



Outposts 서버 사용 설명서

# AWS Outposts



# AWS Outposts: Outposts 서버 사용 설명서

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

# Table of Contents

AWS Outposts란 무엇인가요? .....	1
주요 개념 .....	1
AWS Outposts에 관한 자료 .....	2
요금 .....	5
AWS Outposts 작동 방식 .....	6
네트워크 구성 요소 .....	6
VPCs 및 서브넷 .....	7
라우팅 .....	7
DNS .....	8
서비스 링크 .....	8
로컬 네트워크 인터페이스 .....	9
사이트 요구 사항 .....	10
시설 .....	10
네트워킹 .....	11
서비스 링크 방화벽 .....	12
서비스 링크 최대 전송 단위 () MTU .....	12
서비스 링크 대역폭 권장 사항 .....	12
서비스 링크에는 DHCP 응답이 필요합니다. ....	13
서비스 링크 최대 지연 시간 .....	13
Power .....	13
전력 지원 .....	13
전력 소비량 .....	13
전원 케이블 .....	14
전원 이중화 .....	14
주문 이행 .....	14
시작 .....	16
Outpost를 생성하고 용량을 주문합니다. ....	16
1단계: 사이트 생성 .....	16
2단계: Outpost 생성 .....	17
3단계: 주문하기 .....	18
4단계: 인스턴스 용량 수정 .....	19
다음 단계 .....	21
인스턴스 시작 .....	21
1단계: 서브넷 생성 .....	22

2단계: Outpost에서 인스턴스 시작 .....	23
3단계: 연결 구성 .....	24
4단계: 연결 테스트 .....	24
서비스 링크 .....	27
서비스 링크를 통한 연결 .....	27
서비스 링크 최대 전송 단위 (MTU) 요구 사항 .....	28
서비스 링크 대역폭 권장 사항 .....	12
방화벽 및 서비스 링크 .....	28
업데이트 및 서비스 링크 .....	29
중복 인터넷 연결 .....	30
서버 반환 .....	31
1단계: 서버 반품 준비 .....	31
2단계: 반품 배송 라벨 받기 .....	32
3단계: 서버 포장 .....	32
4단계: 택배를 통해 서버 반송 .....	32
로컬 네트워크 인터페이스 .....	36
로컬 네트워크 인터페이스 기본 사항 .....	37
성능 .....	38
보안 그룹 .....	39
모니터링 .....	39
MAC주소 .....	39
로컬 네트워크 인터페이스 추가 .....	40
로컬 네트워크 인터페이스 보기 .....	41
운영 체제 구성 .....	41
로컬 연결 .....	41
네트워크의 서버 토폴로지 .....	41
서버 물리적 연결 .....	42
서버의 서비스 링크 트래픽 .....	43
로컬 네트워크 인터페이스 링크 트래픽 .....	43
서버 IP 주소 할당 .....	45
서버 등록 .....	45
공유 리소스 .....	46
공유 가능한 Outpost 리소스 .....	47
Outpost의 리소스 공유를 위한 사전 조건 .....	47
관련 서비스 .....	48
가용 영역 공유 .....	48

Outpost 리소스 공유 .....	48
공유된 Outpost 리소스 공유 해제 .....	49
공유 Outpost 리소스 식별 .....	50
공유 Outpost 리소스 권한 .....	51
소유자에 대한 권한 .....	51
소비자에 대한 권한 .....	51
결제 및 측정 .....	51
제한 사항 .....	51
보안 .....	52
데이터 보호 .....	52
저장 중 암호화 .....	53
전송 중 암호화 .....	53
데이터 삭제 .....	53
자격 증명 및 액세스 관리 .....	53
AWS Outposts와 함께 작동하는 방식 IAM .....	54
정책 예시 .....	59
서비스 연결 역할 .....	62
AWS 관리형 정책 .....	64
인프라 보안 .....	66
복원력 .....	67
규정 준수 확인 .....	67
모니터링 .....	69
CloudWatch 메트릭스 .....	70
지표 .....	70
미터식 치수 .....	73
.....	74
다음을 사용하여 API 통화를 기록합니다. CloudTrail .....	75
AWS Outposts 의 관리 이벤트 CloudTrail .....	76
AWS Outposts 이벤트 예제 .....	76
유지 관리 .....	78
하드웨어 유지 관리 .....	78
펌웨어 업데이트 .....	79
전력 및 네트워크 이벤트 .....	79
전력 이벤트 .....	79
네트워크 연결 이벤트 .....	80
리소스 .....	80

---

암호화 방식으로 파쇄된 서버 데이터 .....	81
E 옵션 nd-of-term .....	83
구독 갱신 .....	83
구독 종료 .....	84
구독 전환 .....	85
할당량 .....	86
AWS Outposts 그리고 다른 서비스에 대한 할당량 .....	86
문서 기록 .....	87
.....	lxxxviii

# AWS Outposts란 무엇인가요?

AWS Outposts AWS 인프라, 서비스 및 도구를 고객 사업장으로 확장하는 완전 관리형 서비스입니다. APIs AWS 관리형 인프라에 대한 로컬 액세스를 제공함으로써 고객은 AWS 지역과 동일한 프로그래밍 인터페이스를 사용하여 온프레미스에서 애플리케이션을 구축하고 실행하는 동시에 로컬 컴퓨팅 및 스토리지 리소스를 사용하여 지연 시간을 줄이고 로컬 데이터 처리 요구 사항을 줄일 수 있습니다. AWS Outposts

Outpost는 고객 사이트에 배포되는 AWS 컴퓨팅 및 스토리지 용량 풀입니다. AWS AWS 지역의 일부로서 이 용량을 운영, 모니터링 및 관리합니다. Outpost에서 서브넷을 생성하고 EC2 인스턴스 및 서브넷과 같은 AWS 리소스를 생성할 때 서브넷을 지정할 수 있습니다. Outpost 서브넷의 인스턴스는 모두 같은 사설 IP 주소를 사용하여 AWS 해당 지역의 다른 인스턴스와 통신합니다. VPC

## Note

아웃포스트를 같은 곳에 있는 다른 아웃포스트 또는 로컬 존에 연결할 수 없습니다. VPC

자세한 내용은 [AWS Outposts 제품 페이지](#)를 참조하세요.

