently visited)] 또는 [모든 서비스(All services)]에서 서비스를 선택합니다.

통합 탐색을 통해 AWS Management Console 탐색 모음 사용

이 주제에서는 통합 탐색을 사용하는 방법을 설명합니다. 통합 탐색은 콘솔의 머리글과 바닥글 역할을 하는 탐색 모음을 나타냅니다. 통합 탐색을 사용하여 다음을 수행할 수 있습니다.

- AWS 서비스, 기능, 제품 등을 검색하고 액세스합니다.
- AWS CloudShell을 시작합니다.
- AWS 알림 및 AWS Health 이벤트에 액세스합니다.
- 다양한 AWS 지식 소스의 지원을 받습니다.
- 기본 언어, 시각적 모드, 리전 등을 선택하여 AWS Management Console을 구성합니다.
- 계정, 조직, 서비스 할당량 및 결제 정보에 액세스합니다.

주제

AWS Management Console에서 서비스 메뉴 액세스

검색 창 옆의 서비스 메뉴를 사용하여 최근에 방문한 서비스에 액세스하고, 즐겨찾기 목록을 보고, 모든 AWS 서비스를 볼 수 있습니다. 분석 또는 애플리케이션 통합 등의 서비스 유형을 선택하여 유형별로 서비스를 볼 수도 있습니다.

다음 절차에서는 서비스 메뉴에 액세스하는 방법을 설명합니다.

서비스 메뉴에 액세스하려면

1. 에 로그인합니다..AWS Management Console

2. 탐색 모음에서 서비스(:::)를 선택합니다.
3. (선택 사항) 최근 방문을 선택하여 최근에 상호 작용한 서비스 및 애플리케이션을 확인합니다.
4. (선택 사항) 즐겨찾기를 선택하여 즐겨찾기 목록을 봅니다.
5. (선택 사항) myApplications 애플리케이션을 보려면 모든 애플리케이션을 선택합니다.
6. (선택 사항) 모든 서비스를 선택하여 모든 AWS 서비스의 알파벳순 목록을 봅니다.
7. (선택 사항) 서비스 유형을 선택하여 유형별로 AWS 서비스를 봅니다.

에서 통합 검색을 사용하여 제품, 서비스, 기능 등 검색 AWS Management Console

탐색 모음의 검색 상자는 AWS 서비스 및 기능, 서비스 설명서, AWS Marketplace 제품 등을 찾기 위한 통합 검색 도구를 제공합니다. 몇 글자 또는 질문을 입력하면 사용 가능한 모든 콘텐츠 유형에서 결과가 생성되기 시작합니다. 각 단어를 입력할 때마다 결과가 더욱 구체화됩니다. 사용 가능한 콘텐츠 유형은 다음과 같습니다.

- 서비스
- 특성
- 문서
- 블로그
- 지식 문서
- 이벤트
- 자습서
- Marketplace
- 리소스

> **Note**
>
> 집중 검색을 수행하여 리소스만 표시하도록 검색 결과를 필터링할 수 있습니다. 집중 검색을 수행하려면 검색 창의 쿼리 시작 부분에 `/Resources`를 입력하고 드롭다운 메뉴에서 /Resources를 선택합니다. 그런 다음 쿼리의 나머지 부분을 입력합니다.

주제

에서 AWS 제품 검색 AWS Management Console

다음 절차에서는 검색 도구를 사용하여 AWS 제품을 검색하는 방법을 자세히 설명합니다.

서비스, 기능, 설명서 또는 AWS Marketplace 제품을 검색하려면

1. AWS Management Console의 탐색 모음에 있는 검색 상자에 쿼리를 입력합니다.
2. 원하는 대상으로 이동할 링크를 선택합니다.

> **Tip**
>
> 키보드를 사용하여 상위 검색 결과로 빠르게 이동할 수도 있습니다. 먼저 Alt+s(Windows) 또는 Option+s(macOS)를 눌러 검색 창에 액세스합니다. 그런 다음 검색어를 입력합니다. 의도한 결과가 목록의 상단에 표시되면 Enter 키를 누릅니다. 예를 들어 Amazon EC2 콘솔로 빠르게 이동하려면 ec2를 입력하고 Enter 키를 누릅니다.

에서 검색 구체화 AWS Management Console

콘텐츠 유형별로 검색을 구체화하고 검색 결과에 대한 추가 정보를 볼 수 있습니다.

검색을 특정 콘텐츠 유형으로 구체화하려면

1. AWS Management Console의 탐색 모음에 있는 검색 상자에 쿼리를 입력합니다.
2. 검색 결과 옆에 있는 콘텐츠 유형 중 하나를 선택합니다.
3. (선택 사항) 특정 범주에 대한 모든 결과를 보려면:
   - 자세히 표시를 선택합니다. 결과를 보여주는 새 탭이 열립니다.
4. (선택 사항) 검색 결과에 대한 추가 정보를 보려면:
   a. 검색 결과에서 검색 결과 위에 커서를 놓습니다.
   b. 사용 가능한 추가 정보를 봅니다.

에서 서비스의 기능 보기 AWS Management Console

검색 결과 내에서 서비스의 기능을 볼 수 있습니다.

서비스의 기능을 보려면

1. AWS Management Console의 탐색 모음에 있는 검색 상자에 쿼리를 입력합니다.
2. 검색 결과에서 서비스의 해당 서비스 위에 커서를 놓습니다.
3. 주요 기능에서 링크 중 하나를 선택합니다.

의 탐색 모음 AWS CloudShell 에서 시작 AWS Management Console

AWS CloudShell 는 브라우저 기반의 사전 인증된 셸로, AWS Management Console 탐색 모음에서 직접 시작할 수 있습니다. 원하는 쉘(Bash, PowerShell 또는 Z 쉘)을 사용하여 서비스에 대해 AWS CLI 명령을 실행할 수 있습니다.

다음 두 가지 방법 중 하나를 AWS Management Console 사용하여에서 CloudShell을 시작할 수 있습니다.

- 콘솔 바닥글에서 CloudShell 아이콘을 선택합니다.
- 콘솔 탐색 모음에서 CloudShell 아이콘을 선택합니다.

이 서비스에 대한 자세한 내용은 AWS CloudShell 사용 설명서를 참조하세요.

를 AWS CloudShell 사용할 수 AWS 리전 있는에 대한 자세한 내용은 AWS 리전 서비스 목록을 참조하세요. 콘솔 지역 선택은 CloudShell 리전과 동기화됩니다. 선택한 리전에서 CloudShell을 사용할 수 없는 경우 CloudShell은 가장 가까운 리전에서 실행됩니다.

AWS 알림 및 Health 이벤트 액세스

탐색 모음에서 일부 AWS 알림에 액세스하고 상태 이벤트를 볼 수 있습니다. 탐색 모음에서 AWS 사용자 알림에 액세스하여 모든 AWS 알림과 AWS Health Dashboard를 볼 수도 있습니다.

자세한 내용은 AWS 사용자 알림 사용 설명서의 AWS 사용자 알림란 무엇인가요? 및 AWS Health 사용 설명서의 AWS Health란 무엇인가요?를 참조하세요.

다음 절차에서는 AWS 이벤트 정보에 액세스하는 방법을 설명합니다.

AWS 이벤트 정보에 액세스하려면

1. 에 로그인합니다..AWS Management Console
2. 탐색 모음에서 벨 아이콘을 선택합니다.
3. 알림 및 상태 이벤트를 봅니다.
4. (선택 사항) 모든 알림 보기를 선택하여 사용자 알림 콘솔로 이동합니다.
5. (선택 사항) 모든 상태 이벤트 보기를 선택하여 AWS Health 콘솔로 이동합니다.

지원 받기

탐색 모음에서 물음표 아이콘을 선택하여 지원을 받을 수 있습니다. 지원 메뉴에서 다음을 선택할 수 있습니다.

- Support Center 서비스 콘솔로 이동
- AWS IQ에서 전문가의 도움 받기
- AWS re:Post의 커뮤니티 문서 및 지식 센터에서 선별된 지식 보기
- AWS 설명서로 이동
- AWS 교육으로 이동
- AWS 시작하기 리소스 센터로 이동
- 현재 액세스 중인 서비스 콘솔에 대한 피드백 남기기

> **Note**
>
> 콘솔 바닥글에서 피드백을 선택하여 이 작업을 수행할 수도 있습니다. 열리는 모달의 제목은 현재 피드백을 남기는 콘솔을 나타냅니다.

또한 콘솔에서 언제든지 도움을 받고, 라이브 에이전트와 연결하고, AWS Q와 채팅하여 AWS에 대해 질문할 수 있습니다. 자세한 내용은 ??? 섹션을 참조하세요.

통합 설정을 AWS Management Console 사용하여 구성

이 주제에서는 통합 설정 페이지를 AWS Management Console 사용하여 모든 서비스 콘솔에 적용되는 기본값을 설정하도록를 구성하는 방법을 설명합니다.

주제

에서 통합 설정 구성 AWS Management Console

AWS Management Console 통합 설정 페이지에서 표시, 언어 및 리전과 같은 설정 및 기본값을 구성할 수 있습니다. 통합 탐색의 탐색 모음을 통해 통합 설정에 액세스할 수 있습니다. 시각적 모드와 기본 언어는 탐색 모음에서 직접 설정할 수도 있습니다. 이러한 변경 사항은 모든 서비스 콘솔에 적용됩니다.

> **Important**
>
> 설정, 즐겨찾기 서비스 및 최근에 방문한 서비스가 전역적으로 유지되도록 하기 위해이 데이터는 기본적으로 비활성화된 리전을 AWS 리전포함하여 모든에 저장됩니다. 이러한 리전은 아프리카(케이프타운), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 아시아 태평양(자카르타), 유럽(밀라노), 유럽(스페인), 유럽(취리히), 중동(바레인), 중동(UAE)입니다. 그래도 여전히 수동으로 리전에 액세스할 수 있도록 설정한 다음 해당 리전에서 리소스를 생성하고 관리해야 합니다. 이 데이터를 전혀 저장하지 않으려면 모두 재설정을 AWS 리전선택하여 설정을 지운 다음 설정 관리에서 최근에 방문한 서비스 기억을 옵트아웃합니다.

주제

에서 통합 설정 액세스 AWS Management Console

다음 절차에서는 통합 설정에 액세스하는 방법을 설명합니다.

통합 설정에 액세스하는 방법

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 통합 설정 페이지를 열려면 모든 사용자 설정 보기를 선택합니다.

에서 통합 설정 재설정 AWS Management Console

통합 설정을 재설정하여 모든 통합 설정 구성을 삭제하고 기본 설정을 복원할 수 있습니다.

> **Note**
>
> 이는 탐색 및 서비스 메뉴의 즐겨찾기 서비스 AWS, 콘솔 홈 위젯 및에서 최근에 방문한 서비스 AWS Console Mobile Application, 기본 언어, 기본 리전 및 시각적 모드와 같이 서비스에 적용되는 모든 설정을 포함하여의 여러 영역에 영향을 미칩니다.

모든 통합 설정을 재설정하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 모든 사용자 설정 보기를 선택하여 통합 설정 페이지를 엽니다.
4. 모두 재설정을 선택합니다.

에서 통합 설정 편집 AWS Management Console

다음 절차에서는 기본 설정을 편집하는 방법을 설명합니다.

통합 설정을 편집하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 모든 사용자 설정 보기를 선택하여 통합 설정 페이지를 엽니다.
4. 선호하는 설정 옆의 편집(Edit)을 선택합니다.

    - 현지화 및 기본 지역:(Localization and default Region:)

- 언어에서는 콘솔 텍스트의 기본 언어를 선택할 수 있습니다.
- 기본 리전(Default Region)에서는 로그인할 때마다 적용되는 기본 리전을 선택할 수 있습니다. 계정에 사용할 수 있는 리전 중 하나를 선택할 수 있습니다. 마지막으로 사용한 리전을 기본값으로 선택할 수도 있습니다.

  AWS Management Console의 리전 라우팅에 대한 자세한 내용은 리전 선택을 참조하세요.

- 표시:
  - Visual mode(시각적 모드)에서는 콘솔을 라이트 모드, 다크 모드 또는 브라우저의 기본 표시 모드로 설정할 수 있습니다.

    다크 모드는 베타 기능이며 일부 AWS 서비스 콘솔에는 적용되지 않을 수 있습니다.
  - 즐겨찾기 모음 표시는 해당 아이콘과 함께 전체 서비스 이름을 표시하거나 서비스의 아이콘만 표시하도록 즐겨찾기 모음 표시를 전환합니다.
  - 즐겨찾기 모음 아이콘 크기는 즐겨찾기 모음 표시의 서비스 아이콘 크기를 소형(16x16 픽셀)과 대형(24x24 픽셀) 간에 전환합니다.
- 설정 관리:
  - 최근에 방문한 서비스를 기억하면가 최근에 방문한 서비스를 AWS Management Console 기억할지 여부를 선택할 수 있습니다. 이 기능을 끄면 최근에 방문한 서비스 기록도 삭제되므로 서비스 메뉴 AWS Console Mobile Application또는 콘솔 홈 위젯에 최근에 방문한 서비스가 더 이상 표시되지 않습니다.

5. 변경 사항 저장을 선택합니다.

의 시각적 모드 변경 AWS Management Console

시각적 모드에서는 콘솔을 라이트 모드, 다크 모드 또는 브라우저의 기본 표시 모드로 설정할 수 있습니다.

탐색 모음에서 시각적 모드를 변경하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 시각적 모드에서 라이트 모드를 원하면 라이트, 다크 모드를 원하면 다크, 브라우저의 기본 표시 모드를 사용하려면 브라우저 기본값을 선택합니다.

에서 표시되는 리전 및 서비스 구성 AWS Management Console

계정 관리자는 AWS Management Console 탐색에 표시되는 AWS 리전 및 AWS 서비스를 제어할 수 있습니다. 이러한 계정 수준 설정은 통합 설정 페이지의 계정 설정 탭에서 사용할 수 있습니다. 리전을 숨기면 계정의 모든 사용자에 대해 리전 선택기에서 제거됩니다. 서비스를 숨기면 계정의 모든 사용자가 서비스 메뉴의 별도 섹션에서 서비스를 사용할 수 없는 것으로 표시됩니다. 숨겨진 서비스는 통합 검색 결과와 콘솔 홈의 최근 방문 및 즐겨찾기 위젯에서도 회색으로 표시됩니다.

사용자가 URL을 통해 숨겨진 리전 또는 서비스로 직접 이동하면 계정 수준에서 리전 또는 서비스가 숨겨져 있음을 알리는 오버레이가 표시됩니다.

> **Note**
>
> 통합 설정 페이지로의 탐색은 항상 사용할 수 있으므로 관리자는 이러한 설정을 잠글 수 없습니다. 사용자에게 필요한 권한이 없거나 AWS 사용자 경험 사용자 지정 서비스를 사용할 수 없는 경우 기본적으로 모든 리전 및 서비스가 표시됩니다.

주제

표시되는 리전 및 서비스를 구성하기 위한 사전 조건

표시되는 리전 및 서비스 설정을 보고 변경하려면 특정 IAM 권한이 필요합니다.

- 설정을 보려면 `uxc:GetAccountCustomizations` 권한이 필요합니다.
- 설정을 변경하려면 `uxc:UpdateAccountCustomizations` 권한이 필요합니다.

AWS 관리형 정책 `AWSManagementConsoleBasicUserAccess` 및 에는 이러한 권한이 `AWSManagementConsoleAdministratorAccess` 포함됩니다.

자세한 내용은 ??? 단원을 참조하십시오.

에서 표시되는 리전 구성 AWS Management Console

계정의 모든 사용자에 대해 리전 선택기에 AWS 리전 표시되는를 선택할 수 있습니다.

표시되는 리전을 구성하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 모든 사용자 설정 보기를 선택하여 통합 설정 페이지를 엽니다.
4. 계정 설정 탭을 선택합니다.
5. 가시 리전에서 표시할 리전의 확인란을 선택하거나 숨기려는 리전의 확인란을 선택 취소합니다.
6. 변경 사항 저장을 선택합니다.

저장하면 계정의 모든 사용자에 대해 숨겨진 리전이 리전 선택기에서 제거됩니다.

에서 표시되는 서비스 구성 AWS Management Console

계정의 모든 사용자에 대해 서비스 메뉴에 표시되는 AWS 서비스를 선택할 수 있습니다.

표시되는 서비스를 구성하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 모든 사용자 설정 보기를 선택하여 통합 설정 페이지를 엽니다.
4. 계정 설정 탭을 선택합니다.
5. 표시 서비스에서 표시할 서비스의 확인란을 선택하거나 숨기려는 서비스의 확인란을 선택 취소합니다.
6. 변경 사항 저장을 선택합니다.

저장하면 계정의 모든 사용자가 서비스 메뉴의 별도 섹션에서 숨겨진 서비스를 사용할 수 없는 것으로 표시됩니다. 숨겨진 서비스는 통합 검색 결과와 콘솔 홈의 최근 방문 및 즐겨찾기 위젯에서도 회색으로 표시됩니다.

리전 선택

많은 서비스의 경우 리소스가 관리 AWS 리전 되는 위치를 지정하는를 선택할 수 있습니다. 리전은 동일한 지리적 영역에 위치한 AWS 리소스 집합입니다. 와 같은 일부 서비스의 경우 AWS Management Console 또는에 대한 리전을 선택할 필요가 없습니다 AWS Identity and Access Management. AWS 리전에 대해 자세히 알아보려면 AWS 일반 참조의 AWS 리전관리 섹션을 참조하세요.

> **Note**
>
> AWS 리소스를 생성했지만 콘솔에 해당 리소스가 표시되지 않는 경우 콘솔에 다른 리전의 리소스가 표시될 수 있습니다. 일부 리소스(예: Amazon EC2 인스턴스)는 해당 리소스가 생성된 리전에 한정됩니다.

주제

의 탐색 모음에서 리전 선택 AWS Management Console

다음 절차에서는 탐색 모음에서 리전을 변경하는 방법을 자세히 설명합니다.

탐색 모음에서 리전을 선택하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 현재 표시된 리전의 이름을 선택합니다.
3. 변경할 대상 리전을 선택합니다.

에서 기본 리전 설정 AWS Management Console

다음 절차에서는 통합 설정 페이지에서 기본 리전을 변경하는 방법을 자세히 설명합니다.

기본 리전을 설정하려면

1. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
2. 모든 사용자 설정 보기를 선택하여 통합 설정 페이지로 이동합니다.
3. 현지화 및 기본 지역(Localization and default Region) 옆의 편집(Edit)을 선택합니다.
4. 기본 리전에서 리전을 선택합니다.

> **Note**
>
> 기본 리전을 선택하지 않으면 마지막으로 방문한 리전이 기본값이 됩니다.

5. 설정 저장을 선택합니다.
6. (선택 사항) 새 기본 리전으로 이동을 선택하여 즉시 새 기본 리전으로 이동합니다.

의 즐겨찾기 AWS Management Console

자주 사용하는 서비스 및 애플리케이션에 보다 빠르게 액세스하려면 서비스 콘솔을 즐겨찾기 목록에 저장하면 됩니다. AWS Management Console을 사용하여 즐겨찾기를 추가하거나 제거할 수 있습니다. 즐겨찾기에 서비스를 추가하면 해당 서비스 또는 애플리케이션이 즐겨찾기 퀵바에 표시됩니다.

주제

- 에서 즐겨찾기 추가 AWS Management Console
- 에서 즐겨찾기 액세스 AWS Management Console
- 에서 즐겨찾기 제거 AWS Management Console

에서 즐겨찾기 추가 AWS Management Console

서비스 메뉴와 최근 방문 메뉴에서 즐겨찾기에 서비스 및 애플리케이션을 추가할 수 있습니다. 검색 상자의 검색 결과 페이지를 사용하여 서비스를 즐겨찾기에 추가할 수도 있습니다. 즐겨찾기에 추가한 서비스와 애플리케이션은 즐겨찾기 퀵바에 표시됩니다.

주제

- 의 즐겨찾기 퀵바 AWS Management Console
- 에서 즐겨찾기에 서비스 추가 AWS Management Console
- 에서 즐겨찾기에 애플리케이션 추가 AWS Management Console

의 즐겨찾기 퀵바 AWS Management Console

즐겨찾기에 AWS 서비스 또는 애플리케이션이 하나 이상 추가되면 즐겨찾기 퀵바가 나타납니다. 즐겨찾기 퀵바는 탐색 모음 뒤에 있으며 모든 AWS 서비스 콘솔에 표시되므로 자주 사용하는 서비스 및 애플리케이션에 빠르게 액세스할 수 있습니다. 서비스나 애플리케이션을 왼쪽 또는 오른쪽으로 드래그하여 즐겨찾기 퀵바의 서비스 및 애플리케이션 순서를 재정렬할 수 있습니다.