## 주요 개념

의 핵심 개념은 다음과 같습니다. AWS Outposts

- 전초 기지 부지 — Outpost를 설치할 고객이 관리하는 물리적 건물. AWS 사이트는 Outpost에 대한 시설, 네트워킹 및 전원 요구 사항을 충족해야 합니다.
- Outpost 용량 – Outpost에서 사용할 수 있는 컴퓨팅 및 스토리지 리소스. AWS Outposts 콘솔에서 Outpost의 용량을 확인하고 관리할 수 있습니다.
- 전초 기지 장비 — 서비스에 대한 액세스를 제공하는 물리적 하드웨어. AWS Outposts 하드웨어에는 소유하고 관리하는 랙, 서버, 스위치 및 케이블이 포함됩니다. AWS
- Outpost 랙 – 업계 표준 42U 랙인 Outpost 폼 팩터입니다. Outposts 랙에는 랙 장착형 서버, 스위치, 네트워크 패치 패널, 전원 쉘프 및 블랭크 패널이 포함됩니다.
- Outposts 서버 — 업계 표준 1U 또는 2U 서버인 Outpost 폼 팩터로, 표준 EIA -310D 19 호환 4포트 랙에 설치할 수 있습니다. Outposts 서버는 공간이 제한적이거나 용량 요구 사항이 적은 사이트에 로컬 컴퓨팅 및 네트워킹 서비스를 제공합니다.

- 서비스 링크 — Outpost와 관련 AWS 지역 간의 통신을 가능하게 하는 네트워크 경로입니다. 각 Outpost는 가용 영역과 관련 리전의 확장본입니다.
- 로컬 게이트웨이 (LGW) - Outposts 랙과 온프레미스 네트워크 간의 통신을 지원하는 논리적 상호 연결 가상 라우터입니다.
- 로컬 네트워크 인터페이스 - Outposts 서버와 온-프레미스 네트워크에서 통신할 수 있게 해주는 네트워크 인터페이스입니다.

## AWS Outposts에 관한 자료

Outpost에서 다음 리소스를 생성하여 온프레미스 데이터 및 애플리케이션과 매우 가까운 거리에서 실행해야 하는 대기 시간이 짧은 워크로드를 지원할 수 있습니다.

### 컴퓨팅

리소스 유형	랙	서버
<a href="#">아마존 EC2 인스턴스</a>		
<a href="#">아마존 ECS 클러스터</a>		
<a href="#">아마존 EKS 노드</a>		 아 니 요

## 데이터베이스 및 분석

리소스 유형	랙	서버
Amazon ElastiCache 노드 ( <a href="#">레디스 클러스터</a> , <a href="#">메모리 캐시 클러스터</a> )		 아니요
<a href="#">아마존 EMR 클러스터</a>		 아니요
<a href="#">아마존 RDS DB 인스턴스</a>		 아니요

## 네트워킹

리소스 유형	랙	서버
<a href="#">App Mesh Envoy 프록시</a>		 예
<a href="#">Application Load Balancers</a>		 아니요
<a href="#">아마존 VPC 서브넷</a>		 예

리소스 유형	랙	서버
<a href="#">Amazon Route 53</a>		 아니요

스토리지

리소스 유형	랙	서버
<a href="#">아마존 EBS 볼륨</a>		 아니요
<a href="#">Amazon S3 버킷</a>		 아니요

기타 AWS 서비스

Service	랙	서버
AWS IoT Greengrass		 예
아마존 SageMaker 엣지 매니저		 예

## 요금

다양한 Outpost 구성 중에서 선택할 수 있으며, 각 구성은 EC2 인스턴스 유형과 스토리지 옵션의 조합을 제공합니다. 랙 구성 가격에는 설치, 제거 및 유지 관리가 포함됩니다. 서버의 경우 장비를 설치하고 유지 관리해야 합니다.

1년 또는 3년 약정으로 구성을 구매하면 전체 선결제, 부분 선결제, 선결제 없음의 세 가지 결제 옵션 중에서 선택할 수 있습니다. 부분 선결제 또는 선결제 없음 옵션을 선택하면 월별 요금이 적용됩니다. 모든 선결제 요금은 Outposts 랙이 활성화된 지 24시간 후, 즉 Outposts 랙 용량이 인스턴스를 시작하는 데 사용할 수 있게 되는 시점부터 적용됩니다. 자세한 내용은 다음을 참조하세요.

- [AWS Outposts 랙 가격](#)
- [AWS Outposts 서버 가격](#)

# AWS Outposts 작동 방식

AWS Outposts 전초 기지와 AWS 지역 간의 지속적이고 일관된 연결로 작동하도록 설계되었습니다. 리전 및 온프레미스 환경의 로컬 워크로드에 이렇게 연결하려면 Outpost를 온프레미스 네트워크에 연결해야 합니다. 온프레미스 네트워크는 지역 및 인터넷에 대한 광역 네트워크 (WAN) 액세스를 제공해야 합니다. 또한 온프레미스 워크로드 LAN 또는 애플리케이션이 있는 로컬 네트워크를 제공하거나 이에 WAN 대한 액세스를 제공해야 합니다.

다음은 Outpost 폼 팩터를 나타낸 다이어그램입니다.

## 내용

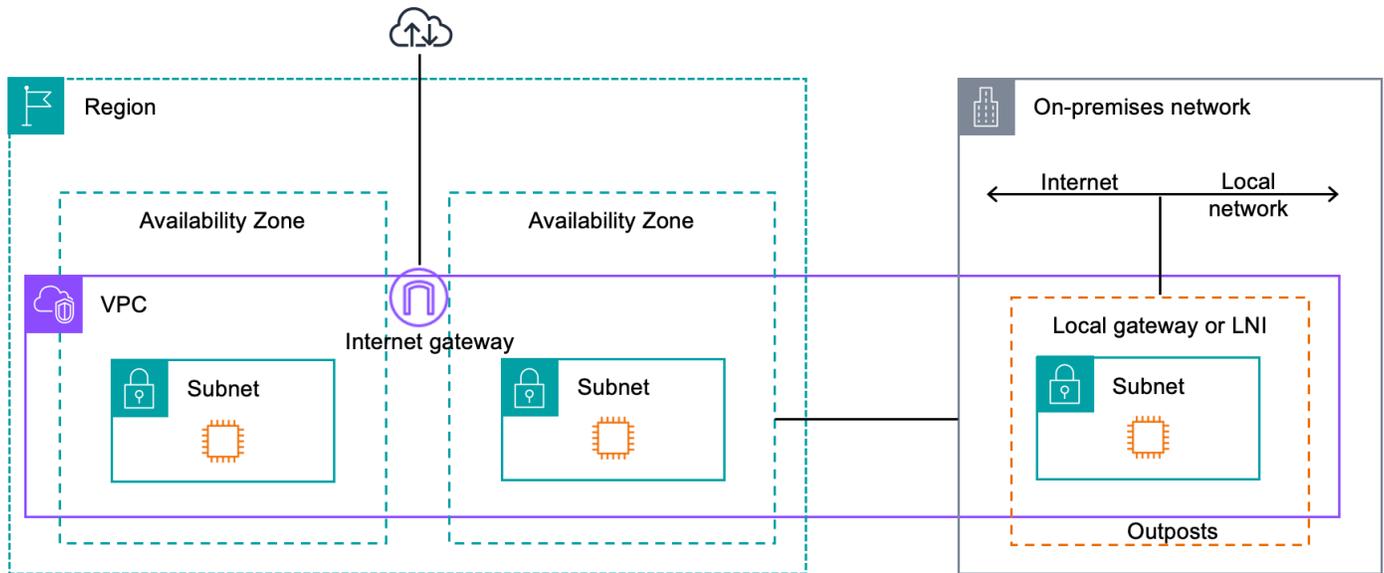
- [네트워크 구성 요소](#)
- [VPCs 및 서브넷](#)
- [라우팅](#)
- [DNS](#)
- [서비스 링크](#)
- [로컬 네트워크 인터페이스](#)

## 네트워크 구성 요소

AWS Outposts 인터넷 게이트웨이, 가상 사설 게이트웨이, Amazon VPC Transit Gateway, 엔드포인트 등 지역에서 액세스할 수 있는 VPC 구성 요소를 사용하여 VPC Amazon을 지역에서 Outpost로 확장합니다. AWS VPC Outpost는 리전의 가용 영역에 위치하며 복원력을 위해 사용할 수 있는 해당 가용 영역의 확장본입니다.

다음은 Outpost의 네트워크 구성 요소를 나타낸 다이어그램입니다.

- A AWS 리전 및 온프레미스 네트워크
- A: VPC 지역에 여러 서브넷이 있습니다.
- 온프레미스 네트워크 내의 Outpost
- 로컬 게이트웨이(랙) 또는 로컬 네트워크 인터페이스(서버)를 통해 제공되는 Outpost와 로컬 네트워크 간 연결



## VPCs 및 서브넷

가상 사설 클라우드 (VPC) 는 해당 AWS 지역의 모든 가용 영역을 포괄합니다. Outpost 서브넷을 추가하여 지역 VPC 내 원하는 지역을 Outpost로 확장할 수 있습니다. Outpost 서브넷을 VPC a에 추가하려면 서브넷을 생성할 때 Outpost의 Amazon 리소스 이름 (ARN) 을 지정하십시오.

Outpost는 여러 서브넷을 지원합니다. Outpost에서 인스턴스를 시작할 때 EC2 인스턴스 서브넷을 지정할 수 있습니다. EC2 Outpost는 AWS 컴퓨팅 및 스토리지 용량 풀이기 때문에 인스턴스가 배포되는 기본 하드웨어를 지정할 수 없습니다.

각 Outpost는 Outpost 서브넷을 하나 이상 포함할 수 VPCs 있는 여러 개를 지원할 수 있습니다. VPC할당량에 대한 자세한 내용은 Amazon 사용 [설명서의 Amazon VPC 할당량](#)을 참조하십시오. VPC

Outpost 서브넷은 Outpost를 만든 곳의 VPC CIDR VPC 범위에서 생성합니다. Outpost 서브넷에 있는 EC2 인스턴스와 같은 리소스에는 Outpost 주소 범위를 사용할 수 있습니다.