에서 즐겨찾기에 서비스 추가 AWS Management Console

서비스 메뉴 또는 검색 상자의 검색 결과 페이지에서 즐겨찾기에 서비스를 추가할 수 있습니다.

Services menu

서비스 메뉴에서 즐겨찾기를 추가하려면

1. AWS Management Console을 엽니다.
2. 탐색 모음에서 서비스(:::)를 선택합니다.
3. (선택 사항) 최근에 방문한 서비스를 즐겨찾기에 추가합니다.
   a. 최근 방문에서 해당 서비스 위에 커서를 놓습니다.
   b. 해당 서비스 이름 옆에 있는 별을 선택합니다.
4. 모든 서비스를 선택합니다.
5. 선택한 서비스 위에 커서를 놓습니다.
6. 해당 서비스 이름 옆에 있는 별을 선택합니다.

Search box

검색 상자에서 즐겨찾기를 추가하려면

1. AWS Management Console을 엽니다.
2. 검색 상자에 서비스 이름을 입력합니다.
3. 검색 결과 페이지에서 서비스 이름 옆에 있는 별을 선택합니다.

> **Note**
> 즐겨찾기에 서비스를 추가하면 탐색 모음 다음에 있는 즐겨찾기 퀵바에 서비스가 추가됩니다.

에서 즐겨찾기에 애플리케이션 추가 AWS Management Console

서비스 메뉴에서 즐겨찾기에 애플리케이션을 추가할 수 있습니다.

서비스 메뉴에서 즐겨찾기를 추가하려면

1. AWS Management Console을 엽니다.
2. 탐색 모음에서 서비스(:::)를 선택합니다.
3. (선택 사항) 최근에 방문한 애플리케이션을 즐겨찾기에 추가합니다.

a. 최근 방문에서 해당 애플리케이션 위에 커서를 놓습니다.

b. 애플리케이션 이름 옆에 있는 별을 선택합니다.

4. [Applications]를 선택합니다.
5. 선택한 애플리케이션 위에 커서를 놓습니다.
6. 애플리케이션 이름 옆에 있는 별을 선택합니다.

> **Note**
>
> 즐겨찾기에 애플리케이션을 추가하면 탐색 모음 다음에 있는 즐겨찾기 퀵바에 서비스가 추가됩니다.

에서 즐겨찾기 액세스 AWS Management Console

서비스 메뉴, 즐겨찾기 퀵바 및 즐겨찾기 위젯에서 즐겨찾기 서비스에 액세스할 수 있습니다.

Services menu

서비스 메뉴에서 즐겨찾기에 액세스하려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.
2. 탐색 모음에서 서비스(⁝⁝⁝)를 선택합니다.
3. 즐겨찾기를 선택합니다.
4. 즐겨찾기에 추가한 서비스 및 애플리케이션을 봅니다.
5. (선택 사항) 애플리케이션 리소스를 확인하려면 다음을 수행합니다.

   a. 애플리케이션을 선택합니다.

   b. (선택 사항) 보기를 선택합니다.

   c. 리소스를 확인합니다.

   d. (선택 사항) 필터를 선택합니다. 속성 또는 태그별로 리소스를 필터링할 수 있습니다. 자세한 내용은 AWS 리소스 탐색기 Resource Explorer 사용 설명서의 Resource Explorer에 대한 검색 쿼리 구문 참조를 참조하세요.

   e. (선택 사항) 관련 서비스 콘솔에서 볼 리소스를 선택합니다.

> **Tip**
>
> 서비스(:::)를 선택하여 중단한 리소스를 계속 탐색할 수 있습니다. 적용된 검색 필터도 유지됩니다.

Favorites quickbar

즐겨찾기 퀵바에서 즐겨찾기에 액세스하려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.
2. 즐겨찾기 퀵바에서 서비스를 확인합니다.

Favorites widget

즐겨찾기 위젯에서 즐겨찾기에 액세스하려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.
2. (선택 사항) 즐겨찾기 위젯이 없는 경우 즐겨찾기 위젯을 추가합니다.
   a. 콘솔 홈 페이지에서 + 위젯 추가 버튼을 선택합니다.
   b. 위젯 추가 메뉴에서 :: 아이콘을 사용하여 즐겨찾기 위젯을 드래그해 콘솔 홈 페이지에 놓습니다.
3. 즐겨찾기 위젯에서 서비스 및 애플리케이션을 확인합니다.

위젯에 대한 자세한 내용은 the section called “위젯 작업” 섹션을 참조하세요.

에서 즐겨찾기 제거 AWS Management Console

서비스 메뉴를 사용하여 즐겨찾기에서 서비스 및 애플리케이션을 제거할 수 있습니다. 검색 창에서 검색 결과 페이지를 사용하여 서비스를 제거할 수도 있습니다.

Services menu

서비스 메뉴에서 즐겨찾기를 제거하려면

1. AWS Management Console을 엽니다.

2. 탐색 모음에서 서비스를 선택합니다.
3. 즐겨찾기를 선택합니다.
4. 서비스 또는 애플리케이션 옆의 별표를 선택 취소합니다.

Search box

> **Note**
> 현재는 검색 창에서 검색 결과 페이지를 사용해야만 서비스를 제거할 수 있습니다.

검색 상자에서 즐겨찾기를 제거하려면

1. AWS Management Console을 엽니다.
2. 검색 상자에 서비스 이름을 입력합니다.
3. 검색 결과 페이지에서 서비스 이름 옆에 있는 별을 선택 취소합니다.

에서 암호 변경 AWS Management Console

사용자 유형 및 권한에 따라 AWS Management Console에서 암호를 변경할 수 있습니다. 다음 주제에서는 각 사용자 유형의 암호를 변경하는 방법을 설명합니다.

주제

- 의 루트 사용자 AWS Management Console
- 의 IAM 사용자 AWS Management Console
- 의 IAM Identity Center 사용자 AWS Management Console
- 의 연동 자격 증명 AWS Management Console

의 루트 사용자 AWS Management Console

루트 사용자는 AWS Management Console에서 직접 암호를 변경할 수 있습니다. 루트 사용자는 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한을 가진 계정 소유자입니다. AWS 계정을 생성하고 루트 사용자 이메일과 암호를 사용하여 로그인하는 경우 루트 사용자입니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 루트 사용자를 참조하세요.

루트 사용자로서 암호를 변경하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 계정 이름을 선택합니다.
3. 보안 자격 증명을 선택합니다.
4. 표시되는 옵션은 AWS 계정 유형에 따라 다릅니다. 콘솔에 표시되는 지침에 따라 암호를 변경합니다.
5. 현재 암호를 한 번 입력하고 새 암호를 두 번 입력합니다.

   새 암호는 8자 이상이어야 하며 다음을 포함해야 합니다.

   - 하나 이상의 기호
   - 하나 이상의 숫자
   - 하나 이상의 대문자
   - 하나 이상의 소문자
6. 암호 변경(Change Password) 또는 변경 사항 저장(Save changes)을 선택합니다.

의 IAM 사용자 AWS Management Console

IAM 사용자는 권한에 AWS Management Console 따라에서 암호를 변경할 수 있습니다. 그렇지 않으면 AWS 액세스 포털을 사용해야 합니다. IAM 사용자는 특정 사용자 지정 권한이 부여된 AWS 계정 내 자격 증명입니다. AWS 계정을 생성하지 않았고 관리자 또는 헬프데스크 직원이 계정 ID 또는 AWS 계정 별칭, IAM 사용자 이름 및 암호가 포함된 로그인 자격 증명을 제공한 경우 IAM 사용자입니다. 자세한 내용은 AWS 로그인 사용 설명서의 IAM 사용자를 참조하세요.

AWS: IAM 사용자가 보안 자격 증명 페이지에서 자신의 콘솔 암호를 변경할 수 있도록 허용 정책의 권한이 있는 경우 콘솔에서 암호를 변경할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 사용자가 자신의 암호를 변경하는 방법을 참조하세요.

에서 암호를 변경하는 데 필요한 권한이 없는 경우 사용 AWS IAM Identity Center 설명서의 AWS IAM Identity Center 사용자 암호 재설정을 AWS Management Console 참조하세요.

의 IAM Identity Center 사용자 AWS Management Console

AWS IAM Identity Center 사용자는 AWS 액세스 포털에서 암호를 변경해야 합니다. 자세한 내용은 사용 AWS IAM Identity Center 설명서의 AWS IAM Identity Center 사용자 암호 재설정을 참조하세요.

IAM Identity Center 사용자는 고유한 URL로 AWS 액세스 포털을 통해 AWS Organizations 로그인하는의 일부 AWS 인 계정을 가진 사용자입니다. 이러한 사용자는 IAM Identity Center, Active Directory, 또는 다른 외부 ID 제공업체가 직접 생성할 수 있습니다. 자세한 내용은 AWS 로그인 사용 설명서의 AWS IAM Identity Center 사용자를 참조하세요.

의 연동 자격 증명 AWS Management Console

페더레이션 자격 증명 사용자는 AWS 액세스 포털에서 암호를 변경해야 합니다. 자세한 내용은 사용 AWS IAM Identity Center 설명서의 AWS IAM Identity Center 사용자 암호 재설정을 참조하세요.

페더레이션형 ID 사용자는 외부 ID 제공업체(idP)를 사용하여 로그인합니다. 다음 중 하나에 해당하면 페더레이션 ID입니다.

- Login with Amazon, Facebook 또는 Google과 같은 타사 자격 증명을 사용하여 AWS 계정 또는 리소스에 액세스합니다.
- 동일한 자격 증명을 사용하여 회사 시스템 및 AWS 서비스에 로그인하고 사용자 지정 회사 포털을 사용하여 로그인합니다 AWS.

자세한 내용은 AWS 로그인 사용 설명서의 페더레이션형 ID를 참조하세요.

의 언어 변경 AWS Management Console

AWS Console Home 환경에는에서 AWS 서비스의 기본 언어를 변경할 수 있는 통합 설정 페이지가 포함되어 있습니다 AWS Management Console. 탐색 모음의 설정 메뉴에서 기본 언어를 빠르게 변경할 수도 있습니다.

> **Note**
>
> 다음 절차에 따라 모든 AWS 서비스 콘솔의 언어를 변경할 수 있지만 AWS 설명서의 언어는 변경할 수 없습니다. 설명서에 사용된 언어를 변경하려면 설명서 페이지의 오른쪽 상단에 있는 언어 메뉴를 사용합니다.

주제

- 지원되는 언어
- 의 탐색 모음에서 기본 언어 변경 AWS Management Console
- 의 통합 설정을 통해 기본 언어 변경 AWS Management Console

지원되는 언어

는 AWS Management Console 현재 다음 언어를 지원합니다.

- 영어(미국)
- 영어(영국)
- 인도네시아어
- 독일어
- 스페인 요리
- 프랑스어
- 일본어
- 이탈리아어
- 포르투갈어
- 한국어
- 중국어 간체
- 중국어 번체
- 터키어

의 탐색 모음에서 기본 언어 변경 AWS Management Console

다음 절차에서는 탐색 모음에서 직접 기본 언어를 변경하는 방법을 자세히 설명합니다.

탐색 모음에서 기본 언어를 변경하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 언어에서, 브라우저 기본값을 선택하거나 드롭다운 목록에서 원하는 언어를 선택합니다.

의 통합 설정을 통해 기본 언어 변경 AWS Management Console

다음 절차에서는 통합 설정 페이지에서 기본 언어를 변경하는 방법을 자세히 설명합니다.

통합 설정에서 기본 언어를 변경하려면

1. AWS Management Console에 로그인합니다.

2. 탐색 모음에서 기어 모양 아이콘(#)을 선택합니다.
3. 통합 설정 페이지를 열려면 모든 사용자 설정 보기를 선택합니다.
4. 통합 설정(Unified Settings)에서 현지화 및 기본 지역(Localization and default Region) 옆의 편집(Edit)을 선택합니다.
5. 콘솔에 사용할 언어를 선택하려면 다음 옵션 중 하나를 선택합니다.

   - 드롭다운 목록에서 브라우저 기본값을 선택한 다음 설정 저장을 선택합니다.

     모든 AWS 서비스에 대한 콘솔 텍스트는 브라우저 설정에서 설정한 기본 언어로 표시됩니다.

     > **Note**
     >
     > 브라우저 기본값은 AWS Management Console에서 지원하는 언어만 지원합니다.

   - 드롭다운 목록에서 브라우저 기본값을 선택한 다음 설정 저장을 선택합니다.

     모든 AWS 서비스의 콘솔 텍스트는 원하는 언어로 표시됩니다.

에서 AWS 계정, 조직, 서비스 할당량 및 결제 정보에 액세스 AWS Management Console

필요한 권한이 있는 경우 콘솔에서 AWS 계정, 서비스 할당량, 조직 및 결제 정보에 액세스할 수 있습니다.

> **Note**
>
> AWS Management Console 만 계정, 조직, 서비스 할당량 및 결제 정보에 대한 액세스를 제공합니다. 이러한 서비스에는 별도의 콘솔이 있습니다. 자세한 내용은 다음 자료를 참조하세요.
>
> - AWS Account Management 참조 안내서에서 AWS 계정을 관리합니다.
> - AWS Organizations 사용 설명서의 란 무엇입니까 AWS Organizations?
> - Service Quotas 사용 설명서의 Service Quotas란 무엇인가요?.
> - AWS 결제 사용 설명서의 AWS 결제 및 비용 관리 홈 페이지 사용.

> **Tip**
>
> Amazon Q에 문의하여 이러한 주제에 대한 자세한 정보를 확인할 수도 있습니다. 자세한 내용은 Amazon Q Developer와 채팅을 참조하세요.

주제

에서 계정 정보 액세스 AWS Management Console

필요한 권한이 있는 경우 콘솔에서 AWS 계정에 대한 정보에 액세스할 수 있습니다.

계정 정보에 액세스하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 계정 이름을 선택합니다.
3. 계정을 선택합니다.
4. 계정 정보를 봅니다.

> **Note**
>
> AWS 계정을 해지하려면 AWS Account Management 참조 안내서의 AWS 계정 해지를 참조하세요.

에서 조직 정보에 액세스 AWS Management Console

필요한 권한이 있는 경우 콘솔에서 AWS 조직에 대한 정보에 액세스할 수 있습니다.

조직 정보에 액세스하려면

1. AWS Management Console에 로그인합니다.

2. 탐색 모음에서 계정 이름을 선택합니다.
3. 조직을 선택합니다.
4. 조직 정보를 봅니다.

에서 서비스 할당량 정보 액세스 AWS Management Console

필요한 권한이 있는 경우 콘솔에서 서비스 할당량에 대한 정보에 액세스할 수 있습니다.

서비스 할당량 정보에 액세스하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 계정 이름을 선택합니다.
3. Service Quotas를 선택하세요.
4. 서비스 할당량 정보를 보고 관리합니다.

에서 결제 정보 액세스 AWS Management Console

필요한 권한이 있는 경우 콘솔에서 AWS 요금에 대한 정보에 액세스할 수 있습니다.

결제 정보에 액세스하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 계정 이름을 선택합니다.
3. 결제 및 비용 관리를 선택합니다.
4. AWS 결제 및 비용 관리 대시보드를 사용하여 월별 지출에 대한 요약 및 내역을 찾을 수 있습니다.

여러 계정에 로그인

AWS Management Console의 단일 웹 브라우저에서 최대 5개의 서로 다른 자격 증명을 동시에 로그인할 수 있습니다. 이들은 서로 다른 계정 또는 동일한 계정의 루트, IAM 또는 페더레이션 역할의 조합일 수 있습니다. AWS Management Console에 로그인하는 각 자격 증명은 새 탭에서의 자체 인스턴스를 엽니다.

멀티 세션 지원을 활성화하면 콘솔 URL에 하위 도메인(예: `https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`)이 포함됩니다. 북마크와 콘솔 링크를 업데이트해야 합니다.

> **Note**
>
> AWS Management Console의 계정 메뉴에서 멀티 세션 켜기를 선택하거나 https://console.aws.amazon.com/에서 멀티 세션 켜기를 선택하여 멀티 세션 지원에 옵트인해야 합니다. https://console.aws.amazon.com/에서 멀티 세션 켜기를 선택하거나 브라우저 쿠키를 삭제하여 언제든지 멀티 세션을 옵트아웃할 수 있습니다. 옵트인은 브라우저별로 다릅니다.

여러 자격 증명에 로그인하려면 다음을 수행합니다.

1. 에 로그인합니다..AWS Management Console
2. 탐색 모음에서 계정 이름을 선택합니다.
3. 세션 추가를 선택하고 로그인을 선택합니다. 새 탭이 열리고 로그인할 수 있습니다.

   > **Note**
   >
   > 루트 또는 IAM 사용자로 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS Management Console에 로그인을 참조하세요.

4. 보안 인증을 입력합니다.
5. 로그인을 선택합니다. 이 탭에서 AWS Management Console은 선택한 AWS 자격 증명으로 로드됩니다.
6. (선택 사항) 추가 역할에 페더레이션하려면 다음을 수행합니다.

   a. AWS IAM Identity Center 액세스 포털 또는 Single Sign-On(SSO) 포털에서 추가 역할에 로그인합니다.

   b. AWS Management Console에서 계정 이름을 선택합니다.

   c. 선택할 수 있는 추가 세션을 봅니다.

AWS의 AWS Management Console 권장 작업

AWS 권장 작업은 태스크를 완료하고 모범 사례를 구현하기 위한 상황별 제안을 제공하여 AWS Management Console에서 더 효율적으로 작업할 수 있도록 지원합니다. 관련 권장 사항이 있을 경우, 이러한 제안을 바탕으로 신속하게 조치를 취할 수 있는 동적 버튼이 표시됩니다.

> **Note**
>
> AWS 권장 작업은 리소스 상태를 분석하여 제안을 제공하지만 사용자 데이터는 처리하지 않습니다.

주제

AWS 권장 작업의 기능

- 작업 권장 사항 - 리소스 상태, 모범 사례 및 일반적인 사용 패턴을 기반으로 관련성 높은 제안 받기
- 원클릭 작업 - 성공 메시지 또는 리소스 보기에서 바로 권장 작업 완료
- 통합형 오른쪽 측면 패널 - 통합 측면 패널에 액세스하여 워크플로를 중단하지 않고 제안 구현
- 다중 서비스 지원 - 여러 AWS 서비스에 대한 권장 사항 가져오기

권장 작업 사용

권장 작업을 사용하려면 다음을 수행합니다.

1. 에 로그인하기AWS Management Console
2. # 권장 작업 버튼을 찾습니다.

   > **Note**
   >
   > 권장 작업 버튼은 AWS Management Console의 모든 위치에 나타날 수 있으며 권장 작업을 사용할 수 있는 경우에만 액세스할 수 있습니다.

3. 버튼을 선택하여 사용 가능한 작업을 봅니다.
4. 직접 또는 측면 패널을 통해 권장 사항을 실행합니다.

를 사용하여 AWS 권장 작업 API 호출 로깅 AWS CloudTrail

AWS 권장 작업은 사용자AWS CloudTrail, 역할 또는가 수행한 작업의 레코드를 제공하는 서비스인와 통합됩니다 AWS 서비스. CloudTrail은 AWS 권장 작업에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는의 AWS Management Console 호출과 AWS 권장 작업 API 작업에 대한 코드 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 AWS 권장 작업에 수행된 요청, 요청이 수행된 IP 주소, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

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

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

AWS CloudTrail의 권장 작업 관리 이벤트

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

AWS 권장 작업은 모든 AWS 권장 작업 컨트롤 플레인 작업을 관리 이벤트로 기록합니다.

AWS 권장 작업 이벤트 예제

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

다음 예제는 작업을 시연하는 CloudTrail 이벤트를 보여줍니다.


```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
```

```
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```


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

AWS Console Home 에서 사용 AWS Management Console

이 주제에서는 콘솔 홈 페이지를 사용자 지정하는 방법을 AWS Console Home포함하여를 사용하는 방법을 설명합니다. 콘솔 홈은 AWS Management Console의 홈 페이지입니다. 콘솔에 처음 로그인하면 콘솔 홈 페이지로 이동합니다. 위젯과 애플리케이션을 사용하여 콘솔 홈 페이지를 사용자 지정할 수 있습니다. 위젯을 사용하면 AWS 서비스 및 리소스에 대한 정보를 추적하는 사용자 지정 구성 요소를 추가할 수 있습니다. 애플리케이션을 사용하면 AWS 리소스와 메타데이터를 그룹화할 수 있습니다. myApplications를 사용하여 애플리케이션을 관리할 수 있습니다. 콘솔 홈을 사용하여 모든 AWS 서비스 목록을 보고 Amazon Q와 채팅할 수도 있습니다.

주제

에서 모든 AWS 서비스 보기 AWS Console Home

콘솔 홈에서 모든 AWS 서비스 목록을 보고 콘솔에 액세스할 수 있습니다.

전체 AWS 서비스 목록에 액세스하려면

1. AWS Management Console에 로그인합니다.
2. 햄버거 아이콘(☰)을 선택하여 콘솔 홈 메뉴를 확장합니다.
3. 모든 서비스를 선택합니다.
4. 콘솔로 이동할 AWS 서비스를 선택합니다.

에서 위젯 작업 AWS Console Home

콘솔 홈 대시보드에는 AWS 환경에 대한 중요한 정보를 표시하고 서비스에 대한 바로 가기를 제공하는 위젯이 포함되어 있습니다. 위젯을 추가 및 제거하거나, 다시 정렬 또는 크기를 조정하여 환경을 사용자 지정할 수 있습니다.

위젯 관리

위젯을 추가, 제거, 재정렬하고 크기를 조정하며 관리할 수 있습니다. 기본 위젯을 제거하고 다시 추가할 수 있습니다. 콘솔 홈을 기본 레이아웃으로 재설정하고 새 위젯을 요청할 수도 있습니다.

위젯을 추가하려면

1. 콘솔 홈 대시보드 오른쪽 상단 또는 하단에 있는 +위젯 추가 버튼을 선택합니다.
2. 위젯 제목 표시줄 왼쪽 상단에 있는 6개의 세로 점(⁞⁞)으로 나타낸 드래그 표시기를 선택한 다음 콘솔 홈 대시보드로 드래그합니다.

위젯을 제거하려면

1. 위젯 제목 표시줄 오른쪽 상단에 있는 3개의 세로 점(⋮)으로 나타낸 줄임표를 선택합니다.
2. 위젯 제거(Remove widget)를 선택합니다.

위젯을 다시 정렬하려면

- 위젯 제목 표시줄 왼쪽 상단에 있는 6개의 세로 점(⁞⁞)으로 나타낸 드래그 표시기를 선택한 다음 콘솔 홈 대시보드의 새 위치로 위젯을 드래그합니다.

위젯의 크기를 조정하려면

- 위젯 오른쪽 하단의 크기 조정 아이콘을 선택한 다음 위젯을 드래그하여 크기를 조정합니다.

위젯 구성 및 설정부터 다시 시작하려면 콘솔 홈 대시보드를 기본 레이아웃으로 재설정하면 됩니다. 이렇게 하면 변경 사항이 콘솔 홈 대시보드 레이아웃으로 되돌아가며 모든 위젯이 기본 위치 및 크기로 복원됩니다.

페이지를 기본 레이아웃으로 재설정하려면

1. 페이지 오른쪽 상단에서 기본 레이아웃으로 재설정을 선택합니다.
2. 확인하려면 재설정을 선택합니다.

> **Note**
>
> 그러면 모든 변경 사항이 콘솔 홈 대시보드의 레이아웃으로 되돌아갑니다.

콘솔 홈 대시보드에서 새 위젯을 요청하려면

1. 콘솔 홈 대시보드 왼쪽 하단에서 다른 위젯을 보고 싶다면 알려주세요!를 선택합니다.

   콘솔 홈 대시보드에 추가되었으면 하는 위젯을 설명해 주세요.
2. 제출을 선택합니다.

> **Note**
>
> 제안은 정기적으로 검토되어, 향후 업데이트 시 새로운 위젯이 AWS Management Console에 추가될 수 있습니다.

의 myApplications는 무엇입니까 AWS Console Home?

myApplications는 AWS에 구축된 애플리케이션의 비용, 상태, 보안 태세 및 성능을 관리하고 모니터링할 수 있도록 하는 콘솔 홈의 확장입니다. 애플리케이션을 사용하면 리소스와 메타데이터를 그룹화할 수 있습니다. 계정의 모든 애플리케이션, 모든 애플리케이션의 주요 지표,의 한 보기에서 여러 서비스 콘솔의 비용, 보안 및 운영 지표와 인사이트에 대한 개요에 액세스할 수 있습니다 AWS Management Console. myApplications에는 다음이 포함됩니다.

- 콘솔 홈 페이지의 애플리케이션 위젯
- 애플리케이션 리소스 비용 및 보안 조사 결과를 보는 데 사용할 수 있는 myApplications
- 비용, 성능, 보안 조사 결과 같은 주요 애플리케이션 지표를 볼 수 있는 myApplications 대시보드

주제

- myApplications의 애플리케이션
- myApplications의 리소스
- 의 myApplications 대시보드 AWS Console Home

myApplications의 기능

- 애플리케이션 생성 - 새 애플리케이션을 생성하고 리소스를 구성합니다. 애플리케이션은 myApplications에 자동으로 표시되므로 AWS Management Console, , APIs, CLI 및 SDKs. 애플리케이션을 생성할 때 코드형 인프라(IAC)가 생성되며 myApplication 대시보드에서 액세스할 수 있습니다. IaC는 AWS CloudFormation 및 Terraform을 포함한 IaC 도구에서 사용할 수 있습니다.
- 애플리케이션 액세스 - myApplications 위젯에서 원하는 애플리케이션을 선택하여 빠르게 액세스할 수 있습니다.
- 리소스 액세스 - 애플리케이션을 선택하여 서비스 메뉴에서 애플리케이션 리소스를 빠르게 확인할 수 있습니다. 리소스를 선택하면 해당 서비스 콘솔로 바로 이동합니다. 리소스 테이블의 위치가 저장되므로 서비스 메뉴에서 언제든지 계속 탐색할 수 있습니다.
- 애플리케이션 지표 비교 - myApplications를 사용하여 애플리케이션 리소스 비용, 여러 애플리케이션에 대한 중요한 보안 조사 결과 수 등 애플리케이션의 주요 지표를 비교할 수 있습니다.
- 애플리케이션 모니터링 및 관리 - 경보, canary 및 서비스 수준 목표, 조사 Amazon CloudWatch결과 AWS Security Hub CSPM및 비용 추세를 사용하여 애플리케이션 상태 및 성능을 평가합니다 AWS Cost Explorer Service. 컴퓨팅 지표 요약 및 최적화를 찾고에서 리소스 규정 준수 및 구성 상태를 관리할 수도 있습니다 AWS Systems Manager.

관련 서비스

myApplications는 다음과 같은 서비스를 사용합니다.

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS 리소스 탐색기
- AWS Security Hub CSPM
- Systems Manager

- AWS Service Catalog
- 태그 지정

myApplications 액세스

AWS Management Console의 왼쪽 사이드바에서 myApplications를 선택하여 myApplications에 액세스할 수 있습니다.

가격 책정

의 myApplications AWS 는 추가 비용 없이 제공됩니다. 설정 요금이나 사전 약정은 없습니다. myApplications 대시보드에 요약된 기본 리소스 및 서비스의 사용 요금은 해당 리소스에 대해 게시된 요금으로 여전히 적용됩니다.

myApplications에 지원되는 리전

myApplications는 AWS 리전다음에서 사용할 수 있습니다.

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 아시아 태평양(뭄바이)
- 아시아 태평양(오사카)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(파리)

- 유럽(스톡홀름)
- 남아메리카(상파울루)

옵트인 리전

옵트인 리전에서 기본 지원 리전으로 이러한 리전에서 myApplications를 사용하려면 해당 리전을 수동으로 활성화해야 합니다. 에 대한 자세한 내용은 관리를 AWS 리전 AWS 리전참조하세요. 다음과 같은 옵트인 리전이 지원됩니다.

- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 유럽(밀라노)
- 유럽(스페인)
- 유럽(취리히)
- Middle East (Bahrain)
- 중동(UAE)
- 이스라엘(텔아비브)

myApplications의 애플리케이션

애플리케이션을 사용하여 리소스와 메타데이터를 그룹화할 수 있습니다. 애플리케이션을 생성, 온보딩, 확인, 편집 또는 삭제하며 관리할 수 있습니다. 코드 스니펫을 생성하여 애플리케이션에 새 리소스를 자동으로 추가할 수도 있습니다.

> **Note**
>
> 즐겨찾기에 애플리케이션을 추가하여 더 쉽게 액세스할 수 있습니다. 자세한 내용은 ??? 단원을 참조하십시오.

주제

- myApplications의 애플리케이션 생성
- myApplications의 기존 AppRegistry 애플리케이션 온보딩
- myApplications의 애플리케이션 보기
- myApplications의 애플리케이션 편집
- myApplications의 애플리케이션 삭제
- myApplications의 코드 스니펫 생성

myApplications의 애플리케이션 생성

새 애플리케이션을 생성하거나 2023년 11월 8일 이전에 생성된 the section called “애플리케이션 온보딩”하여 myApplications를 시작할 수 있습니다. 새 애플리케이션을 생성하는 경우 리소스를 검색하여 선택하거나 기존 태그를 사용하여 리소스를 추가할 수 있습니다.

새 애플리케이션을 생성하려면

1. AWS Management Console에 로그인합니다.
2. 왼쪽 사이드바를 확장하여 myApplications를 선택합니다.
3. 애플리케이션 생성을 선택합니다.
4. 애플리케이션 이름을 입력합니다.
5. (선택 사항) 애플리케이션 설명을 입력합니다.
6. (선택 사항) 태그를 추가합니다. 태그는 리소스에 대한 메타데이터를 유지하기 위해 리소스에 적용되는 키-값 쌍입니다.

   > **Note**
   >
   > AWS 애플리케이션 태그는 새로 생성된 애플리케이션에 자동으로 적용됩니다. 자세한 내용은 AWS Service Catalog AppRegistry 관리자 안내서의 AWS 애플리케이션 태그를 참조하세요.

7. (선택 사항) 속성 그룹을 추가합니다. 속성 그룹을 사용하여 애플리케이션 메타데이터를 저장할 수 있습니다.
8. 다음을 선택합니다.
9. (선택 사항) 리소스를 추가합니다.

Search and select resources

> **Note**
>
> 리소스를 검색하고 추가하려면 AWS 리소스 탐색기를 켜야 합니다. 자세한 내용은 시작하기를 참조하세요 AWS 리소스 탐색기.
> 추가된 모든 리소스에는 AWS 애플리케이션 태그가 지정됩니다.

검색을 사용하여 리소스를 추가하려면

1. 리소스 검색 및 선택을 선택합니다.
2. 리소스 선택을 선택합니다.
3. (선택 사항) 보기를 선택합니다.
4. 리소스를 검색합니다. 키워드, 이름 또는 유형별로 검색하거나 리소스 유형을 선택할 수 있습니다.

   > **Note**
   >
   > 찾고 있는 리소스를 찾을 수 없는 경우 문제를 해결합니다 AWS 리소스 탐색기. 자세한 내용은 Resource Explorer User Guide의 Troubleshooting Resource Explorer search issues를 참조하세요.

5. 추가할 리소스 옆에 있는 확인란을 선택합니다.
6. 추가를 선택합니다.
7. 다음을 선택합니다.
8. 선택 사항을 검토합니다.

Automatically add resources using tags

애플리케이션을 생성할 때 기존 태그 키-값 페어를 지정하여 대량 온보드 리소스를 만들 수 있습니다. 이 방법을 사용하면가 지정된 키-값 페어로 태그가 지정된 모든 리소스에 `awsApplication` 태그를 AWS 자동으로 적용하고 기본적으로 애플리케이션 리소스에 대한 태그 동기화를 생성합니다. 태그 동기화가 활성화되면 지정된 태그 키-값 페어로 태그가 지정된 모든 리소스가 애플리케이션에 자동으로 추가됩니다. 태그 동기화 오류 해결에 대한 자세한 내용은 the section called “myApplications의 태그 동기화 오류 해결” 섹션을 참조하세요.

> **Note**
>
> 태그를 사용하여 애플리케이션에 리소스를 추가하려면 AppRegistry 애플리케이션을 생성하고, 리소스를 그룹화 및 그룹화 해제하고, 리소스에 태그를 지정 및 해제할 수 있는 권한이 필요합니다. Resource Groups `ResourceGroupsTaggingAPITagUntagSupportedResources` AWS 관리형 정책을 추가하거나 자체 사용자 지정 정책을 생성하고 유지 관리할 수 있습니다. 다음 권한이 IAM의 사용자 정책 문에 추가되어야 합니다.
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

기존 태그를 사용하여 리소스를 추가하려면

1. 태그를 사용하여 자동으로 리소스 추가를 선택합니다.
2. 기존 태그 키 및 값을 선택합니다.
   a. 리소스에 태그를 지정하는 데 사용되는 역할을 선택합니다. 자세한 내용은 AWS Service Catalog AppRegistry 관리자 안내서의 태그 동기화에 필요한 권한을 참조하세요.
   b. 태그 키를 선택합니다.
   c. 태그 값을 선택합니다.
   d. (선택 사항) 리소스 미리 보기를 선택하여 태그 키-값 페어로 태그가 지정된 리소스를 미리 봅니다.
   e. 태그 동기화를 생성하기 위해 그룹 수명 주기 이벤트가 활성화된다는 것을 인식함을 검토하고 동의합니다. GLE를 사용하면 AWS 가 키-값 페어로 태그가 지정된 리소스의 변경 사항을 확인할 수 있습니다.
3. 다음을 선택합니다.
4. 애플리케이션 세부 정보, 선택한 태그 키-값 페어, 애플리케이션에 추가할 리소스의 미리 보기를 검토합니다.

> **Note**
>
> 기본적으로 기존 태그 키-값 페어를 사용하여 애플리케이션을 생성하면 태그 동기화가 생성됩니다. 또한 설정 후 태그 동기화는 지정된 키-값 페어로 태그가 지정되거나 지정 해제된 리소스를 추가하거나 제거하며 애플리케이션 리소스를 지속적으로 관리합니다. 애플리케이션의 리소스 관리 페이지에서 태그 동기화를 관리할 수 있습니다.

10. CloudFormation 스택을 연결하는 경우 페이지 하단의 확인란을 선택합니다.

> **Note**
>
> 애플리케이션에 CloudFormation 스택을 추가하려면 스택 업데이트가 필요합니다. 애플리케이션에 추가된 모든 리소스에 AWS 애플리케이션 태그가 지정되기 때문입니다. 스택이 마지막으로 업데이트된 이후에 수행된 수동 구성은 이 업데이트 후에 반영되지 않을 수 있습니다. 따라서 다운타임이나 기타 애플리케이션 문제가 발생할 수 있습니다. 자세한 정보는CloudFormation 사용 설명서의 스택 리소스의 업데이트 동작을 참조하세요.

11. 애플리케이션 생성을 선택합니다.

myApplications의 기존 AppRegistry 애플리케이션 온보딩

myApplications를 시작하려면 2023년 11월 8일 이전에 생성된 기존 AppRegistry 애플리케이션을 온보딩합니다.

기존 AppRegistry 애플리케이션을 온보딩하려면

1. AWS Management Console에 로그인합니다.
2. 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 검색 창을 사용하여 애플리케이션을 찾습니다.
4. 애플리케이션을 선택합니다.
5. ****** ## 온보딩을 선택합니다.
6. CloudFormation 스택을 연결하는 경우 알림 상자에서 확인란을 선택합니다.
7. 애플리케이션 온보딩을 선택합니다.

myApplications의 애플리케이션 보기

myApplications 또는 서비스 메뉴에서 애플리케이션을 볼 수 있습니다. myApplications에서 애플리케이션을 보는 경우 카드 AWS 리전 또는 테이블 보기에서 모든 또는 특정 AWS 리전 및 관련 정보를 볼 수 있습니다.

> **Note**
>
> 즐겨찾기 메뉴에서 즐겨찾기에 추가된 애플리케이션을 볼 수도 있습니다. 자세한 내용은 의 즐겨찾기 AWS Management Console 단원을 참조하십시오.

myApplications

myApplications의 애플리케이션을 보려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.
2. 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 리전에서 현재 리전 또는 지원되는 리전을 선택합니다.
4. 특정 애플리케이션을 찾으려면 검색 창에 이름, 키워드 또는 설명을 입력합니다.
5. (선택 사항) 기본 보기는 카드 보기입니다. 애플리케이션 페이지를 사용자 지정하려면 다음을 수행합니다.
   a. 기어 모양 아이콘을 선택합니다.
   b. (선택 사항) 페이지 크기를 선택합니다.
   c. (선택 사항) 카드 보기 또는 테이블 보기를 선택합니다.
   d. (선택 사항) 페이지 크기를 선택합니다.
   e. (선택 사항) 테이블 보기를 사용하는 경우 테이블 보기의 속성을 선택합니다.
   f. (선택 사항) 표시되는 애플리케이션 속성과 나타나는 순서를 전환합니다.
   g. 확인을 선택합니다.

Services menu

서비스 메뉴에서 애플리케이션을 보려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.

2. 탐색 모음에서 서비스(:::)를 선택합니다.
3. 모든 애플리케이션을 선택하세요.
4. 애플리케이션을 선택합니다.
5. (선택 사항) 보기를 선택합니다.
6. (선택 사항) 필터를 선택합니다. 속성 또는 태그별로 리소스를 필터링할 수 있습니다. 자세한 내용은 AWS 리소스 탐색기 Resource Explorer 사용 설명서의 Resource Explorer에 대한 검색 쿼리 구문 참조를 참조하세요.
7. (선택 사항) 관련 서비스 콘솔에서 볼 리소스를 선택합니다.

> **Tip**
>
> 서비스(:::)를 선택하여 중단한 리소스를 계속 탐색할 수 있습니다. 적용된 검색 필터도 유지됩니다.

myApplications의 애플리케이션 편집

애플리케이션을 편집하면 AppRegistry가 열리고 설명을 업데이트할 수 있습니다. 또한 AppRegistry를 사용하여 애플리케이션의 태그와 속성 그룹을 편집할 수 있습니다.

애플리케이션을 편집하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 편집하려는 애플리케이션을 선택합니다.
4. myApplication 대시보드에서 작업을 선택한 다음 애플리케이션 편집을 선택합니다.
5. 애플리케이션 편집에서 애플리케이션의 설명, 태그 및 속성 그룹을 원하는 대로 변경합니다.

> **Note**
>
> 태그 및 속성 그룹 관리에 대한 자세한 내용은 AWS Service Catalog AppRegistry 관리자 안내서의 태그 관리 및 속성 그룹 편집을 참조하세요.

6. 업데이트를 선택합니다.

myApplications의 애플리케이션 삭제

더 이상 필요하지 않은 애플리케이션은 삭제할 수 있습니다. 애플리케이션을 삭제하기 전에 AWS 서비스에서 생성하지 않은 모든 관련 리소스 공유 및 속성 그룹을 제거해야 합니다.

> **Note**
>
> 애플리케이션을 삭제해도 리소스에는 영향을 주지 않습니다. AWS 애플리케이션 태그로 태그가 지정된 리소스는 태그가 지정된 상태로 유지됩니다.

애플리케이션을 삭제하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 삭제하려는 애플리케이션을 선택합니다.
4. myApplication 대시보드에서 작업을 선택합니다.
5. 애플리케이션 삭제를 선택합니다.
6. 삭제를 확인한 다음 삭제(Delete)를 선택합니다.

myApplications의 코드 스니펫 생성

myApplications는 모든 애플리케이션에 대한 코드 스니펫을 생성합니다. 코드 스니펫을 사용하면 코드형 인프라(IaC) 도구를 통해 새로 생성된 리소스를 애플리케이션에 자동으로 추가할 수 있습니다. 추가된 모든 리소스에는 AWS 애플리케이션 태그가 지정되어 애플리케이션과 연결됩니다.

애플리케이션에 대한 코드 스니펫을 생성하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 애플리케이션을 검색하고 선택합니다.
4. 작업을 선택합니다.
5. 코드 스니펫 받기를 선택합니다.
6. 코드 스니펫 유형을 선택합니다.
7. 복사를 선택하여 코드를 클립보드로 복사합니다.
8. 코드를 IaC 도구에 붙여 넣습니다.

myApplications의 리소스

에서 AWS리소스는 작업할 수 있는 엔터티입니다. 예를 들어 Amazon EC2 인스턴스, AWS CloudFormation 스택 또는 Amazon S3 버킷이 있습니다. 애플리케이션에서 리소스를 추가하고 제거하여 myApplications의 리소스를 관리할 수 있습니다.

주제

myApplications의 리소스 추가

애플리케이션에 리소스를 추가하면 리소스를 그룹화하고 보안, 성능 및 규정 준수를 관리할 수 있습니다. 리소스를 검색하여 선택하거나 기존 태그를 사용하고 태그 동기화를 수행하여 기존 애플리케이션에 리소스를 추가할 수 있습니다.

Search and select resources

리소스를 검색하고 선택하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 애플리케이션을 검색하고 선택합니다.
4. 리소스 관리를 선택합니다.
5. 리소스 추가(Add resources)를 선택합니다.
6. (선택 사항) 보기를 선택합니다.
7. 리소스를 검색합니다. 키워드, 이름 또는 유형별로 검색하거나 리소스 유형을 선택할 수 있습니다.

> **Note**
>
> 찾고 있는 리소스를 찾을 수 없는 경우 문제를 해결합니다 AWS 리소스 탐색기. 자세한 내용은 Resource Explorer User Guide의 Troubleshooting Resource Explorer search issues를 참조하세요.

8. 추가할 리소스 옆에 있는 확인란을 선택합니다.
9. 추가를 선택합니다.

Automatically add resources using tags

애플리케이션을 생성할 때 기존 태그 키-값 페어를 지정하여 대량 온보드 리소스를 만들 수 있습니다. 이 방법을 사용하면가 모든 리소스에 `awsApplication` 태그를 AWS 자동으로 적용하고 기본적으로 애플리케이션 리소스에 대한 태그 동기화를 생성합니다. 태그 동기화가 활성화되면 지정된 태그 키-값 페어로 태그가 지정된 모든 리소스가 애플리케이션에 자동으로 추가됩니다.

기존 태그를 사용하여 리소스를 추가하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 리소스 관리를 선택합니다.
4. 태그 동기화 생성을 선택합니다.
5. 기존 태그 키 및 값을 선택합니다.
   a. 리소스에 태그를 지정하는 데 사용되는 역할을 선택합니다. 자세한 내용은 AWS Service Catalog AppRegistry 관리자 안내서의 태그 동기화 태스크에 필요한 권한을 참조하세요.
   b. 태그 키를 선택합니다.
   c. 태그 값을 선택합니다.
   d. 태그 동기화를 생성하기 위해 그룹 수명 주기 이벤트가 활성화된다는 것을 인식함을 검토하고 동의합니다. GLE를 사용하면 AWS 가 키-값 페어로 태그가 지정된 리소스의 변경 사항을 확인할 수 있습니다.
6. 태그 동기화 생성을 선택합니다.

myApplications의 태그 동기화 오류 해결

이 섹션에서는 일반적인 태그 동기화 오류와 이를 해결하는 방법을 설명합니다. 오류를 해결하려고 시도한 후 실패한 태그 동기화 작업을 다시 시도할 수 있습니다.

- 불충분한 권한 - 태그 동기화를 시작, 업데이트 또는 취소하는 데 필요한 최소 권한이 없습니다. 자세한 내용은 태그 동기화에 필요한 권한을 검토하세요. 태그 동기화를 수행하도록 지정한 역할에 필요한 최소 권한이 있는지 확인한 후 실패한 태그 동기화 작업을 다시 시도합니다.

- 이미 있음 - 이 애플리케이션에 대해 이 태그 키-값 페어가 있는 작업이 이미 존재합니다. 애플리케이션은 둘 이상의 태그 동기화를 지원할 수 있지만 각 태그 동기화에는 서로 다른 태그 키-값 페어가 있어야 합니다. 다른 태그 키-값 페어를 지정한 후 실패한 태그-동기화 작업을 다시 시도합니다.
- 최대 한도 도달 - 모든 애플리케이션에서 계정당 최대 한도인 100개의 태그 동기화 작업에 도달했습니다.

myApplications의 리소스 제거

리소스를 제거하여 애플리케이션에서 리소스 연결을 해제할 수 있습니다.

리소스를 제거하려면

1. AWS Management Console을 엽니다.
2. 콘솔의 왼쪽 사이드바에서 myApplications를 선택합니다.
3. 애플리케이션을 검색하고 선택합니다.
4. 리소스 관리를 선택합니다.
5. (선택 사항) 보기를 선택합니다.
6. 리소스를 검색합니다. 키워드, 이름 또는 유형별로 검색하거나 리소스 유형을 선택할 수 있습니다.

> **Note**
>
> 찾고 있는 리소스를 찾을 수 없는 경우 문제를 해결합니다 AWS 리소스 탐색기. 자세한 내용은 Resource Explorer User Guide의 Troubleshooting Resource Explorer search issues를 참조하세요.

7. 제거를 선택합니다.
8. 리소스 제거를 선택하여 리소스를 제거하려고 함을 확인합니다.

myApplications의 리소스 보기

myApplications 및 서비스 메뉴에서 애플리케이션 리소스를 볼 수 있습니다.

myApplications

myApplications에서 리소스를 보려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.

2. 왼쪽 사이드바를 확장하여 myApplications를 선택합니다.
3. 애플리케이션을 선택합니다.
4. 리소스 위젯에서 리소스를 확인합니다.

Services menu

서비스 메뉴에서 애플리케이션을 보려면 다음을 수행합니다.

1. AWS Management Console을 엽니다.
2. 탐색 모음에서 서비스(:::)를 선택합니다.
3. 모든 애플리케이션을 선택하세요.
4. 애플리케이션을 선택합니다.
5. (선택 사항) 보기를 선택합니다.
6. (선택 사항) 필터를 선택합니다. 속성 또는 태그별로 리소스를 필터링할 수 있습니다. 자세한 내용은 AWS 리소스 탐색기 Resource Explorer 사용 설명서의 Resource Explorer에 대한 검색 쿼리 구문 참조를 참조하세요.