## 라우팅

기본적으로 모든 Outpost 서브넷은 해당 서브넷의 기본 라우팅 테이블을 상속합니다. VPC 사용자 지정 라우팅 테이블을 생성하여 Outpost 서브넷과 연결할 수 있습니다.

Outpost 서브넷의 라우팅 테이블은 가용 영역 서브넷의 라우팅 테이블과 동일하게 작동합니다. IP 주소, 인터넷 게이트웨이, 로컬 게이트웨이, 가상 프라이빗 게이트웨이 및 피어링 연결을 대상으로 지정할 수 있습니다. 예를 들어 상속된 기본 라우팅 테이블이나 사용자 지정 테이블을 통해 각 Outpost 서브

넷은 로컬 경로를 상속합니다. VPC 즉 VPC, 목적지가 있는 Outpost 서브넷을 포함하여 의 모든 트래픽 이 에서 라우팅된 상태를 유지합니다. VPC CIDR VPC

Outpost 서브넷 라우팅 테이블에는 다음 대상이 포함될 수 있습니다.

- VPC CIDR 범위 - 설치 시 이 AWS 값을 정의합니다. 이는 로컬 경로이며 동일한 VPC Outpost 인스턴스 간의 트래픽을 포함하여 모든 VPC 라우팅에 적용됩니다.
- AWS 지역 대상 — 여기에는 Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB 게이트웨이 엔드포인트 AWS Transit Gateway, 가상 프라이빗 게이트웨이, 인터넷 게이트웨이 및 피어링에 대한 접두사 목록이 포함됩니다. VPC

동일한 VPCs Outpost에 여러 개의 피어링 연결이 있는 경우 두 Outpost 간의 트래픽은 Outpost에 VPCs 남아 있으며 해당 지역으로 다시 연결되는 서비스 링크를 사용하지 않습니다.

## DNS

VPCa에 연결된 네트워크 인터페이스의 경우 Outposts 서브넷의 EC2 인스턴스는 Amazon Route 53 DNS 서비스를 사용하여 도메인 이름을 IP 주소로 확인할 수 있습니다. Route 53은 Outpost에서 실행 중인 인스턴스의 도메인 등록, DNS 라우팅, 상태 확인과 같은 DNS 기능을 지원합니다. 퍼블릭 호스팅 가용 영역과 프라이빗 호스팅 가용 영역 모두 트래픽을 특정 도메인으로 라우팅하는 데 지원됩니다. Route 53 리졸버는 지역에서 호스팅됩니다. AWS 따라서 이러한 DNS 기능이 작동하려면 Outpost에서 AWS 지역으로 다시 연결되는 서비스 링크 연결이 가동되고 실행되어야 합니다.

Outpost와 지역 간의 경로 지연 시간에 따라 Route 53을 사용하면 DNS 해결 시간이 더 오래 걸릴 수 있습니다. AWS 이 경우 온프레미스 환경에 로컬로 설치된 DNS 서버를 사용할 수 있습니다. 자체 DNS 서버를 사용하려면 온-프레미스 서버용 DHCP 옵션 세트를 만든 다음 DNS 해당 서버에 연결해야 합니다. VPC 또한 이러한 DNS 서버에 IP 연결이 가능한지 확인해야 합니다. 연결을 위해 로컬 게이트웨이 라우팅 테이블에 경로를 추가해야 할 수도 있지만 이는 로컬 게이트웨이가 있는 Outposts 랙에만 사용할 수 있습니다. DHCP 옵션 세트에는 VPC 범위가 있기 때문에 Outpost 서브넷과 의 가용 영역 서브넷 모두에 있는 인스턴스는 이름 확인을 위해 지정된 VPC 서버를 사용하려고 합니다. DNS DNS

Outpost에서 시작된 쿼리에는 DNS 쿼리 로깅이 지원되지 않습니다.

## 서비스 링크

서비스 링크는 Outpost에서 선택한 AWS 지역 또는 Outposts 홈 지역으로 다시 연결되는 링크입니다. 서비스 링크는 Outpost가 선택한 거주 지역과 통신할 때마다 사용되는 암호화된 VPN 연결 세트입니다. 가상 LAN (VLAN) 을 사용하여 서비스 링크의 트래픽을 분류합니다. 서비스 링크를 VLAN 사용하면

전초 기지 관리와 AWS 지역 및 전초 기지 간의 내부 VPC 트래픽 관리를 위한 전초 기지와 AWS 지역 간의 통신이 가능합니다.

Outpost가 프로비저닝되면 서비스 링크가 생성됩니다. 서버 폼 팩터가 있는 경우 연결을 생성합니다. 랙이 있는 경우, 서비스 링크를 AWS 생성합니다. 자세한 내용은 다음을 참조하세요.

- [아웃포스트 연결: AWS 리전](#)
- AWS Outposts 고가용성 설계 및 아키텍처 고려 사항 백서의 [애플리케이션/워크로드 라우팅](#) AWS

## 로컬 네트워크 인터페이스

Outposts 서버에는 온프레미스 네트워크에 대한 연결을 제공하는 로컬 네트워크 인터페이스가 포함되어 있습니다. 로컬 네트워크 인터페이스는 Outpost 서브넷에서 실행되는 Outpost 서버에서만 사용할 수 있습니다. Outposts 랙 또는 지역의 EC2 인스턴스에서는 로컬 네트워크 인터페이스를 사용할 수 없습니다. AWS 로컬 네트워크 인터페이스는 온프레미스 위치에서만 사용할 수 있습니다. 자세한 내용은 [Outposts 서버를 위한 로컬 네트워크 인터페이스](#)을(를) 참조하세요.