7. (선택 사항) 관련 서비스 콘솔에서 볼 리소스를 선택합니다.

> **Tip**
>
> 서비스(:::)를 선택하여 중단한 리소스를 계속 탐색할 수 있습니다. 적용된 검색 필터도 유지됩니다.

의 myApplications 대시보드 AWS Console Home

생성하거나 온보딩하는 각 애플리케이션에는 고유한 myApplications 대시보드가 있습니다. myApplications 대시보드에는 여러 AWS 서비스의 인사이트를 표시하는 비용, 보안 및 운영 위젯이 포함되어 있습니다. 또한 각 위젯은 즐겨찾기에 추가하거나, 재정렬하거나, 제거하거나, 크기를 조정할 수 있습니다. 자세한 내용은 에서 위젯 작업 AWS Console Home 단원을 참조하십시오.

주제

- 애플리케이션 대시보드 설정 위젯
- 애플리케이션 요약 위젯
- 컴퓨팅 위젯

- 비용 및 사용량 위젯
- AWS 보안 위젯
- AWS 복원력 위젯
- 리소스 위젯
- DevOps 위젯
- 모니터링 및 운영 위젯
- 태그 위젯

애플리케이션 대시보드 설정 위젯

이 위젯에는 애플리케이션 리소스 관리를 AWS 서비스 위해를 구성하는 데 사용할 수 있는 권장 시작 활동 목록이 포함되어 있습니다.

애플리케이션 요약 위젯

이 위젯은 애플리케이션의 이름, 설명, AWS 애플리케이션 태그를 보여줍니다. 코드형 인프라(IAC)에서 애플리케이션 태그를 액세스하고 복사하여 리소스에 수동으로 태그를 지정할 수 있습니다.

컴퓨팅 위젯

이 위젯은 애플리케이션에 추가하는 컴퓨팅 리소스에 대한 정보와 지표를 표시합니다. 여기에는 총 경보 수 및 총 컴퓨팅 리소스 유형 수가 포함됩니다. 위젯에는 Amazon EC2 인스턴스 CPU 사용률 및 Lambda 호출에 Amazon CloudWatch 대한의 리소스 성능 지표 추세 차트도 표시됩니다.

컴퓨팅 위젯 구성

컴퓨팅 위젯에 데이터를 채우려면 애플리케이션에 대해 하나 이상의 Amazon EC2 인스턴스 또는 Lambda 함수를 설정합니다. 자세한 내용은 AWS Lambda 개발자 안내서의 Amazon Elastic Compute 클라우드 문서 및 Lambda 시작하기를 참조하세요.

비용 및 사용량 위젯

이 위젯은 애플리케이션 리소스의 AWS 비용 및 사용량 데이터를 보여줍니다. 이 데이터를 사용하여 월별 비용을 비교하고 AWS 서비스별 비용을 볼 수 있습니다. 이 위젯은 리소스와 직접 연결되지 않은 세금, 수수료 및 기타 공유 비용을 제외하고 AWS 애플리케이션 태그로 태그가 지정된 리소스에 대한 비용만 요약합니다. 표시된 비용은 일반 비용이며 24시간마다 최소 1회 이상 업데이트됩니다. 자세한

내용은 AWS Cost Management 사용 설명서의 AWS 리소스 탐색기를 사용한 비용 분석을 참조하세요.

비용 및 사용량 위젯 구성

비용 및 사용량 위젯을 구성하려면 애플리케이션 및 계정에 AWS Cost Explorer Service 대해를 활성화합니다. 이 서비스는 추가 비용 없이 제공되며 설정 비용이나 사전 약정이 없습니다. 자세한 내용은 AWS Cost Management 사용 설명서의 Cost Explorer 활성화를 참조하세요.

AWS 보안 위젯

이 위젯은 애플리케이션에 대한 AWS 보안 조사 결과를 표시합니다. AWS 보안은의 애플리케이션에 대한 보안 조사 결과를 포괄적으로 보여줍니다 AWS. 심각도별로 최근 우선순위 조사 결과에 액세스하고, 보안 태세를 모니터링하고, 중요하거나 심각도가 높은 최근 조사 결과에 액세스하고, 다음 단계를 위한 인사이트를 얻을 수 있습니다. 자세한 내용은 AWS Security Hub CSPM 단원을 참조하십시오.

AWS 보안 위젯 구성

AWS 보안 위젯을 구성하려면 애플리케이션 및 계정에 AWS Security Hub CSPM 맞게를 설정합니다. 자세한 내용은 AWS Security Hub CSPM 사용 설명서의 What is AWS Security Hub CSPM?를 참조하세요. 요금 정보는 AWS Security Hub CSPM 사용 설명서의 AWS Security Hub CSPM 무료 평가판, 사용량 및 가격을 참조하세요.

AWS Security Hub CSPM 에서는 AWS Config Recording을 구성해야 합니다. 이 서비스는 AWS 계정과 연결된 리소스에 대한 세부 보기를 제공합니다. 자세한 내용은AWS Systems Manager 사용 설명서의 AWS Systems Manager를 참조하세요.

AWS 복원력 위젯

이 위젯은 애플리케이션에 대한 AWS Resilience Hub의 복원력 세부 정보를 표시합니다. 평가를 시작한 후 AWS Resiliency Hub는 미리 정의된 복원력 정책을 기준으로 리소스를 평가하여 애플리케이션의 복원력 상태를 분석합니다. 복원력 점수, 정책 위반, 정책 드리프트, 리소스 드리프트 및 복원력 점수 이력 같은 지표에 접근할 수 있습니다. 향상된 추적을 위해 애플리케이션이 매일 평가되지만 언제든지 이 기능을 비활성화할 수 있습니다. 자세한 내용은 AWS Resilience Hub 단원을 참조하십시오. 요금 정보는 AWS Resilience Hub 요금을 참조하세요.

AWS 복원력 위젯 구성

AWS 복원력 위젯을 구성하려면 애플리케이션을 추가합니다. 자세한 내용은 AWS Resilience Hub 사용 설명서의 What is AWS Resilience Hub?를 참조하세요.

리소스 위젯

이 위젯은 AWS Resource Explorer를 사용하여 뷰 내에서 애플리케이션에 추가한 리소스를 표시합니다. 이 위젯을 사용하여 이름, 태그, ID와 같은 리소스 메타데이터로 리소스를 검색하거나 필터링할 수 있습니다. 자세한 내용은 AWS Resource Explorer를 참조하세요.

리소스 위젯 구성

리소스 위젯을 구성하려면 Resource Explorer를 온보딩합니다. 자세한 내용은 AWS Resource Explorer 사용 설명서의 Resource Explorer 시작하기를 참조하세요.

DevOps 위젯

이 위젯은 운영 인사이트를 보여주므로 규정 준수를 평가하고 애플리케이션에 대한 조치를 취할 수 있습니다. 이러한 인사이트에는 다음이 포함됩니다.

- 집합 관리
- 상태 관리
- 패치 관리
- 구성 및 OpsItems 관리

DevOps 위젯 구성

DevOps 위젯을 구성하려면 애플리케이션 및 계정에 대해 AWS Systems Manager OpsCenter를 활성화합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 Systems Manager Explorer 및 OpsCenter 시작하기를 참조하세요. OpsCenter를 활성화하면가 AWS Config 및 AWS Systems Manager Explorer 를 구성 Amazon CloudWatch 하여 이벤트가 일반적으로 사용되는 규칙 및 이벤트를 기반으로 OpsItems 자동으로 생성할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 OpsCenter 설정을 참조하세요.

Systems Manager 에이전트가 실행되도록 인스턴스를 구성하고 권한을 적용하여 패치 스캔을 활성화할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Systems Manager 빠른 설정을 참조하세요.

패치 관리자를 설정하여 애플리케이션에 대한 Amazon EC2 인스턴스의 자동 AWS Systems Manager 패치를 설정할 수도 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 빠른 설정 패치 정책 사용을 참조하세요.

요금 정보는 AWS Systems Manager 요금을 참조하세요.

모니터링 및 운영 위젯

이 위젯은 다음을 보여줍니다.

- 애플리케이션과 관련된 리소스에 대한 경보 및 알림
- 애플리케이션 서비스 수준 목표(SLO) 및 지표
- 사용 가능한 AWS Application Signals 지표

모니터링 및 운영 위젯 구성

모니터링 및 작업 위젯을 구성하려면 AWS 계정에서 CloudWatch 경보 및 canary를 생성합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 경보 사용 및 canary 생성을 참조하세요. CloudWatch 경보 및 가상 canary 요금에 대해서는 각각 Amazon CloudWatch 요금 및 AWS Cloud Operations and Migrations Blog를 참조하세요.

CloudWatch Application Signals에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch Application Signals 활성화를 참조하세요.

태그 위젯

이 위젯은 애플리케이션과 관련된 모든 태그를 표시합니다. 이 위젯을 사용하여 애플리케이션 메타데이터(중요도, 환경, 비용 센터)를 추적하고 관리할 수 있습니다. 자세한 내용은 리소스 태그 지정 모범 사례 백서의 태그란 무엇입니까?를 참조하세요. AWS AWS

AWS Console Home에서 Amazon Q Developer와 채팅

Amazon Q Developer는 AWS 애플리케이션을 이해하고, 구축하고, 확장하고, 운영하는 데 도움을 줄 수 있는 생성형 인공 지능(AI) 기반 대화형 어시스턴트입니다. AWS 아키텍처, AWS 리소스, 모범 사례, 설명서 등에 대한 질문을 포함하여 AWS 관련 모든 질문을 Amazon Q에 할 수 있습니다. 지원 사례를 생성하고 라이브 에이전트로부터 지원을 받을 수도 있습니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 Amazon Q란 무엇인가요?를 참조하세요.

Amazon Q 시작하기

AWS Management Console, AWS 설명서 웹사이트, AWS 웹사이트 또는 AWS Console 모바일 애플리케이션에서 육각형 Amazon Q 아이콘을 선택하여 Amazon Q와 채팅을 시작할 수 있습니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 Amazon Q Developer 시작하기를 참조하세요.

예시 질문

다음은 Amazon Q에 물어볼 수 있는 몇 가지 예시 질문입니다.

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

AWS Management Console 프라이빗 액세스

AWS Management Console 프라이빗 액세스는에 대한 액세스를 제어하는 고급 보안 기능입니다 AWS Management Console. 콘솔 프라이빗 액세스는 사용자가 네트워크 내에서 예기치 못한 AWS 계정 에 로그인하지 못하게 하려는 경우 유용합니다. 이 기능을 사용하면 트래픽이 네트워크 내에서 시작될 AWS 계정 때 알려진 지정된 집합으로 AWS Management Console 만에 대한 액세스를 제한할 수 있습니다. 콘솔 프라이빗 액세스는의 AWS 서비스 모든 호출이 네트워크 내부 및 허용된 계정에서 AWS Management Console 시작되도록 하려는 경우에도 유용합니다.

주제

지원되는 AWS 리전서비스 콘솔 및 프라이빗 액세스 기능

AWS Management Console 프라이빗 액세스는 리전 및 AWS 서비스의 하위 집합만 지원합니다. 지원되지 않는 서비스 콘솔은 AWS Management Console에서 비활성화됩니다. 또한 통합 설정의 기본 리전 선택과 같이 AWS Management Console 프라이빗 액세스를 사용할 때 특정 AWS Management Console 기능이 비활성화될 수 있습니다.

지원되는 리전 및 서비스 콘솔은 아래와 같습니다.

지원되는 리전:

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(뭄바이)

- 아시아 태평양(서울)
- 아시아 태평양(오사카)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(말레이시아)
- 아시아 태평양(태국)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(파리)
- 유럽(스톡홀름)
- 남아메리카(상파울루)
- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 캐나다 서부(캘거리)
- 멕시코(중부)
- 유럽(밀라노)
- 유럽(스페인)
- 유럽(취리히)
- Middle East (Bahrain)
- 중동(UAE)
- 이스라엘(텔아비브)

지원되는 서비스 콘솔

- Amazon API Gateway
- AWS App Mesh

- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS 결제 및 비용 관리
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer

- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service:
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- Amazon GameLift Servers
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector –
- Amazon Kendra
- AWS Key Management Service

- Amazon Kinesis
- Amazon Managed Service for Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow(MWAA)
- AWS Migration Hub 전략 권장 사항
- Amazon MQ
- Network Access Analyzer
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service
- AWS Organizations
- AWS Private Certificate Authority
- Public Health Dashboard
- Amazon Rekognition
- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups 및 태그 편집기
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver DNS 방화벽
- Outposts에서의 Amazon S3
- Amazon SageMaker
- Amazon SageMaker 런타임

- Amazon SageMaker AI Synthetic Data
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service(Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- 지원
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- 통합 설정
- Amazon VPC IP 주소 관리자
- Amazon Virtual Private Cloud
- Amazon WorkSpaces Thin Client

AWS Management Console 프라이빗 액세스 보안 제어 개요

AWS Management Console 네트워크의에 대한 계정 제한

AWS Management Console 프라이빗 액세스는 AWS Management Console 네트워크에서 조직에 알려진 지정된 집합으로만에 대한 액세스를 제한하려는 시나리오 AWS 계정 에서 유용합니다. 이렇게 하면 사용자가 네트워크 내에서 예기치 못한 AWS 계정 에 로그인하는 것을 방지할 수 있습니다. AWS Management Console VPC 엔드포인트 정책을 사용하여 이러한 제어를 구현할 수 있습니다. 자세한 내용은 서비스 제어 정책 및 VPC 엔드포인트 정책 구현 단원을 참조하십시오.

네트워크에서 인터넷으로 연결

정적 콘텐츠(JavaScript AWS Management Console, CSS, 이미지)와 같이에서 사용하는 자산과에서 활성화 AWS 서비스 하지 않은 모든 자산에 액세스하려면 네트워크의 인터넷 연결이 여전히 필요합니다AWS PrivateLink. 에서 사용하는 최상위 도메인 목록은 섹션을 AWS Management Console참조하세요문제 해결.

> **Note**
>
> 현재 AWS Management Console 프라이빗 액세스는 , `health.aws.amazon.com`및와 같은 엔드포인트`status.aws.amazon.com`를 지원하지 않습니다`docs.aws.amazon.com`. 이러한 도메인을 공용 인터넷으로 라우팅해야 합니다.

필수 VPC 엔드포인트 및 DNS 구성

AWS Management Console 프라이빗 액세스에는 리전당 다음 두 개의 VPC 엔드포인트가 필요합니다. *`region`*을 현재의 해당하는 리전 정보로 바꿉니다.

1. 에 대한 com.amazonaws.*`region`*.console AWS Management Console
2. 에 대한 com.amazonaws.*`region`*.signin AWS 로그인

> **Note**
>
> AWS Management Console과 함께 사용하는 기타 리전과 상관없이, 인프라 및 네트워킹 연결을 항상 미국 동부(버지니아 북부)(us-east-1) 리전으로 프로비저닝합니다. AWS Transit Gateway 를 사용하여 미국 동부(버지니아 북부) 리전과 다른 모든 리전 간의 연결을 설정할 수 있습니다. 자세한 내용은 Amazon VPC Transit Gateway 가이드의 전송 게이트웨이 시작하기를 참조하세요. Amazon VPC 피어링도 사용할 수 있습니다. 자세한 내용은 Amazon VPC Peering Guide의 VPC 피어링이란?을 참조하세요. 이러한 옵션을 비교하려면 Amazon Virtual Private Cloud(VPC) 연결 옵션 백서에서 Amazon VPC 간 연결 옵션을 참조하세요.

주제

- DNS AWS Management Console 및에 대한 구성 AWS 로그인
- 의 AWS 서비스에 대한 VPC 엔드포인트 및 DNS 구성 AWS Management Console

DNS AWS Management Console 및에 대한 구성 AWS 로그인

네트워크 트래픽을 각 VPC 엔드포인트로 라우팅하려면 사용자가 AWS Management Console에 액세스할 네트워크에서 DNS 레코드를 구성하세요. 이러한 DNS 레코드는 사용자의 브라우저 트래픽을 생성된 VPC 엔드포인트로 이동합니다.

단일 호스팅 영역을 생성할 수 있습니다. 그러나 `health.aws.amazon.com` 및 `docs.aws.amazon.com`과 같은 엔드포인트는 VPC 엔드포인트가 없으므로 액세스할 수 없습니다. 이러한 도메인을 공용 인터넷으로 라우팅해야 합니다. 다음 CNAME 레코드를 사용하여 리전별로 `signin.aws.amazon.com`용과 `console.aws.amazon.com`용으로 각각 하나씩 두 개의 프라이빗 호스팅 영역을 생성하는 것이 좋습니다.

- 로그인
  - *`region`*.signin.aws.amazon.com 리전이 원하는 *`##`*인 로그인 DNS 영역의 AWS 로그인 VPC 엔드포인트를 가리킵니다.
  - 미국 동부(버지니아 북부)의 AWS 로그인 VPC 엔드포인트를 가리키는 signin.aws.amazon.com(us-east-1)
- 콘솔
  - *`region`*.console.aws.amazon.com - *`##`*이 원하는 리전인 콘솔 DNS 영역의 AWS Management Console VPC 엔드포인트를 가리킵니다.
  - *.*`region`*.console.aws.amazon.com 리전이 원하는 *`##`*인 콘솔 DNS 영역의 AWS Management Console VPC 엔드포인트를 가리킵니다.
  - 콘솔 DNS 영역의 AWS Management Console VPC 엔드포인트를 가리키는 *.*`region`*.console.aws.amazon.com
  - 리전이 없는 CNAME 레코드는 미국 동부(버지니아 북부) 리전에서만 사용할 수 있습니다. 항상 미국 동부(버지니아 북부) 리전을 설정해야 합니다.
    - 미국 동부(버지니아 북부)(us-east-1)의 AWS 로그인 VPC 엔드포인트를 가리키는 signin.aws.amazon.com
    - *.console.aws.amazon.com 미국 동부(버지니아 북부)(us-east-1)의 AWS Management Console VPC 엔드포인트를 가리킵니다.

  CNAME 레코드 생성에 대한 지침은 Amazon Route 53 개발자 안내서의 레코드 작업을 참조하세요.

  Amazon S3를 포함한 일부 AWS 콘솔은 DNS 이름에 다른 패턴을 사용합니다. 다음은 두 가지 예제입니다.

  - support.console.aws.amazon.com

- s3.console.aws.amazon.com

이 트래픽을 AWS Management Console VPC 엔드포인트로 전달하려면 해당 이름을 개별적으로 추가해야 합니다. 완전한 프라이빗 환경을 위해 모든 엔드포인트에 대해 라우팅을 구성하는 것이 좋습니다. 하지만 AWS Management Console 프라이빗 액세스를 사용하는 데는 필요하지 않습니다.

다음 `json` 파일에는 리전별로 구성할 AWS 서비스및 콘솔 엔드포인트의 전체 목록이 포함되어 있습니다. DNS 이름의 `com.amazonaws.`*`region`*`.console` 엔드포인트 아래에 있는 `PrivateIpv4DnsNames` 필드를 사용하세요.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> AWS Management Console 프라이빗 액세스 범위에 엔드포인트가 수시로 추가되므로 이 목록은 매달 업데이트됩니다. 프라이빗 호스팅 영역을 최신 상태로 유지하려면 이전 파일 목록을 주기적으로 가져오세요.

Route 53을 사용하여 DNS를 구성할 경우 https://console.aws.amazon.com/route53/v2/hostedzones#로 이동하여 DNS 설정을 확인하세요. Route 53의 각 프라이빗 호스팅 영역에 대해 다음과 같은 레코드 세트가 있는지 확인합니다.

- console.aws.amazon.com
- signin.aws.amazon.com
- *.*region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *.*region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- 이전에 목록에 등록된 JSON 파일에 있는 추가 레코드

의 AWS 서비스에 대한 VPC 엔드포인트 및 DNS 구성 AWS Management Console

직접 브라우저 요청과 웹 서버에서 프록시되는 요청의 조합을 AWS 서비스 통한 AWS Management Console 호출입니다. 이 트래픽을 AWS Management Console VPC 엔드포인트로 전달하려면 VPC 엔드포인트를 추가하고 각 종속 AWS 서비스에 DNS 대해를 구성해야 합니다.

다음 json 파일에는 사용할 수 있는 AWS PrivateLink 지원되는 AWS 서비스 가 나열되어 있습니다. 서비스가와 통합되지 않으면 이러한 파일에 포함되지 AWS PrivateLink않습니다.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

해당하는 서비스의 VPC 엔드포인트에 대한 `ServiceName` 필드를 사용하여 VPC에 추가합니다.

> **Note**
>
> 이 목록은 더 많은 서비스 콘솔에 AWS Management Console 프라이빗 액세스에 대한 지원을 추가함에 따라 매달 업데이트됩니다. 최신 상태를 유지하려면 이전 파일 목록을 주기적으로 가져와서 VPC 엔드포인트를 업데이트하세요.

서비스 제어 정책 및 VPC 엔드포인트 정책 구현

프라이빗 액세스에 대한 AWS Management Console 서비스 제어 정책(SCPs) 및 VPC 엔드포인트 정책을 사용하여 VPC 및 연결된 온프레미스 네트워크 AWS Management Console 내에서를 사용할 수 있는 계정 세트를 제한할 수 있습니다.

주제

- AWS Organizations 서비스 제어 정책과 함께 AWS Management Console 프라이빗 액세스 사용
- 예상 계정 및 조직에 대해서만 AWS Management Console 사용 허용(신뢰할 수 있는 자격 증명)

AWS Organizations 서비스 제어 정책과 함께 AWS Management Console 프라이빗 액세스 사용

AWS 조직에서 특정 서비스를 허용하는 서비스 제어 정책(SCP)을 사용하는 경우 허용된 작업에 `signin:*`를 추가해야 합니다. 프라이빗 액세스 VPC 엔드포인트를 AWS Management Console 통해에 로그인하면 SCP가 권한 없이 차단하는 IAM 권한이 수행되므로이 권한이 필요합니다. 예를 들어 다음 서비스 제어 정책은 AWS Management Console 프라이빗 액세스 엔드포인트를 사용하여 액세스하는 경우를 포함하여 조직에서 Amazon EC2 및 CloudWatch 서비스를 사용하도록 허용합니다.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 서비스 제어 정책(SCP)을 참조하세요.

예상 계정 및 조직에 대해서만 AWS Management Console 사용 허용(신뢰할 수 있는 자격 증명)

AWS Management Console 및는 로그인한 계정의 자격 증명을 특별히 제어하는 VPC 엔드포인트 정책을 AWS 로그인 지원합니다.

다른 VPC 엔드포인트 정책과 달리, 이 정책은 인증 전에 평가됩니다. 따라서 인증된 세션의 로그인 및 사용만 제어하고 세션이 수행하는 AWS 서비스별 작업은 제어하지 않습니다. 예를 들어 세션이 Amazon EC2 콘솔과 같은 AWS 서비스 콘솔에 액세스할 때 이러한 VPC 엔드포인트 정책은 해당 페이지를 표시하기 위해 수행된 Amazon EC2 작업에 대해 평가되지 않습니다. 대신 로그인한 IAM 보안 주체와 연결된 IAM 정책을 사용하여 AWS 서비스 작업에 대한 권한을 제어할 수 있습니다.

> **Note**
>
> AWS Management Console 및 SignIn VPC 엔드포인트에 대한 VPC 엔드포인트 정책은 제한된 정책 구성 하위 집합만 지원합니다. 모든 `Principal` 및 `Resource`는 `*`로 설정해야 하며 `Action`은 `*` 또는 `signin:*` 중 하나여야 합니다. `aws:PrincipalOrgId` 및 `aws:PrincipalAccount` 조건 키를 사용하여 VPC 엔드포인트에 대한 액세스를 제어할 수 있습니다.

콘솔 및 로그인 VPC 엔드포인트 양쪽 모두에 권장되는 정책은 다음과 같습니다.

이 VPC 엔드포인트 정책은 지정된 AWS 조직의 AWS 계정 에 대한 로그인을 허용하고 다른 계정에 대한 로그인을 차단합니다.

JSON

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

```
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

이 VPC 엔드포인트 정책은 특정 목록으로 로그인을 제한 AWS 계정 하고 다른 계정에 대한 로그인을 차단합니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

AWS Management Console 및 로그인 VPC 엔드포인트에서 AWS 계정 또는 조직을 제한하는 정책은 로그인 시 평가되며 기존 세션에 대해 주기적으로 재평가됩니다.

자격 증명 기반 정책 및 기타 정책 유형 구현

정책을 AWS 생성하고 IAM 자격 증명(사용자, 사용자 그룹 또는 역할) 또는 AWS 리소스에 연결하여에서 액세스를 관리합니다. 이 페이지에서는 AWS Management Console 프라이빗 액세스와 함께 사용할 때 정책이 작동하는 방식을 설명합니다.

지원되는 AWS 전역 조건 컨텍스트 키

AWS Management Console 프라이빗 액세스는 `aws:SourceVpce` 및 `aws:VpcSourceIp` AWS 전역 조건 컨텍스트 키를 지원하지 않습니다. AWS Management Console 프라이빗 액세스를 사용할 경우 정책에서 `aws:SourceVpc` IAM 조건을 대신 사용할 수 있습니다.

AWS Management Console 프라이빗 액세스가 aws:SourceVpc와 작동하는 방식

이 섹션에서는에서 생성된 요청이 수행할 AWS Management Console 수 있는 다양한 네트워크 경로를 설명합니다 AWS 서비스. 일반적으로 AWS 서비스 콘솔은 직접 브라우저 요청과 AWS Management Console 웹 서버가 프록시하는 요청을 혼합하여 구현됩니다 AWS 서비스. 이러한 구현은 사전 고지 없이 변경될 수 있습니다. 보안 요구 사항에 VPC 엔드포인트 AWS 서비스 사용에 대한 액세스가 포함된 경우 직접 또는 AWS Management Console 프라이빗 액세스를 통해 VPC에서 사용하려는 모든 서비스에 대해 VPC 엔드포인트를 구성하는 것이 좋습니다. 또한 AWS Management Console 프라이빗 액세스 기능과 함께 특정 `aws:SourceVpce` 값이 아닌 정책에서 `aws:SourceVpc` IAM 조건을 사용해야 합니다. 이 섹션에서는 다양한 네트워크 경로의 작동 방식에 대한 세부 정보를 제공합니다.

사용자가에 로그인하면 직접 브라우저 AWS Management Console요청과 AWS Management Console 웹 서버에서 AWS 서버로 프록시되는 요청의 조합을 AWS 서비스 통해에 요청합니다. 예를 들어, CloudWatch 그래프 데이터 요청이 브라우저에서 직접 이루어집니다. 반면 Amazon S3와 같은 일부 AWS 서비스 콘솔 요청은 웹 서버에서 Amazon S3로 프록시됩니다.

직접 브라우저 요청의 경우 AWS Management Console 프라이빗 액세스를 사용해도 아무것도 변경되지 않습니다. 이전과 마찬가지로, 요청은 VPC가 monitoring.region.amazonaws.com에 도달하도록 구성한 네트워크 경로를 통해 서비스에 도달합니다. VPC가 com.amazonaws.region.monitoring에 대한 VPC 엔드포인트로 구성된 경우, 요청은 해당 CloudWatch VPC 엔드포인트를 통해 CloudWatch에 도달합니다. CloudWatch에 대한 VPC 엔드포인트가 없는 경우, 요청은 VPC의 인터넷 게이트웨이를 통해 퍼블릭 엔드포인트에서 CloudWatch에 도달합니다. CloudWatch VPC 엔드포인트를 통해 CloudWatch에 도착한 요청은 IAM 조건인 `aws:SourceVpc` 및 `aws:SourceVpce`가 각각 해당하는 값으로 설정됩니다. 퍼블릭 엔드포인트를 통해 CloudWatch에 도달하는 요청은 `aws:SourceIp`가 요청의 소스 IP 주소로 설정됩니다. IAM 조건 키에 대한 자세한 정보는 IAM 사용 설명서의 전역 조건 키를 참조하세요.

Amazon S3 콘솔을 방문할 때 버킷을 나열하기 위해 Amazon S3 콘솔이 수행하는 요청과 같이 AWS Management Console 웹 서버에서 프록시되는 요청의 경우 Amazon S3 네트워크 경로는 다릅니다. 이러한 요청은 VPC에서 시작되지 않으므로 해당 서비스에 대해 VPC에 구성된 VPC 엔드포인트를

사용하지 않습니다. 이 경우 Amazon S3에 대한 VPC 엔드포인트가 있더라도, 버킷 목록을 나열해달라는 Amazon S3에 대한 세션의 요청은 Amazon S3 VPC 엔드포인트를 사용하지 않습니다. 그러나 지원되는 서비스와 함께 AWS Management Console 프라이빗 액세스를 사용하는 경우 이러한 요청(예: Amazon S3)은 요청 컨텍스트에 `aws:SourceVpc` 조건 키를 포함합니다. `aws:SourceVpc` 조건 키는 로그인 및 콘솔에 대한 AWS Management Console 프라이빗 액세스 엔드포인트가 배포되는 VPC ID로 설정됩니다. 따라서 자격 증명 기반 정책에서 `aws:SourceVpc` 제한을 사용할 경우, AWS Management Console 프라이빗 액세스 로그인과 콘솔 엔드포인트를 호스팅하는 이 VPC의 VPC ID를 추가해야 합니다. `aws:SourceVpce` 조건은 각각의 로그인 또는 콘솔 VPC 엔드포인트 ID로 설정됩니다.

> **Note**
>
> 사용자가 AWS Management Console 프라이빗 액세스에서 지원되지 않는 서비스 콘솔에 액세스해야 하는 경우, `aws:SourceIP` 조건 키를 사용하여 사용자의 ID 기반 정책에 예상 퍼블릭 네트워크 주소(예: 온프레미스 네트워크 범위) 목록을 포함해야 합니다.

다양한 네트워크 경로가 CloudTrail에 반영되는 방식

에서 생성된 요청에 사용되는 다양한 네트워크 경로 AWS Management Console 가 CloudTrail 이벤트 기록에 반영됩니다.

직접 브라우저 요청의 경우 AWS Management Console 프라이빗 액세스를 사용해도 아무 것도 변경되지 않습니다. CloudTrail 이벤트에는 서비스 API 호출에 사용된 VPC 엔드포인트 ID 등 연결에 대한 세부 정보가 포함됩니다.

AWS Management Console 웹 서버에서 프록시되는 요청의 경우 CloudTrail 이벤트에는 VPC 관련 세부 정보가 포함되지 않습니다. 그러나 `AwsConsoleSignIn` 이벤트 유형과 같은 브라우저 세션을 설정하는 데 AWS 로그인 필요한에 대한 초기 요청은 이벤트 세부 정보에 AWS 로그인 VPC 엔드포인트 ID를 포함합니다.

AWS Management Console 프라이빗 액세스 시도

이 섹션에서는 새 계정에서 AWS Management Console 프라이빗 액세스를 설정하고 테스트하는 방법을 설명합니다.

AWS Management Console 프라이빗 액세스는 고급 보안 기능이며 네트워킹 및 VPCs 필요합니다. 이번 주제에서는 대규모 인프라 없이 AWS Management Console 프라이빗 액세스를 사용해 볼 수 있는 방법을 설명합니다.

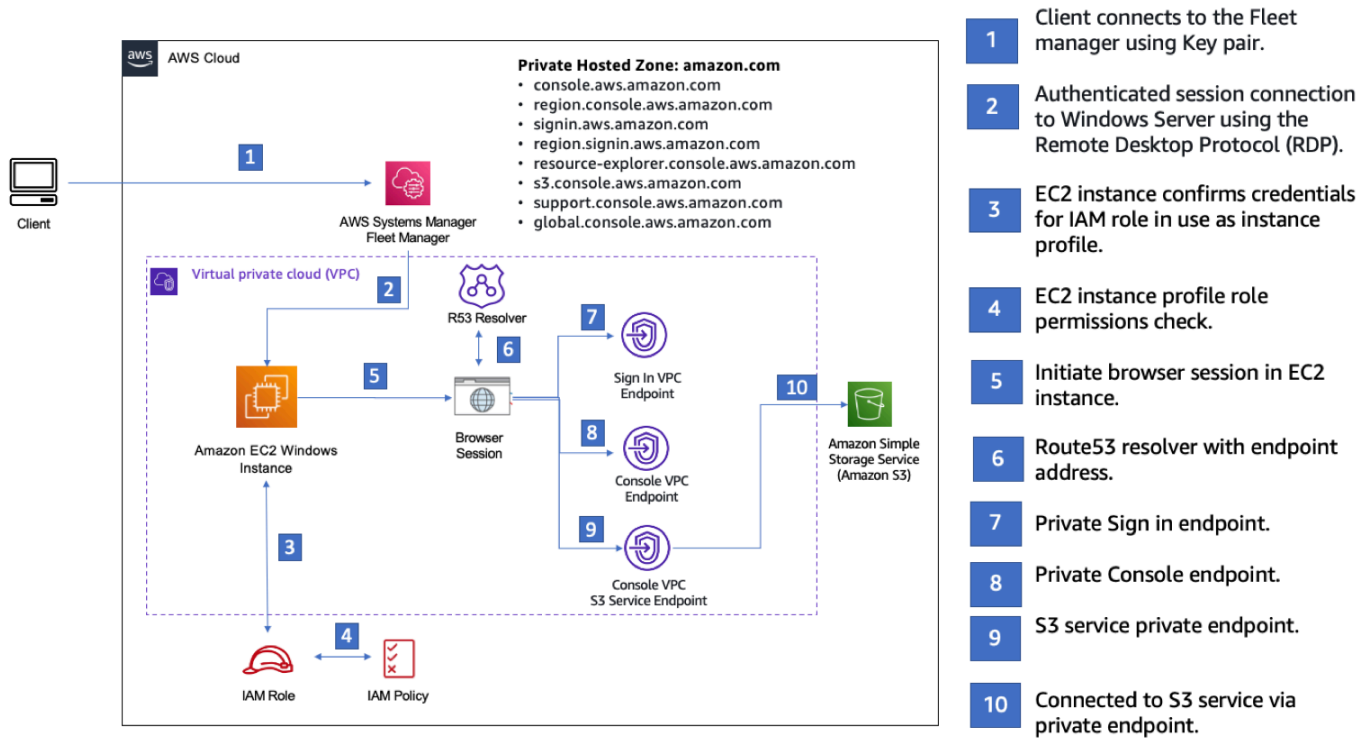
주제

Amazon EC2를 사용한 테스트 설정

Amazon Elastic Compute Cloud(Amazon EC2)는 Amazon Web Services 클라우드에서 확장 가능한 컴퓨팅 용량을 제공합니다. Amazon EC2를 사용하여 원하는 수의 가상 서버를 빌드하고 보안 및 네트워킹을 구성하며 스토리지를 관리할 수 있습니다. 이 설정에서는 AWS Systems Manager의 기능인 Fleet Manager를 사용하여 원격 데스크톱 프로토콜(RDP)을 사용하는 Amazon EC2 Windows 인스턴스에 연결합니다.

이 가이드는 Amazon EC2 인스턴스에서 Amazon Simple Storage Service에 대한 AWS Management Console 프라이빗 액세스 연결을 설정하고 경험하는 테스트 환경을 보여줍니다. 이 자습서에서는 CloudFormation 를 사용하여 Amazon EC2에서이 기능을 시각화하는 데 사용할 네트워크 설정을 생성하고 구성합니다.

아래의 다이어그램은 Amazon EC2를 사용하여 AWS Management Console 프라이빗 액세스 설정에 액세스하는 워크플로를 설명합니다. 여기에서는 사용자가 프라이빗 엔드포인트를 사용하여 Amazon S3에 연결하는 방법을 보여줍니다.



다음 CloudFormation 템플릿을 복사하여 네트워크 설정 절차의 3단계에서 사용할 파일에 저장합니다.

> **Note**
>
> 이 CloudFormation 템플릿은 현재 이스라엘(텔아비브) 리전에서 지원되지 않는 구성을 사용합니다.