# Outposts 서버의 사이트 요구 사항

Outpost 사이트는 Outpost가 운영되는 물리적 장소입니다. 사이트는 일부 국가 및 지역에서만 사용할 수 있습니다. 자세한 내용은 [AWS Outposts 서버를 FAQs](#) 참조하십시오. 다음 질문을 참조하세요 - Outpost 서버를 사용할 수 있는 국가 및 영토는 어디입니까?

이 페이지에서는 Outpost 서버의 요구 사항을 다룹니다. Outposts 랙에 대한 요구 사항은 Outposts 랙 AWS Outposts 사용 설명서에서 Outposts 랙에 대한 [사이트 요구 사항](#)을 참조하십시오.

## 내용

- [시설](#)
- [네트워킹](#)
- [Power](#)
- [주문 이행](#)

## 시설

서버의 시설 요구 사항은 다음과 같습니다.

### Note

사양은 정상 작동 조건의 서버를 위한 것입니다. 예를 들어 초기 설치 시에는 음향이 더 크게 들리다가 설치가 완료된 후에는 정격 사운드 출력으로 작동할 수 있습니다.

- 온도 – 주변 온도는 41 ~ 95°F (5 ~ 35°C) 사이여야 합니다.

온도가 이 범위를 벗어나면 서버가 종료되고, 온도가 다시 해당 범위 내에 돌아오면 서버가 다시 시작됩니다.

- 습도 – 상대 습도는 8 ~ 80% 사이여야 하며 결로 현상이 없어야 합니다.
- 공기 품질 — MERV8 (또는 그 이상) 필터를 사용하여 공기를 필터링해야 합니다.
- 공기 흐름 – 충분한 공기 흐름 간격을 확보하기 위해 서버의 위치는 서버와 서버 앞뒤 벽 사이에 최소 6인치(15cm)의 간격을 두어야 합니다.
- 무게 – 1U 서버의 무게는 26파운드이고 2U 서버의 무게는 36파운드입니다. 서버를 배치하려는 위치가 서버의 무게를 지탱할 수 있는지 확인하세요.

다양한 Outposts 리소스의 무게 요구 사항을 확인하려면 AWS Outposts 콘솔에서 카탈로그 찾아보기를 선택하십시오. <https://console.aws.amazon.com/outposts/>

- 레일 키트 호환성 - 배송 패키지에 포함된 레일 키트는 EIA -310-D 호환 19인치 랙의 표준 L자형 장착 브래킷과 호환됩니다. 레일 키트는 다음 이미지에 표시된 U자형 장착 브래킷과 호환되지 않습니다.
- 랙 배치 - 최소 36인치 (914mm) 깊이의 표준 19인치 EIA -310D 랙을 사용하는 것이 좋습니다. AWS 서버를 랙에 장착하기 위한 레일 키트를 제공합니다.
  - Outposts 2U 서버에는 높이 3.5인치 (88.9mm), 너비 17.5인치 (447mm), 깊이 30인치 (762mm)의 공간이 필요합니다.
  - Outposts 1U 서버에는 높이 1.75인치 (44.45mm), 너비 17.5인치 (447mm), 깊이 24인치 (610mm)의 공간이 필요합니다.
  - 서버를 수직으로 장착하는 것은 지원되지 않습니다. AWS Outposts
  - Outposts 1U 서버는 Outposts 2U 서버와 너비가 같지만 높이는 절반이고 깊이는 작습니다.

서버를 랙에 배치하지 않는 경우에도 다른 사이트 요구 사항을 충족해야 합니다.

- 서비스 용이성 - Outpost 서버는 전면 통로에서 서비스가 가능합니다.
- 음향 — 27°C (80°F) 의 온도에서 사운드 파워가 78dBA 미만이며 GR-63 CORE NEBS 규정을 준수합니다.
- 지진 브레이싱 - 규정 또는 규정에서 요구하는 범위 내에서 서버가 시설에 있는 동안 적절한 지진 고정 장치 및 브레이스를 설치하고 유지 관리해야 합니다.
- 고도 - 랙이 설치된 공간의 고도는 10,005피트(3,050미터) 미만이어야 합니다.
- 청소 - 승인된 정전기 방지 세척제가 들어 있는 젖은 물티슈로 표면을 닦습니다.

## 네트워킹

각 Outposts 서버에는 중복되지 않은 물리적 업링크 포함되어 있습니다. 포트에는 아래에 자세히 설명된 바와 같이 자체 속도 및 커넥터 요구 사항이 있습니다.

포트 라벨	Speed	업스트림 네트워킹 장치의 커넥터	트래픽
Port 3	10Gbe	SFP+	서비스 및 LNI 링크 트래픽 모두 — QSFP +

포트 라벨	Speed	업스트림 네트워킹 장치의 커넥터	트래픽
			브레이크아웃 케이블 (10피트/3m) 은 트래픽을 분할합니다.

## 서비스 링크 방화벽

UDP 그리고 TCP 443은 방화벽에 안전하게 등록되어 있어야 합니다.

프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	1024~65535	서비스 링크 IP	53	DHCP제공된 서버 DNS
UDP	443, 1024-65535	서비스 링크 IP	443	Outposts 서비스 링크 엔드포인트
TCP	1024~65535	서비스 링크 IP	443	Outposts 등록 엔드포인트

AWS Direct Connect 연결 또는 공용 인터넷 연결을 사용하여 Outpost를 지역에 다시 연결할 수 있습니다. AWS Outposts 서비스 링크 연결의 경우 방화벽 또는 에지 NAT PAT 라우터에서 또는 를 사용할 수 있습니다. 서비스 링크 설정은 항상 Outpost에서 시작됩니다.

## 서비스 링크 최대 전송 단위 ( ) MTU

네트워크는 Outpost와 상위 지역의 서비스 링크 엔드포인트 MTU 사이에서 1500바이트를 지원해야 합니다. AWS 서비스 링크에 대한 자세한 내용은 서버 사용 설명서의 [AWS 지역AWS Outposts 연결을 참조하십시오.](#) AWS Outposts

## 서비스 링크 대역폭 권장 사항

최적의 경험과 복원력을 AWS 위해서는 지역에 대한 서비스 링크 연결에 최소 500Mbps의 이중 연결과 최대 175ms의 왕복 지연 시간을 사용해야 합니다. AWS 각 Outposts 서버의 최대 사용률은 500Mbps입니다. 연결 속도를 높이려면 여러 Outposts 서버를 사용하십시오. 예를 들어 AWS Outposts 서버

가 세 대인 경우 최대 연결 속도는 1.5Gbps(1,500Mbps)로 빨라집니다. 자세한 내용은 서버 AWS Outposts 사용 설명서의 [서버 서비스 링크 트래픽을](#) 참조하십시오.

AWS Outposts 서비스 링크 대역폭 요구 사항은 AMI 크기, 애플리케이션 탄력성, 버스트 속도 요구 사항, 지역으로의 Amazon VPC 트래픽과 같은 워크로드 특성에 따라 달라집니다. 단, AWS Outposts 서버는 AMIs 캐싱되지 않습니다. AMIs 인스턴스가 시작될 때마다 지역에서 다운로드됩니다.

요구 사항에 필요한 서비스 링크 대역폭에 대한 맞춤 권장 사항을 받으려면 AWS 영업 담당자 또는 APN 파트너에게 문의하십시오.

서비스 링크에는 DHCP 응답이 필요합니다.

서비스 링크에는 네트워크 설정을 구성하기 위한 IPv4 DHCP 응답이 필요합니다.

## 서비스 링크 최대 지연 시간

서비스 링크는 서버 및 가용 영역에서 최대 175ms의 네트워크 지연 시간을 지원할 수 있습니다.

## Power

Outpost 서버의 전력 요구 사항은 다음과 같습니다.

요구 사항

- [전력 지원](#)
- [전력 소비량](#)
- [전원 케이블](#)
- [전원 이중화](#)

## 전력 지원

서버의 정격 AC 전력은 최대 1600W 90-264VAC 47/63Hz입니다.

## 전력 소비량

다양한 Outposts 리소스의 전력 소비량 요구 사항을 보려면 AWS Outposts 콘솔에서 카탈로그 찾아보기를 선택하십시오. <https://console.aws.amazon.com/outposts/>

## 전원 케이블

서버에는 IEC C14-C13 전원 케이블이 함께 제공됩니다.

서버에서 랙으로 전원 케이블 연결

제공된 IEC C14-C13 전원 케이블을 사용하여 서버를 랙에 연결합니다.

서버와 벽면 콘센트의 전원 케이블 연결

서버를 표준 벽면 콘센트에 연결하려면 C14 콘센트용 어댑터 또는 국가별 전원 코드를 사용해야 합니다.

서버 설치 시 시간을 절약하려면 해당 리전에 맞는 어댑터나 전원 코드가 있는지 확인하세요.

- 미국의 경우 IEC NEMA C13~5-15P 전원 코드가 필요합니다.
- 유럽 일부 지역에서는 IEC CEE C13~7/7 전원 코드가 필요할 수 있습니다.
- 인도에서는 코드에 전원을 공급하기 위해 IEC IS1293 C13이 필요합니다.

## 전원 이중화

서버에는 다중 전원 연결이 포함되며 전원 중복 작동이 가능한 케이블이 함께 제공됩니다. 전원 이중화를 권장하지만 이중화가 필요하지는 않습니다.

서버에는 무정전 전원 공급 장치 () 가 포함되어 있지 않습니다. UPS

## 주문 이행

주문을 처리하기 위해 레일 마운트와 필요한 전원 및 네트워크 케이블을 포함한 Outposts 서버 장비를 AWS 귀하가 제공한 주소로 배송합니다. 서버가 배송되는 상자의 크기는 다음과 같습니다.

- 2U 서버가 포함된 박스:
  - 길이: 44인치/111.8cm
  - 높이: 26.5인치/67.3센티미터
  - 너비: 17인치/43.2센티미터
- 1U 서버가 포함된 박스:
  - 길이: 34.5인치/87.6센티미터
  - 높이: 24인치/61센티미터

- 너비: 9인치/22.9센티미터

사용자의 팀 또는 서드 파티 공급업체가 장비를 설치해야 합니다. 자세한 내용은 서버 AWS Outposts 사용 설명서의 [서버 서비스 링크 트래픽](#)을 참조하십시오.

Outposts 서버의 Amazon EC2 용량을 다음에서 사용할 수 있는지 확인하면 설치가 완료됩니다. AWS 계정

시작하려면 Outposts 서버를 주문하세요. Outpost 장비를 설치한 후 Amazon EC2 인스턴스를 시작하고 온프레미스 네트워크에 대한 연결을 구성합니다.