AWS Management Console 프라이빗 액세스 환경 Amazon EC2 CloudFormation template

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance
```

```
  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't3.medium'


Resources:

##########################
# VPC AND SUBNETS
```

```
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  PrivateSubnetA:
```

```
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
```

```
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
```

```
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
```

```
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

########################
# VPC ENDPOINTS
########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
```

```
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

##########################
# ROUTE53 RESOURCES
##########################
```

```
 ConsoleHostedZone:
   Type: "AWS::Route53::HostedZone"
   Properties:
     HostedZoneConfig:
       Comment: 'Console VPC Endpoint Hosted Zone'
     Name: 'console.aws.amazon.com'
     VPCs:
       -
         VPCId: !Ref AppVPC
         VPCRegion: !Ref "AWS::Region"

 ConsoleRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 'console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 GlobalConsoleRecord:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 'global.console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleS3ProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 's3.console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 WidgetProxyRecord:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "*.widget.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
       HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
```

```
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

  Ec2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
       - !Ref Ec2InstanceRole

  EC2WinInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestWindowsAmiId
      IamInstanceProfile: !Ref Ec2InstanceProfile
```

```
      KeyName: !Ref Ec2KeyPair
      InstanceType:
        Ref: InstanceTypeParameter
      SubnetId: !Ref PrivateSubnetA
      SecurityGroupIds:
        - Ref: EC2SecurityGroup
      BlockDeviceMappings:
        - DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
      Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```

네트워크를 설정하려면

1. 조직의 관리 계정으로 로그인하고 CloudFormation 콘솔을 엽니다.
2. 스택 생성을 선택합니다.
3. 새 리소스 사용(표준)(With new resources (standard))을 선택합니다. 이전에 생성한 CloudFormation 템플릿 파일을 업로드하고 다음을 선택합니다.
4. **PrivateConsoleNetworkForS3** 같은 스택 이름을 입력한 후 다음을 선택합니다.
5. VPC 및 서브넷의 경우, 원하는 IP CIDR 범위를 입력하거나 제공된 기본값을 사용합니다. 기본값을 사용하는 경우 기본값이의 기존 VPC 리소스와 겹치지 않는지 확인합니다 AWS 계정.
6. EC2KeyPair 파라미터의 경우, 계정의 기존 Amazon EC2 키 페어 중에서 하나를 선택합니다. 기존 Amazon EC2 키 페어가 없다면 다음 단계로 진행하기 전에 이를 새로 생성해야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2를 사용하여 키 페어 생성을 참조하세요.
7. 스택 생성을 선택합니다.
8. 스택이 생성된 후 리소스 탭을 선택하여 생성된 리소스를 확인합니다.

Amazon EC2 인스턴스에 연결하려면

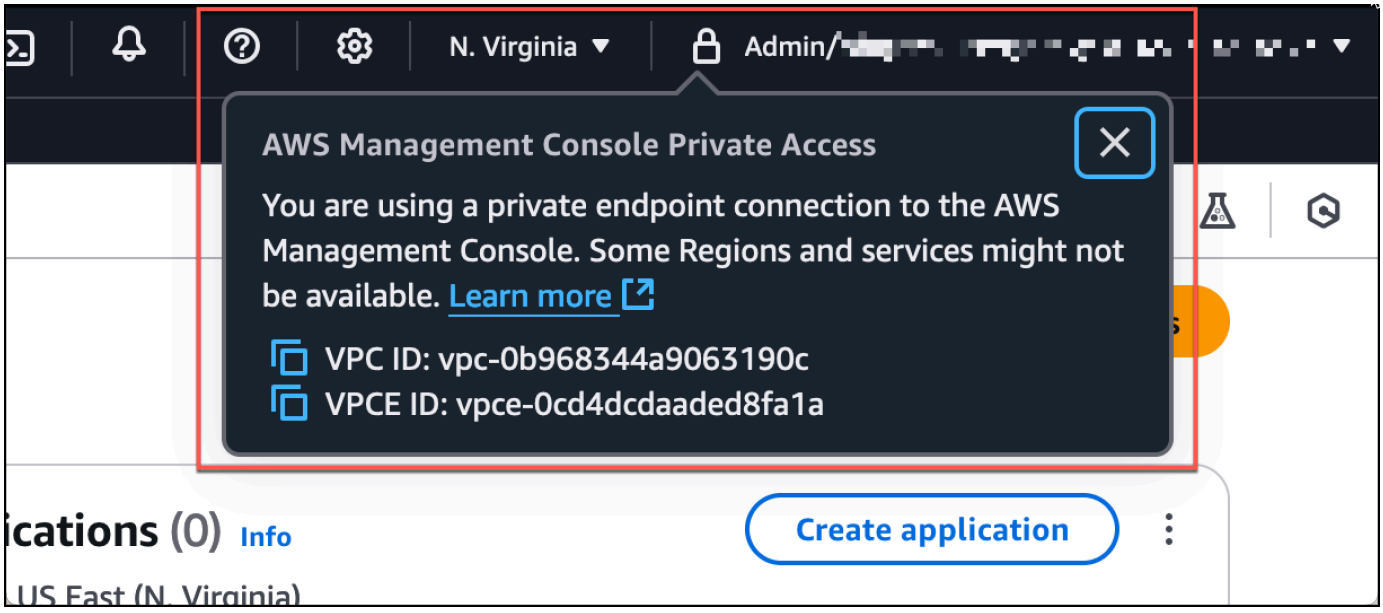
1. 조직의 관리 계정으로 로그인하고 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택합니다.
3. 인스턴스 페이지에서 CloudFormation 템플릿으로 생성된 콘솔 VPCE 테스트 인스턴스를 선택합니다. 그런 다음 연결을 선택합니다.

> **Note**
>
> 이 예제에서는의 기능인 Fleet Manager를 사용하여 Windows Server AWS Systems Manager Explorer에 연결합니다. 연결이 시작되기까지 몇 분 정도 걸릴 수 있습니다.

4. 인스턴스에 연결 페이지에서 RDP 클라이언트를 선택한 다음, Fleet Manager를 사용하여 연결을 선택합니다.
5. Fleet Manager 원격 데스크톱을 선택합니다.
6. Amazon EC2 인스턴스의 관리 암호를 가져오고 웹 인터페이스를 사용하여 Windows 데스크톱에 액세스하려면 CloudFormation 템플릿을 생성할 때 사용한 Amazon EC2 키 페어와 연결된 프라이빗 키를 사용합니다.
7. Amazon EC2 Windows 인스턴스에서 브라우저 AWS Management Console 에서를 엽니다.
8. 자격 AWS 증명으로 로그인한 후 Amazon S3 콘솔을 열고 프라이빗 액세스를 사용하여 AWS Management Console 연결되어 있는지 확인합니다.

AWS Management Console 프라이빗 액세스 설정을 테스트하려면

1. 조직의 관리 계정으로 로그인하고 Amazon S3 콘솔을 엽니다.
2. 탐색 메뉴에서 잠금-프라이빗 아이콘을 선택하면 사용 중인 VPC 엔드포인트를 볼 수 있습니다. 아래의 스크린샷은 잠금-프라이빗 아이콘의 위치와 VPC 정보를 보여줍니다.



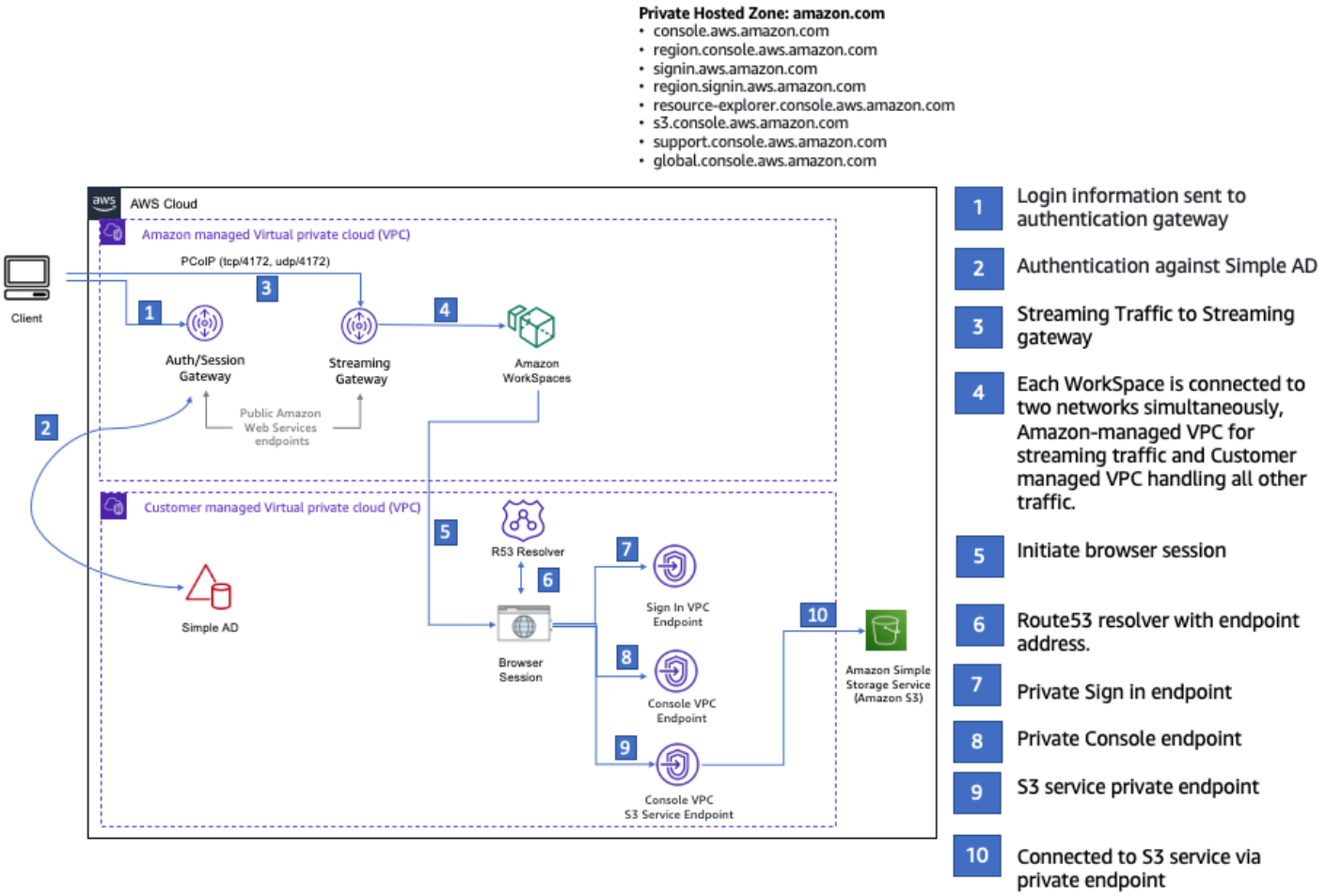
Amazon WorkSpaces를 사용한 테스트 설정

Amazon WorkSpaces를 사용하면 WorkSpaces라고 하는, 사용자를 위한 가상의 클라우드 기반 Windows, Amazon Linux 또는 Ubuntu Linux 데스크톱을 프로비저닝할 수 있습니다. 필요에 따라 신속하게 사용자를 추가 또는 제거할 수 있습니다. 사용자는 여러 디바이스 또는 웹 브라우저에서 가상 데스크톱에 액세스할 수 있습니다. WorkSpaces에 대해 자세히 알아보려면 Amazon WorkSpaces 관리 가이드를 참조하세요.

이 섹션의 예제에서는 사용자 환경이 WorkSpace에서 실행되는 웹 브라우저를 사용하여 AWS Management Console 프라이빗 액세스에 로그인하는 테스트 환경을 설명합니다. 그런 다음 사용자가 Amazon Simple Storage Service 콘솔을 방문합니다. 이 WorkSpace는 브라우저 AWS Management Console 에서에 액세스하여 VPC에 연결된 네트워크에서 노트북을 사용하는 기업 사용자의 경험을 시뮬레이션하기 위한 것입니다.

이 자습서에서는 AWS CloudFormation 를 사용하여 네트워크 설정과 WorkSpaces에서 사용할 Simple Active Directory를 생성하고 구성하며,를 사용하여 WorkSpace를 설정하는 단계별 지침을 사용합니다 AWS Management Console.

아래의 다이어그램은 WorkSpace를 사용하여 AWS Management Console 프라이빗 액세스 설정을 테스트하는 워크플로를 설명합니다. 여기에는 클라이언트 WorkSpace, Amazon 관리형 VPC, 고객 관리형 VPC 간의 관계가 나와 있습니다.



다음 CloudFormation 템플릿을 복사하여 절차 3단계에서 네트워크를 설정하는 데 사용할 파일에 저장합니다.

AWS Management Console 프라이빗 액세스 환경 CloudFormation 템플릿

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
```

```
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
```

```
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
```

```
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
```

```
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

########################
# VPC AND SUBNETS
########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
```

```
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
```

```
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
```

```
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC
```

```
#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref "ConsoleHostedZone"
      Name: "*.widget.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
        HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

  ConsoleRecordRegional:
```

```
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
```

```
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: !Ref DSAdminPasswordResourceName
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC
```

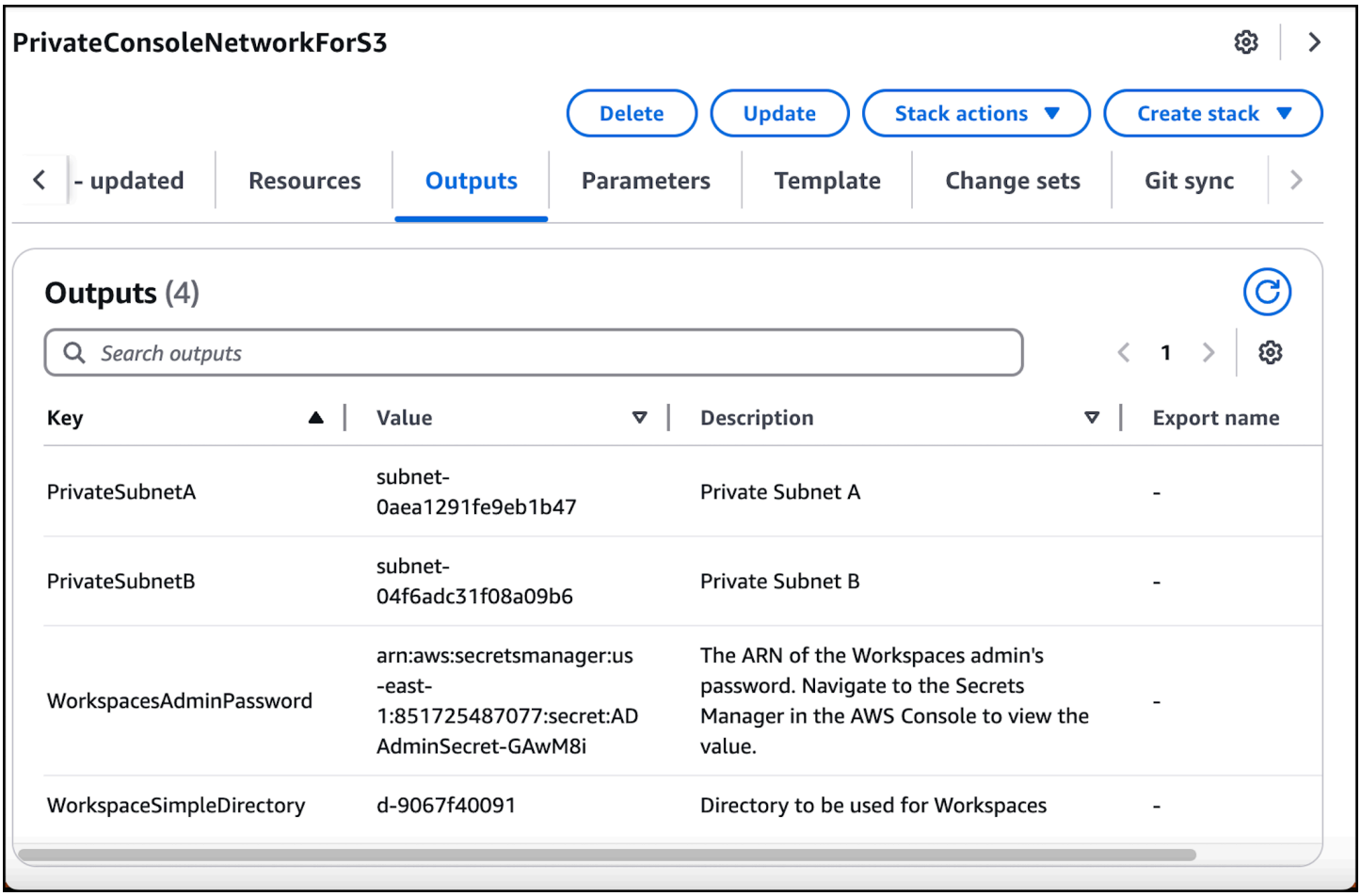
```
Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
 Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **Note**
>
> 이 테스트 설정은 미국 동부(버지니아 북부)(us-east-1) 리전에서 실행되도록 설계되었습니다.

네트워크를 설정하려면

1. 조직의 관리 계정으로 로그인하고 CloudFormation 콘솔을 엽니다.
2. 스택 생성을 선택합니다.
3. 새 리소스 사용(표준)(With new resources (standard))을 선택합니다. 이전에 생성한 CloudFormation 템플릿 파일을 업로드하고 다음을 선택합니다.
4. **`PrivateConsoleNetworkForS3`** 같은 스택 이름을 입력한 후 다음을 선택합니다.
5. VPC 및 서브넷의 경우, 원하는 IP CIDR 범위를 입력하거나 제공된 기본값을 사용합니다. 기본값을 사용하는 경우 기본값이의 기존 VPC 리소스와 겹치지 않는지 확인합니다 AWS 계정.
6. 스택 생성을 선택합니다.
7. 스택이 생성된 후 리소스 탭을 선택하여 생성된 리소스를 확인합니다.
8. 출력 탭을 선택하여 프라이빗 서브넷과 Workspace Simple Directory의 값을 확인합니다. 이러한 값은 WorkSpace를 생성하고 구성하는 다음 프로시저의 4단계에서 사용할 예정이므로 기록해 둡니다.

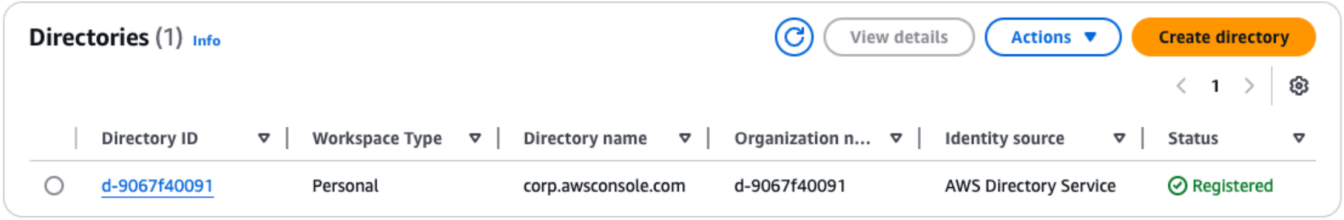
아래의 스크린샷은 프라이빗 서브넷과 Workspace Simple Directory의 값이 표시된 출력 탭의 보기를 보여줍니다.



이제 네트워크를 생성했으니 다음 프로시저를 사용하여 WorkSpace를 생성하고 액세스하세요.

WorkSpaces를 생성하려면

1. WorkSpaces 콘솔을 엽니다.
2. 탐색 창에서 디렉터리를 선택합니다.
3. 디렉터리 페이지에서 디렉터리 상태가 활성인지 확인합니다. 아래의 스크린샷은 활성 디렉터리가 있는 디렉터리 페이지를 보여줍니다.



4. WorkSpaces에서 디렉터리를 사용하려면 해당 디렉터리를 등록해야 합니다. 탐색 창에서 WorkSpaces를 선택한 다음 WorkSpaces 생성을 선택합니다.
5. 디렉터리 선택의 경우, 이전 프로시저에서 CloudFormation 에 의해 생성된 디렉터리를 선택합니다. 작업 메뉴에서 등록을 선택합니다.
6. 서브넷 선택의 경우, 이전 프로시저의 9단계에서 설명한 두 개의 프라이빗 서브넷을 선택합니다.
7. 셀프 서비스 권한 활성화를 선택한 다음 등록을 선택합니다.
8. 디렉터리를 등록한 후 WorkSpace 생성을 계속 진행합니다. 등록된 디렉터리를 선택한 후 다음을 선택합니다.
9. 사용자 생성 페이지에서 추가 사용자 생성을 선택합니다. WorkSpace를 사용할 수 있도록 이름과 이메일을 입력합니다. WorkSpace 로그인 정보가 이 이메일 주소로 전송되면 이메일 주소가 유효한지 확인하세요.
10. 다음을 선택합니다.
11. 사용자 식별 페이지에서, 9단계에서 생성한 사용자를 선택한 후 다음을 선택합니다.
12. 번들 선택 페이지에서 Standard with Amazon Linux 2를 선택한 후 다음을 선택합니다.
13. 실행 모드 및 사용자 지정에 대해 기본 설정을 사용하고 WorkSpace 생성을 선택합니다. WorkSpace는 `Pending` 상태에서 시작하며 약 20분 이내에 `Available`로 전환됩니다.
14. WorkSpaces를 사용할 수 있게 되면 9단계에서 제공한 이메일 주소로 액세스 지침이 포함된 이메일이 발송됩니다.

WorkSpace에 로그인한 후 AWS Management Console 프라이빗 액세스를 사용하여 WorkSpace에 액세스 중인지 테스트할 수 있습니다.

WorkSpace에 액세스하려면

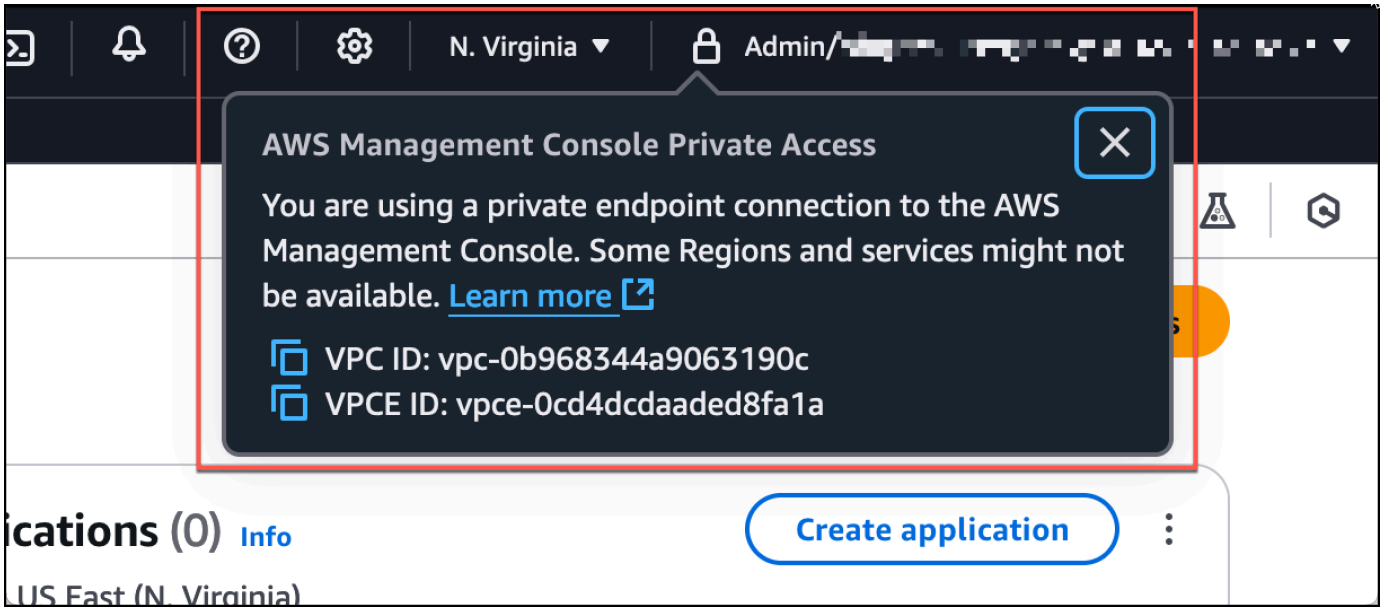
1. 이전 프로시저의 14단계에서 받은 이메일을 엽니다.
2. 이메일에서 제공된 고유 링크를 선택하여 프로파일을 설정하고 WorkSpaces 클라이언트를 다운로드합니다.
3. 암호를 설정합니다.
4. 선택한 클라이언트를 다운로드합니다.
5. 클라이언트를 설치하고 실행합니다. 이메일에 제공된 등록 코드를 입력한 다음 등록을 선택합니다.
6. 3단계에서 생성한 자격 증명을 사용하여 Amazon WorkSpaces에 로그인합니다.

AWS Management Console 프라이빗 액세스 설정을 테스트하려면

1. WorkSpaces에서 브라우저를 엽니다. 그런 다음, AWS Management Console로 이동하고 보안 인증 정보를 사용하여 로그인합니다.

   > **Note**
   >
   > Firefox를 브라우저로 사용하는 경우 브라우저 설정에서 HTTPS를 통한 DNS 활성화 옵션이 꺼져 있는지 확인합니다.

2. AWS Management Console 프라이빗 액세스를 사용하여 연결되었는지 확인할 수 있는 Amazon S3 콘솔을 엽니다.
3. 탐색 메뉴에서 잠금-프라이빗 아이콘을 선택하면 사용 중인 VPC 및 VPC 엔드포인트를 볼 수 있습니다. 아래의 스크린샷은 잠금-프라이빗 아이콘의 위치와 VPC 정보를 보여줍니다.



IAM 정책을 사용하여 VPC 설정 테스트

액세스를 제한하는 IAM 정책을 배포하여 Amazon EC2 또는 WorkSpaces를 사용하여 설정한 VPC를 추가로 테스트할 수 있습니다.

아래의 정책은 지정된 VPC를 Amazon S3가 사용하지 않는 한 Amazon S3에 대한 액세스를 거부합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

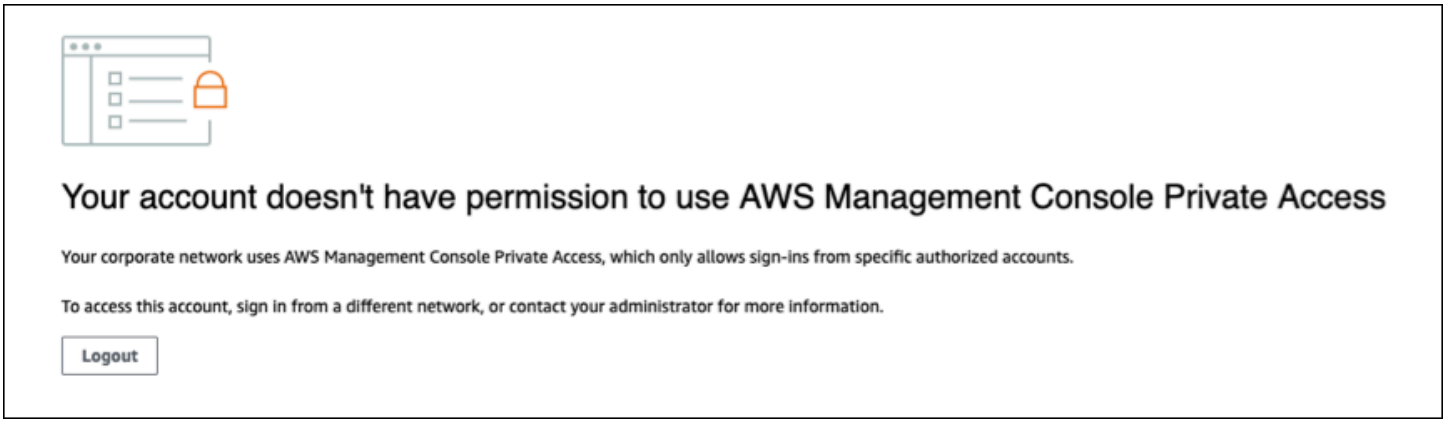
다음 정책은 로그인 엔드포인트에 프라이빗 액세스 정책을 사용하여 AWS Management Console 선택한 AWS 계정 IDs에 대한 로그인을 제한합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
```

```
            }
        }
    ]
}
```

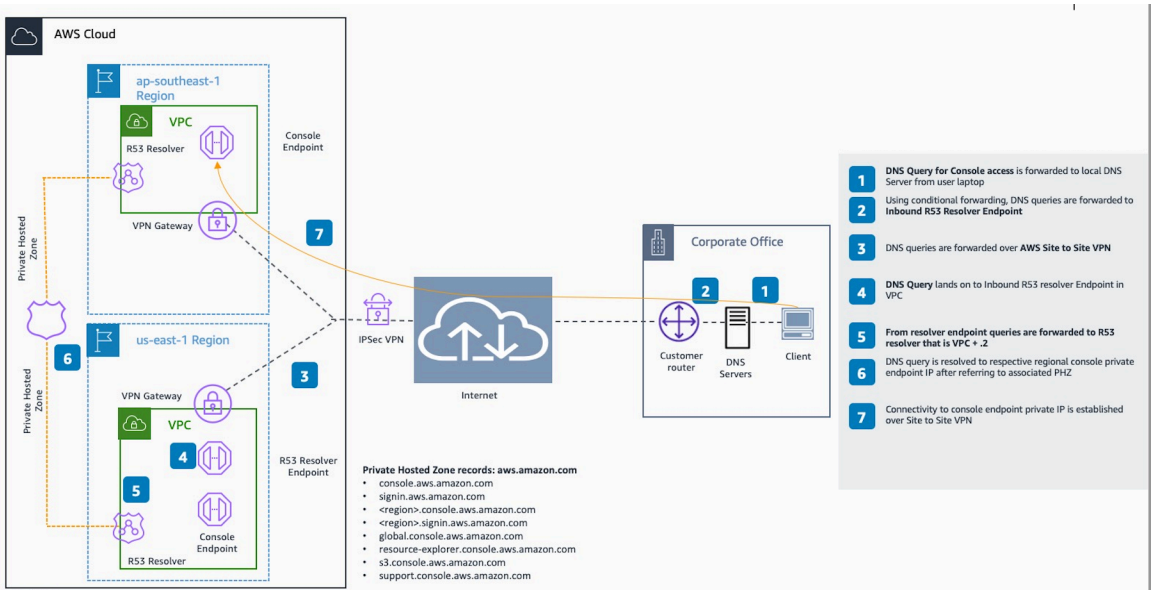
계정에 속하지 않는 ID로 연결할 경우 다음과 같은 오류 페이지가 표시됩니다.



참조 아키텍처

온프레미스 네트워크에서 AWS Management Console 프라이빗 액세스에 비공개로 연결하려면 AWS Site-to-Site VPN AWS 가상 프라이빗 게이트웨이(VGW) 연결 옵션을 활용할 수 있습니다. AWS Site-to-Site VPN 에서는 연결을 생성하고 연결을 통해 트래픽을 전달하도록 라우팅을 구성하여 VPC에서 원격 네트워크에 액세스할 수 있습니다. 자세한 내용은 SiteAWS Site-to-Site VPN 사용 설명서의 WhatisSiteAWS Site-to-Site VPN을 참조하세요. AWS VGW(가상 프라이빗 게이트웨이)는 VPC와 온프레미스 네트워크 간의 게이트웨이 역할을 하는 가용성이 높은 리전 서비스입니다.

AWS Site-to-Site VPN AWS 가상 프라이빗 게이트웨이(VGW)로



이 참조 아키텍처 설계의 필수 구성 요소는 Amazon Route 53 Resolver, 특히 인바운드 해석기입니다. AWS Management Console 프라이빗 액세스 엔드포인트가 생성되는 VPC에서 설정하면 지정된 서브넷에 해석기 엔드포인트(네트워크 인터페이스)가 생성됩니다. 그런 다음 온프레미스 DNS 서버의 조건부 전달자에서 해당 IP 주소를 참조하여 프라이빗 호스팅 영역에 있는 레코드를 쿼리할 수 있습니다. 온프레미스 클라이언트가에 연결되면 AWS Management Console 프라이빗 액세스 엔드포인트의 프라이빗 IPs로 라우팅 AWS Management Console됩니다.

AWS Management Console 프라이빗 액세스 엔드포인트에 대한 연결을 설정하기 전에 액세스하려는 모든 리전 AWS Management Console과 미국 동부(버지니아 북부) 리전에서 AWS Management Console 프라이빗 액세스 엔드포인트를 설정하고 프라이빗 호스팅 영역을 구성하는 사전 조건 단계를 완료합니다.

AWS 사용자 경험 사용자 지정(UXC)

AWS 사용자 경험 사용자 지정(UXC)은 계정 관리자가의 시각적 모양을 사용자 지정 AWS Management Console 하고 계정 수준에서 이러한 설정을 관리할 수 있는 유틸리티입니다.

UXC를 사용하면 다음 설정을 사용자 지정할 수 있습니다.

- 계정 색상 - 계정의 색상을 설정하여 계정을 시각적으로 구분할 수 있습니다. 예를 들어 개발 계정에는 녹색을, 테스트 계정에는 노란색을, 프로덕션 계정에는 빨간색을 사용할 수 있습니다.
- 서비스 가시성 - 콘솔 탐색에 표시되는 AWS 서비스를 제어할 수 있습니다. 서비스 가시성은 계정과 관련된 AWS 서비스만 표시 AWS Management Console 하도록를 간소화합니다.
- 리전 가시성 - AWS 리전 선택기에 표시되는 리전을 제어할 수 있습니다. 리전 가시성은 계정과 관련된 리전만 표시 AWS Management Console 하도록를 간소화합니다.

설정을 구성하지 않은 경우 기본 동작이 적용됩니다. 모든 서비스 및 리전이 표시되고 계정 색상이 설정되지 않습니다. 값을 로 설정하여 계정 색상을 기본값으로 재설정할 수 있습니다`"none"`. 값을 로 설정하여 표시되는 서비스 및 리전을 기본값으로 재설정할 수 있습니다`null`.

> **Note**
>
> `visibleServices` 및 `visibleRegions` 설정은에서 서비스 및 리전의 모양만 제어합니다 AWS Management Console. , AWS Command Line Interface SDKs 또는 기타 APIs를 통한 액세스를 제한하지 않습니다.

주제

- AWS 사용자 경험 사용자 지정 시작하기
- 를 사용하여 AWS 사용자 경험 사용자 지정 API 호출 로깅 AWS CloudTrail
- AWS 사용자 경험 사용자 지정의 보안

AWS 사용자 경험 사용자 지정 시작하기

UXC를 사용하면 계정 관리자가에 대한 계정 사용자 지정을 구성할 수 있습니다 AWS Management Console.

사전 조건

시작하려면 다음이 필요합니다.

- AWS 계정
- UXC에 대한 적절한 AWS Identity and Access Management (IAM) 권한. 자세한 내용은 AWS 사용자 경험 사용자 지정이에 대한 IAM 및 관리형 정책을 사용하는 방법을 AWS 참조하세요 AWS Management Console.

에서 UXC 설정 액세스 AWS Management Console

의 계정 색상에 액세스하려면의 계정 정보 액세스를 AWS Management Console참조하세요. AWS Management Console 에서 서비스 가시성 및 리전 가시성에 액세스하려면 통합 설정을 AWS Management Console 사용하여 구성을 AWS Management Console참조하세요.

콘솔에서 계정 색상을 설정하려면

1. AWS Management Console에 로그인합니다.
2. 탐색 모음에서 계정 이름을 선택합니다.
3. 계정을 선택합니다.
4. 계정 표시 설정에서 색상을 선택합니다.
5. 업데이트를 선택합니다.

콘솔에서 표시되는 리전을 설정하려면

1. AWS Management Console에 로그인합니다.
2. 통합 설정을 엽니다.
3. 가시 리전 섹션에서 편집을 선택합니다.
4. 표시되는 리전을 사용 가능한 모든 리전 또는 리전 선택으로 설정하고 목록을 구성합니다.
5. 변경 사항 저장을 선택합니다.

콘솔에서 표시되는 서비스를 설정하려면

1. AWS Management Console에 로그인합니다.
2. 통합 설정을 엽니다.

3. 표시 서비스 섹션에서 편집을 선택합니다.
4. 표시되는 서비스를 모든 서비스 또는 서비스 선택으로 설정하고 목록을 구성합니다.
5. 변경 사항 저장을 선택합니다.

프로그래밍 방식으로 UXC 설정 액세스

프로그래밍 방식으로 또는 코드형 인프라로 계정 사용자 지정 설정을 관리할 수도 있습니다. 자세한 내용은 AWS 사용자 경험 사용자 지정 API 참조 및 AWS::UXC::AccountCustomization CloudFormation 템플릿 참조를 참조하세요.

를 사용하여 AWS 사용자 경험 사용자 지정 API 호출 로깅 AWS CloudTrail

AWS 사용자 경험 사용자 지정은 사용자AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스인와 통합됩니다 AWS 서비스. CloudTrail은 UXC에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 UXC 콘솔로부터의 직접 호출과 UXC API 작업에 대한 코드 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 UXC에 수행된 요청, 요청이 수행된 IP 주소, 요청이 수행된 시간, 추가 세부 정보를 확인할 수 있습니다.

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

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

CloudTrail의 UXC 관리 이벤트

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

AWS 사용자 경험 사용자 지정은 모든 UXC 컨트롤 플레인 작업을 관리 이벤트로 로깅합니다. UXC가 CloudTrail에 로깅하는 AWS 사용자 경험 사용자 지정 컨트롤 플레인 작업 목록은 AWS 사용자 경험 사용자 지정 API 참조를 참조하세요.

UXC 이벤트 예제

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

다음 예제는 작업을 시연하는 CloudTrail 이벤트를 보여줍니다.


```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
  "eventType" : "AwsApiCall",
```

```
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```

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

AWS 사용자 경험 사용자 지정의 보안

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

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

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

이 설명서는 UXC를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 UXC를 구성하는 방법을 보여줍니다. 또한 UXC 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- AWS 사용자 경험 사용자 지정을 위한 ID 및 액세스 관리

AWS 사용자 경험 사용자 지정을 위한 ID 및 액세스 관리

AWS 사용자 경험 사용자 지정(UXC)은 IAM 정책을 사용하여 UXC API 작업에 대한 액세스를 관리합니다.

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 사용자 경험 사용자 지정 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

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

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS 사용자 경험 사용자 지정 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(AWS 사용자 경험 사용자 지정이 IAM과 작동하는 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(AWS 사용자 경험 사용자 지정을 위한 자격 증명 기반 정책 예제 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증해야 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 사용자가 필요한 작업 목록은 IAM 사용자 설명서의 루트 사용자 자격 증명이 필요한 작업을 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.

AWS 사용자 경험 사용자 지정이 IAM과 작동하는 방식

AWS 사용자 경험 사용자 지정(UXC)은 IAM 정책과 함께 작동하여 UXC API 작업에 대한 액세스를 관리합니다.

IAM을 사용하여 AWS 사용자 경험 사용자 지정(사용자 경험 사용자 지정)에 대한 액세스를 관리하기 전에 사용자 경험 사용자 지정과 함께 사용할 수 있는 IAM 기능에 대해 알아봅니다. AWS 관리형 정책을 통해 사용자 경험 사용자 지정과 통합하는 것이 좋습니다. 자세한 내용은 AWS 의 관리형 정책을 참조하세요 AWS Management Console.

IAM을 사용하여 사용자 경험 사용자 지정에 대한 액세스를 관리하기 전에 사용자 경험 사용자 지정과 함께 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM 특성	사용자 경험 사용자 지정 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	아니요
정책 조건 키	아니요
임시 보안 인증	예
서비스 간 주요 권한	아니요
서비스 연결 역할	아니요
서비스 역할	아니요

사용자 경험 사용자 지정 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

사용자 경험 사용자 지정을 위한 자격 증명 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지

를 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.

사용자 경험 사용자 지정 자격 증명 기반 정책의 예제를 보려면 AWS 사용자 경험 사용자 지정에 대한 자격 증명 기반 정책 예제를 참조하세요.

사용자 경험 사용자 지정을 위한 정책 작업

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.

모든 사용자 경험 사용자 지정 작업을 보려면 API 참조를 참조하세요.

사용자 경험 사용자 지정의 정책 작업은 작업 앞에 `uxc:` 접두사를 사용합니다(예: `uxc:GetAccountCustomizations`).

단일 구문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "uxc:GetAccountCustomizations",
      "uxc:ListServices"
         ]
```

사용자 경험 사용자 지정 자격 증명 기반 정책의 예제를 보려면 AWS 사용자 경험 사용자 지정에 대한 자격 증명 기반 정책 예제를 참조하세요.

사용자 경험 사용자 지정을 위한 정책 리소스

사용자 경험 사용자 지정은 정책 리소스를 지원하지 않습니다.

사용자 경험 사용자 지정에서 임시 자격 증명 사용

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 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 작업하는AWS 서비스 섹션을 참조하세요.

AWS 사용자 경험 사용자 지정 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 사용자 경험 사용자 지정 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

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 uxc:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 uxc:GetWidget on resource: my-example-widget because no identity-based policy allows
 the GetWidget action
```

이 경우, uxc:*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 사용자 액세스 키를 생성한 후에는 언제든지 액세스 키 ID를 볼 수 있습니다. 하지만 보안 액세스 키는 다시 볼 수 없습니다. 보안 액세스 키를 잃어버린 경우 새로운 액세스 키 페어를 생성해야 합니다.