#### Tasks

- [Outpost를 생성하고 Outpost 용량을 주문합니다.](#)
- [Outposts 서버에서 인스턴스 시작](#)

## Outpost를 생성하고 Outpost 용량을 주문합니다.

사용을 AWS Outposts 시작하려면 Outpost를 소유할 AWS 계정으로 로그인하세요. 사이트와 Outpost를 생성합니다. 그런 다음 필요한 Outpost 서버를 주문합니다.

#### 사전 조건

- Outpost 서버에 [사용 가능한 구성](#)을 검토합니다.
- Outpost 사이트는 Outpost 장비가 배치되는 물리적 장소입니다. 용량을 주문하기 전에 사이트가 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [Outposts 서버의 사이트 요구 사항](#) 단원을 참조하십시오.
- AWS 엔터프라이즈 지원 플랜 또는 AWS 엔터프라이즈 온램프 지원 플랜이 있어야 합니다.
- 전초 기지를 AWS 계정 소유할 사람을 결정하십시오. 이 계정을 사용하여 Outpost 사이트를 생성하고 Outpost를 생성하고 주문합니다. 이 계정과 연결된 이메일에서 AWS정보를 확인하세요.

#### Tasks

- [1단계: 사이트 생성](#)
- [2단계: Outpost 생성](#)
- [3단계: 주문하기](#)
- [4단계: 인스턴스 용량 수정](#)
- [다음 단계](#)

### 1단계: 사이트 생성

사이트를 만들어 운영 주소를 지정합니다. 운영 주소는 Outpost 서버를 설치하고 실행할 위치입니다. 사이트를 만든 후 사이트에 ID를 AWS Outposts 할당합니다. Outpost를 생성할 때 이 사이트를 지정해야 합니다.

## 사전 조건

- 운영 주소를 결정합니다.

사이트를 생성하려면 다음과 같이 하세요.

1. Outpost를 AWS 계정 소유하게 될 계정을 AWS 사용하여 로그인하세요.
2. 에서 AWS Outposts 콘솔을 여세요. <https://console.aws.amazon.com/outposts/>
3. AWS 리전부모를 선택하려면 페이지 오른쪽 상단의 지역 선택기를 사용합니다.
4. 탐색 창에서 사이트를 선택합니다.
5. 사이트 생성을 선택합니다.
6. 지원되는 하드웨어 유형에서 서버만을 선택합니다.
7. 사이트의 이름, 설명, 운영 주소를 입력합니다.
8. (선택 사항) 사이트 노트의 경우 사이트에 대해 알아두면 유용할 수 있는 기타 정보를 입력합니다.  
AWS
9. 사이트 생성을 선택합니다.

## 2단계: Outpost 생성

각 서버에 대해 Outpost를 생성합니다. Outpost는 단일 서버와만 연결할 수 있습니다. 주문할 때 이 Outpost를 지정하게 됩니다.

### 사전 조건

- 사이트와 연결할 AWS 가용 영역을 결정하십시오.

Outpost를 생성하려면 다음과 같이 하세요.

1. 탐색 창에서 Outpost를 선택합니다.
2. Outpost 생성을 선택합니다.
3. 서버를 선택합니다.
4. Outpost에 대한 이름과 설명을 입력합니다.
5. Outpost의 가용 영역을 선택합니다.
6. 사이트 ID에서 사이트를 선택합니다.

7. Outpost 생성을 선택합니다.

## 3단계: 주문하기

필요한 Outposts 서버를 주문하세요.

### Important

제출한 후에는 주문을 수정할 수 없으므로 제출하기 전에 모든 세부 정보를 주의 깊게 검토하십시오. 주문을 변경해야 하는 경우 문의하세요 AWS Support.

### 사전 조건

- 주문 결제 방법을 결정합니다. 선결제 없음, 부분 선결제, 혹은 전체 선결제로 결제할 수 있습니다. 부분 선결제 또는 선결제 없음 옵션을 선택하면 계약 기간 동안 월별 요금을 지불하게 됩니다.

요금에는 제공, 인프라 서비스 유지 보수, 소프트웨어 패치 및 업그레이드가 포함됩니다.

- 배송 주소가 사이트에 지정한 운영 주소와 다른지 확인합니다.

주문하려면 다음과 같이 하세요.

1. 탐색 창에서 구매 주문을 선택합니다.
2. 주문하기를 선택합니다.
3. 지원되는 하드웨어 유형에서 서버를 선택합니다.
4. 용량을 추가하려면 구성을 선택합니다.
5. Next(다음)를 선택합니다.
6. 기존 Outpost 사용을 선택하고 Outpost를 선택합니다.
7. Next(다음)를 선택합니다.
8. 계약 기간 및 지불 옵션을 선택합니다.
9. 배송 주소를 지정합니다. 새 주소를 지정하거나 사이트 운영 주소를 선택할 수 있습니다. 운영 주소를 선택한 경우 향후 사이트 운영 주소에 대한 변경 사항이 기존 주문에는 적용되지 않는다는 점에 유의하십시오. 기존 주문의 배송 주소를 변경해야 하는 경우 계정 관리자에게 문의하세요.  
AWS
10. Next(다음)를 선택합니다.

11. 검토 및 주문 페이지에서 정보가 정확한지 확인하고 필요에 따라 수정합니다. 주문을 제출한 후에는 주문을 편집할 수 없습니다.
12. 주문하기를 선택합니다.