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

> **Important**
>
> 정식 사용자 ID를 찾는 데 도움이 되더라도 액세스 키를 타사에 제공하지 마시기 바랍니다. 이렇게 하면 누군가에게에 대한 영구 액세스 권한을 부여할 수 있습니다 AWS 계정.

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

다른 사용자가 사용자 경험 사용자 지정에 액세스하도록 허용하려면 액세스 권한이 필요한 사용자 또는 애플리케이션에 권한을 부여해야 합니다. AWS IAM Identity Center 를 사용하여 사용자 및 애플리

케이션을 관리하는 경우 사용자 또는 그룹에 권한 세트를 할당하여 액세스 수준을 정의합니다. 권한 세트는 IAM 정책을 자동으로 생성하고 사용자 또는 애플리케이션과 연결된 IAM 역할에 할당합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 권한 세트를 참조하세요.

IAM Identity Center를 사용하지 않는 경우 액세스가 필요한 사용자 또는 애플리케이션에 대한 IAM 엔터티(사용자 또는 역할)를 생성해야 합니다. 그런 다음 사용자 경험 사용자 지정에서 올바른 권한을 부여하는 정책을 엔터티에 연결해야 합니다. 권한이 부여되면 사용자 또는 애플리케이션 개발자에게 자격 증명을 제공합니다. 이들은 이 자격 증명을 사용하여 AWS에 액세스합니다. IAM 사용자, 그룹, 정책 및 권한 생성에 대해 자세히 알아보려면 IAM 사용자 설명서의 IAM 자격 증명과 IAM의 권한 및 정책을 참조하세요.

AWS 사용자 경험 사용자 지정을 위한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 UXC 리소스를 가져오거나 수정할 수 있는 권한이 없습니다. 사용자에게 리소스에 대한 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

주제

- 정책 모범 사례
- UXC 계정 사용자 지정에 대한 읽기 전용 액세스
- UXC 계정 사용자 지정에 대한 전체 액세스

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 사용자 경험 사용자 지정 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.

UXC 계정 사용자 지정에 대한 읽기 전용 액세스

다음 예제에서는 UXC 계정 사용자 지정에 대한 읽기 전용 액세스를 허용하는 정책을 생성하는 방법을 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "uxc:GetAccountCustomizations",
                "uxc:ListServices"
            ],
            "Resource": "*"
        }
    ]
}
```

UXC 계정 사용자 지정에 대한 전체 액세스

다음 예제에서는 UXC 계정 사용자 지정에 대한 전체 액세스를 허용하는 정책을 생성하는 방법을 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "uxc:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 에 대한 관리형 정책 AWS Management Console

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

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

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

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSManagementConsoleBasicUserAccess

사용자, 그룹 및 역할에 `AWSManagementConsoleBasicUserAccess`를 연결할 수 있습니다.

이 정책은 AWS Management Console의 관리자가 아닌 사용자에게 필요한 권한을 부여합니다. 여기에는 리소스 검색, 알림, 브라우저 기반 셸 액세스, 사용자 지정 탐색과 같은 기능이 포함됩니다.

권한 세부 정보

이 `AWSManagementConsoleBasicUserAccess`는 다음 권한 집합으로 그룹화됩니다.

- `cloudshell` - 보안 주체가 환경 생성, 세션 관리 및 명령 실행을 포함한 AWS CloudShell 기능에 대한 모든 액세스 권한을 허용합니다.
- `ec2` - 보안 주체가 통합 탐색에서 계정에 활성화된 리전을 설명할 수 있도록 허용합니다.
- `notifications` - 보안 주체가 이벤트를 가져올 수 있도록 허용합니다 AWS 사용자 알림.

- q - 보안 주체가 Amazon Q Developer와 채팅할 수 있도록 허용합니다.
- resource-explorer-2 - 보안 주체가 통합 검색을 사용하여 AWS 리소스를 검색하고 검색할 수 있습니다.
- uxc - 보안 주체가 AWS 사용자 경험 사용자 지정 설정을 읽을 수 있도록 허용합니다.
- action-recommendations - 보안 주체가 상황별 작업 권장 사항을 수신할 수 있도록 허용합니다.
- account - 보안 주체가 계정 이름, 계정 ID, 계정 생성 날짜 및 시간을 포함하여 지정된 계정에 대한 정보를 검색할 수 있도록 허용합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조에서 AWSManagementConsoleBasicUserAccess를 참조하세요.

AWS 관리형 정책: AWSManagementConsoleAdministratorAccess

사용자, 그룹 및 역할에 AWSManagementConsoleAdministratorAccess를 연결할 수 있습니다.

이 정책은 AWS Management Console을 구성하고 사용자 지정할 수 있는 전체 액세스 권한을 부여합니다. 이를 통해 관리자는 계정 색상을 설정하고, 사용자 알림을 활성화하며, 리소스 검색을 구성할 수 있습니다. 또한 AWS Management Console의 관리자가 아닌 사용자에게 필수적인 AWSManagementConsoleBasicUserAccess 관리형 정책의 권한도 포함됩니다.

권한 세부 정보

이 AWSManagementConsoleAdministratorAccess는 다음 권한 집합으로 그룹화됩니다.

- cloudshell - 보안 주체가 환경 생성, 세션 관리 및 명령 실행을 포함한 AWS CloudShell 기능에 대한 모든 액세스 권한을 허용합니다.
- ec2 - 보안 주체가 통합 탐색에서 계정에 활성화된 리전을 설명할 수 있도록 허용합니다.
- notifications - 보안 주체가 알림 구성, 이벤트 및 기능 옵트인 상태에 액세스하고 업데이트할 수 있도록 허용합니다.
- q - 보안 주체가 AI 지원 지원을 위해 Amazon Q Developer와 채팅할 수 있도록 허용합니다.
- resource-explorer-2 - 보안 주체가 통합 검색을 사용하여 AWS 리소스를 검색하고 검색할 수 있습니다.

- `uxc` - 보안 주체가 AWS 사용자 경험 사용자 지정 설정에 대한 전체 액세스 권한을 허용합니다.
- `action-recommendations` - 보안 주체가 상황별 작업 권장 사항을 수신할 수 있도록 허용합니다.
- `account` - 보안 주체가 계정 이름, 계정 ID, 계정 생성 날짜 및 시간을 포함하여 지정된 계정에 대한 정보를 검색할 수 있도록 허용합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 AWSManagementConsoleAdministratorAccess를 참조하세요.

AWS Management Console AWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Management Console 이후부터의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Management Console 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AWSManagementConsoleBasicUserAccess – 업데이트된 정책	`uxc:GetAccountCustomizations` 및 `uxc:ListServices` 권한이 추가되었습니다.	2026년 3월 26일
AWSManagementConsoleAdministratorAccess – 업데이트된 정책	`uxc:GetAccountCustomizations` , `uxc:UpdateAccountCustomizations` 및 `uxc:ListServices` 권한이 추가되었습니다.	2026년 3월 26일
AWSManagementConsoleBasicUserAccess – 업데이트된 정책	사용자가를 탐색하는 동안 계정 정보를 보고 작업 권장 사항을 받을 수 있도록 권한을 추가하도록 정책이 업데이트되었습니다 AWS Management Console.	2025년 12월 9일

변경	설명	Date
AWSManagementConsoleAdministratorAccess – 업데이트된 정책	사용자가를 탐색하는 동안 계정 정보를 보고 작업 권장 사항을 받을 수 있도록 권한을 추가하도록 정책이 업데이트되었습니다 AWS Management Console.	2025년 12월 9일
AWSManagementConsoleBasicUserAccess – 새 정책	기본 AWS Management Console 탐색, 계정 색상 보기 및 리소스 검색에 필요한 권한을 부여하는 새로운 AWS 관리형 정책이 추가되었습니다.	2025년 8월 14일
AWSManagementConsoleAdministratorAccess – 새 정책	를 구성하고 사용자 지정할 수 있는 전체 액세스 권한을 제공하는 새로운 AWS 관리형 정책이 추가되었습니다 AWS Management Console.	2025년 8월 14일
AWS Management Console 에서 변경 내용 추적 시작	AWS Management Console 가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2025년 8월 14일

콘솔에서 마크다운 사용

Amazon CloudWatch AWS Management Console와 같은의 일부 서비스는 특정 필드에서 마크다운 사용을 지원합니다. 이 단원에서는 콘솔에서 지원되는 마크다운 서식 유형에 대해 설명합니다.

내용

단락, 행 간격, 수평 행

단락은 빈 행으로 구분합니다. HTML로 변환할 때 문단 사이의 빈 줄이 렌더링되도록 하려면 줄 바꿈하지 않는 공백( )이 있는 새 줄과 빈 줄을 차례로 추가하십시오. 다음 예제와 같이 빈 줄을 여러 개 삽입하려면 이 선의 쌍을 반복합니다.

```
 

 
```

문단을 구분하는 수평 규칙을 만들려면 하이픈이 3개씩(---) 있는 새 줄을 추가합니다.

```
Previous paragraph.
---
Next paragraph.
```

고정 너비 유형의 텍스트 블록을 생성하려면 3개의 백틱(`)이 있는 줄을 추가합니다. 고정 너비 유형으로 표시할 텍스트를 입력합니다. 그런 다음 3개의 백틱이 있는 새 줄을 추가합니다. 다음 예제에서는 표시 시 고정 너비 유형으로 서식이 지정되는 텍스트를 보여 줍니다.

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

```
```

제목

제목을 생성하려면 파운드 기호(#)를 사용합니다. 단일 파운드 기호와 공백은 최상위 제목을 나타냅니다. 2개의 파운드 기호는 두 번째 수준의 제목을 생성하며 3개의 파운드 기호는 세 번째 수준의 제목을 생성합니다. 다음 예제에서는 최상위 수준, 두 번째 수준 및 세 번째 수준의 제목을 보여 줍니다.

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

텍스트 서식 지정

텍스트를 기울임꼴로 지정하려면 해당 텍스트 앞 뒤에 1개의 밑줄(_)이나 별표(*)를 입력하여 텍스트를 묶습니다.

```
*This text appears in italics.*
```

텍스트를 굵은체로 지정하려면 해당 텍스트 앞 뒤에 두 개의 밑줄이나 별표를 입력하여 텍스트를 묶습니다.

```
**This text appears in bold.**
```

텍스트에 취소선 서식을 지정하려면 해당 텍스트 앞 뒤에 2개의 물결 기호(~)를 입력하여 텍스트를 묶습니다.

```
~~This text appears in strikethrough.~~
```

링크

텍스트 하이퍼링크를 추가하려면 다음 예제와 같이 대괄호([ ])로 둘러싸인 링크 텍스트를 입력한 다음 괄호(( ))에 전체 URL을 입력합니다.

```
Choose [link_text](http://my.example.com).
```

Lists

글머리표 목록으로 행 서식을 지정하려면 다음 예제와 같이 하나의 별표(*)와 함께 별도의 줄에 입력한 후 공백을 입력합니다.

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

번호가 매겨진 목록으로 행 서식을 지정하려면 다음 예제와 같이 숫자, 마침표(.), 공백과 함께 별도의 줄에 입력합니다.

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

표와 버튼(CloudWatch 대시보드)

CloudWatch 대시보드 텍스트 위젯은 마크다운 표와 버튼을 지원합니다.

테이블을 생성하려면 세로 막대(|)를 사용하여 열을 구분하고 새 줄을 사용하여 행을 구분합니다. 첫 번째 행을 헤더 행으로 생성하려면 헤더 행과 값의 첫 번째 행 사이에 줄을 삽입합니다. 그런 다음 표의 각 열에 대해 최소 3개의 하이픈(-)을 추가합니다. 세로 막대를 사용하여 열을 구분합니다. 다음 예제에서는 2개의 열, 헤더 행 및 2개의 데이터 행이 있는 테이블의 마크다운을 보여 줍니다.

```
Table | Header
----|-----
Amazon Web Services | AWS
1 | 2
```

이전 예제의 마크다운 텍스트는 다음 테이블을 생성합니다.

표	헤더
Amazon Web Services	AWS
1	2

CloudWatch 대시보드 텍스트 위젯에서 하이퍼링크를 버튼으로 표시하도록 서식을 지정할 수도 있습니다. 버튼을 만들려면 다음 예제와 같이 [button:*Button text*]를 사용한 다음 괄호(( ))에 전체 URL을 입력합니다.

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

문제 해결

의 일반적인 문제에 대한 해결책을 찾으려면이 섹션을 참조하세요 AWS Management Console.

Amazon Q Developer를 사용하여 일부 AWS 서비스의 일반적인 오류를 진단하고 해결할 수도 있습니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 Amazon Q Developer를 사용하여 콘솔의 일반적인 오류 진단을 참조하세요.

주제

페이지가 정상적으로 로드되지 않음

- 이 문제가 가끔 발생하는 경우 인터넷 연결을 확인합니다. VPN을 사용하거나 사용하지 않고 다른 네트워크를 통해 연결해 보거나 다른 웹 브라우저를 사용해 봅니다.
- 영향을 받는 모든 사용자가 동일한 팀의 사용자인 경우 개인 정보 보호 브라우저 확장 또는 보안 방화벽 문제일 수 있습니다. 개인 정보 보호 브라우저 확장 및 보안 방화벽이 AWS Management Console에서 사용하는 도메인에 대한 액세스를 차단할 수 있습니다. 이러한 확장을 끄거나 방화벽 설정을 조정해 봅니다. 연결 문제를 확인하려면 브라우저 개발자 도구(Chrome, Firefox)를 열고 콘솔(Console) 탭에서 오류를 조사합니다. 는 다음 목록을 포함한 도메인의 접미사를 AWS Management Console 사용합니다. 단, 이 목록이 전부는 아니며 추후 변경될 수 있습니다. 이러한 도메인의 접미사는 AWS에서 독점적으로 사용하는 것은 아닙니다.
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com
  - .aws.dev
  - .awscloud.com

- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

> **Warning**
>
> 2022년 7월 31일 이후는 더 이상 Internet Explorer 11을 지원하지 AWS 않습니다. 지원되는 다른 브라우저 AWS Management Console 에서를 사용하는 것이 좋습니다. 자세한 내용은 AWS News 블로그를 참조하세요.

에 연결할 때 브라우저에 '액세스 거부됨' 오류가 표시됨 AWS Management Console

다음 조건이 모두 충족되는 경우 콘솔에 대한 최근 변경 사항이 액세스에 영향을 미칠 수 있습니다.

- VPC 엔드포인트를 통해 AWS 서비스 엔드포인트 AWS Management Console 에 도달하도록 구성된 네트워크에서에 액세스합니다.
- IAM 정책에서 `aws:SourceIp` 또는 `aws:SourceVpc` 전역 조건 키를 사용하여 AWS 서비스에 대한 액세스를 제한합니다.

`aws:SourceIp` 또는 `aws:SourceVpc` 전역 조건 키가 포함된 IAM 정책을 검토하는 것이 좋습니다. 해당하는 경우 `aws:SourceIp`와 `aws:SourceVpc`를 모두 적용합니다.

일부 AWS Management Console 기능은 IPv4 및 IPv6 연결을 모두 지원하는 듀얼 스택 도메인을 사용합니다. IAM 정책이 IPv4 CIDR 블록`aws:SourceIp`에서만를 사용하여 액세스를 제한하는 경우 운영 체제가 IPv6 연결을 선호하는 경우(또는 그 반대) 요청이 실패할 수 있습니다. 이를 방지하려면 `aws:SourceIp` 조건에 IPv4 및 IPv6 CIDR 블록을 모두 포함합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 aws:SourceIp를 참조하세요.

AWS Management Console 프라이빗 액세스 기능에 온보딩하여 VPC 엔드포인트를 AWS Management Console 통해에 액세스하고 정책의 `aws:SourceVpc` 조건을 사용할 수도 있습니다. 자세한 내용은 다음을 참조하세요.

- AWS Management Console 프라이빗 액세스

- the section called “AWS Management Console 프라이빗 액세스가 aws:SourceVpc와 작동하는 방식”
- the section called “지원되는 AWS 전역 조건 컨텍스트 키”

에 연결할 때 브라우저에 제한 시간 오류가 표시됨 AWS Management Console

기본값에 서비스 중단이 있는 경우에 연결하려고 할 때 AWS 리전브라우저에 504 게이트웨이 제한 시간 오류가 표시될 수 있습니다 AWS Management Console. 다른 리전 AWS Management Console 에서에 로그인하려면 URL에 대체 리전 엔드포인트를 지정합니다. 예를 들어 `us-west-1`(캘리포니아 북부) 리전에서 중단이 발생한 경우 `us-west-2`(오레곤) 리전에 액세스하려면 다음 템플릿을 사용합니다.

```
https://region.console.aws.amazon.com
```

자세한 내용은 AWS 일반 참조의 AWS Management Console 서비스 엔드포인트를 참조하세요.

를 AWS 서비스포함한 모든의 상태를 보려면 단원을 AWS Management Console참조하십시오AWS Health Dashboard.

의 언어를 변경하고 싶지 AWS Management Console 만 페이지 하단에서 언어 선택 메뉴를 찾을 수 없습니다.

언어 선택 메뉴가 새로운 통합 설정(United Settings) 페이지로 이동했습니다. 의 언어를 변경하려면 통합 설정 페이지로 AWS Management Console이동한 다음 콘솔의 언어를 선택합니다. 에서 통합 설정 구성 AWS Management Console

자세한 내용은 AWS Management Console의 언어 변경을 참조하세요.

문서 기록

다음 표에서는 2021년 3월을 기준으로 AWS Management Console 시작 가이드에서 변경된 중요 사항에 대해 설명합니다.

변경	설명	Date
업데이트된 AWS 관리형 정책	AWSManagementConsoleAdministratorAccess 및 AWSManagementConsoleBasicUserAccess 정책을 새 UXC 권한으로 업데이트했습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2026년 3월 26일
페이지 추가	권장 작업을 설명하기 위해 새 페이지가 추가되었습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2025년 10월 15일
새로운 AWS 관리형 정책	AWS Management Console사용, 구성 및 사용자 지정에 대한 권한 범위를 지정하는 두 가지 새 정책이 추가되었습니다. • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	2025년 8월 14일
사용자 경험 사용자 지정(UXC)	새 서비스를 사용할 수 있습니다.	2025년 8월 14일
페이지 업데이트됨	이제 서비스 메뉴의 myApplications에서 애플리케이션을 볼 수 있습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2025년 7월 29일

변경	설명	Date
페이지 추가	멀티 세션 기능을 설명하기 위해 새 페이지가 추가되었습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2024년 12월 6일
페이지 업데이트됨	암호 변경 페이지가 업데이트되었습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2024년 6월 18일
새 페이지 추가됨	서비스 메뉴 및 AWS 이벤트 알림에 액세스하는 방법을 설명하는 새 페이지가 추가되었습니다. 자세한 내용은 ??? 및 ??? 섹션을 참조하세요.	2024년 6월 18일
페이지 업데이트됨	란 무엇입니까 AWS Management Console? 페이지가 업데이트되었습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2024년 6월 18일
지원 받기	지원을 받는 방법을 설명하는 새 페이지가 추가되었습니다. 자세한 내용은 ??? 단원을 참조하십시오.	2024년 6월 18일
통합 탐색 및 AWS Console Home	콘솔 작업 방법을 설명하는 새 페이지가 추가되었습니다. 자세한 내용은 ??? 및 ??? 섹션을 참조하세요.	2024년 6월 18일

변경	설명	Date
Amazon Q와 채팅	사용자가 Amazon Q Developer에 AWS 질문하는 방법을 자세히 설명하는 새 설정 페이지입니다. 자세한 내용은 Amazon Q Developer와 채팅을 참조하세요.	2024년 5월 29일
myApplications	myApplications를 소개하는 새 페이지입니다. 자세한 내용은 myApplications가 어디에 있습니까 AWS?를 참조하세요.	2023년 11월 29일
통합 설정 구성	언어 및 리전을 포함하여 현재 사용자에게 적용되는 설정 및 기본값을 구성하는 데 사용되는 새 설정 페이지입니다. 자세한 내용은 통합 설정 구성을 참조하세요.	2022년 4월 6일
새 AWS Console Home UI	새로운 AWS Console Home UI에는 중요한 사용 정보 및 AWS 서비스에 대한 바로 가기를 표시하기 위한 위젯이 포함되어 있습니다. 자세한 내용은 위젯 작업을 참조하세요.	2022년 2월 25일
콘솔 언어 변경	AWS Management Console에 대해 다른 언어를 선택합니다. 자세한 내용은 AWS Management Console의 언어 변경을 참조하세요.	2021년 4월 1일

변경	설명	Date
CloudShell 시작	AWS CloudShell 에서 AWS Management Console 를 열고 AWS CLI 명령을 실행합니다. 자세한 내용은 시작을 참조하세요 AWS CloudShell.	2021년 3월 22일

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