## 4단계: 인스턴스 용량 수정

각 새 Outpost 주문의 용량은 기본 용량 구성으로 구성됩니다. 기본 구성을 변환하여 비즈니스 요구 사항에 맞는 다양한 인스턴스를 만들 수 있습니다. 이렇게 하려면 용량 작업을 생성하고, 인스턴스 크기 및 수량을 지정하고, 용량 작업을 실행하여 변경을 구현해야 합니다.

### Note

- Outposts를 주문한 후 인스턴스 크기 수량을 변경할 수 있습니다.
- 인스턴스 크기 및 수량은 Outpost 수준에서 정의됩니다.
- 인스턴스는 모범 사례에 따라 자동으로 배치됩니다.

인스턴스 용량을 수정하려면

1. [AWS Outposts 콘솔의](#) AWS Outposts 왼쪽 탐색 창에서 용량 작업을 선택합니다.
2. 용량 작업 페이지에서 용량 작업 생성을 선택합니다.
3. 시작하기 페이지에서 순서를 선택합니다.
4. 용량을 수정하려면 콘솔의 단계를 사용하거나 JSON 파일을 업로드할 수 있습니다.

Console steps

1. 새 Outpost 용량 구성 수정을 선택합니다.
2. Next(다음)를 선택합니다.
3. 인스턴스 용량 구성 페이지에서 각 인스턴스 유형에는 최대 수량이 미리 선택된 인스턴스 크기가 하나씩 표시됩니다. 인스턴스 크기를 더 추가하려면 [Add instance size] 를 선택합니다.
4. 인스턴스 수량을 지정하고 해당 인스턴스 크기에 표시된 용량을 기록해 둡니다.
5. 각 인스턴스 유형 섹션의 끝에서 용량이 초과되었는지 또는 부족한지 알려주는 메시지를 확인하십시오. 인스턴스 크기 또는 수량 수준을 조정하여 총 가용 용량을 최적화하십시오.
6. 특정 인스턴스 크기에 맞게 인스턴스 수량을 AWS Outposts 최적화하도록 요청할 수도 있습니다. 그렇게 하려면 다음을 수행하세요.

- a. 인스턴스 크기를 선택합니다.
- b. 관련 인스턴스 유형 섹션 끝에서 Auto-Balance를 선택합니다.
7. 각 인스턴스 유형에 대해 최소 하나의 인스턴스 크기에 대해 인스턴스 수량을 지정해야 합니다.
8. Next(다음)를 선택합니다.
9. 검토 및 생성 페이지에서 요청하는 업데이트를 확인합니다.
10. 만들기를 선택합니다. AWS Outposts 용량 작업을 생성합니다.
11. 용량 작업 페이지에서 작업 상태를 모니터링합니다.

 Note

AWS Outposts 용량 작업을 실행할 수 있도록 하나 이상의 인스턴스 실행을 중지하도록 요청할 수 있습니다. 이러한 인스턴스를 AWS Outposts 중지하면 에서 작업을 실행합니다.

### Upload JSON file

1. 용량 구성 업로드를 선택합니다.
2. Next(다음)를 선택합니다.
3. 용량 구성 계획 업로드 페이지에서 인스턴스 유형, 크기, 수량을 지정하는 JSON 파일을 업로드합니다.

### Example

예제 JSON 파일:

```
{
  "RequestedInstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ]
}
```

```
    ]
  }
```

4. 용량 구성 계획 섹션에서 JSON 파일 내용을 검토하십시오.
5. Next(다음)를 선택합니다.
6. 검토 및 생성 페이지에서 요청하는 업데이트를 확인합니다.
7. 만들기를 선택합니다. AWS Outposts 용량 작업을 생성합니다.
8. 용량 작업 페이지에서 작업 상태를 모니터링합니다.

#### Note

AWS Outposts 용량 작업을 실행할 수 있도록 하나 이상의 인스턴스 실행을 중지하도록 요청할 수 있습니다. 이러한 인스턴스를 AWS Outposts 중지하면 에서 작업을 실행합니다.

## 다음 단계

AWS Outposts 콘솔을 사용하여 주문 상태를 볼 수 있습니다. 주문의 초기 상태는 주문 접수입니다. 주문에 대해 궁금한 점이 있으면 문의하세요 AWS Support.

주문을 처리하기 위해 배송 날짜를 정합니다. AWS

물리적 설치 및 네트워크 구성을 포함한 모든 설치 작업은 사용자가 담당합니다. 이 작업을 대신 수행하도록 타사와 계약할 수 있습니다. 설치를 하든 제3자와 계약을 맺든 관계없이 설치하려면 AWS 계정 Outpost가 포함된 사이트에 새 장치의 ID를 확인하기 위한 IAM 자격 증명이 필요합니다. 이러한 액세스를 제공하고 관리하는 것은 귀하의 책임입니다. 자세한 내용은 [서버 설치 안내서](#)를 참조하십시오.

Outpost의 Amazon EC2 용량이 다음에서 사용 가능해지면 설치가 완료됩니다. AWS 계정용량이 확보되면 Outposts 서버에서 Amazon EC2 인스턴스를 시작할 수 있습니다. 자세한 내용은 [the section called “인스턴스 시작”](#) 단원을 참조하십시오.

## Outposts 서버에서 인스턴스 시작

Outpost가 설치되고 컴퓨팅 및 스토리지 용량을 사용할 수 있게 되면 리소스를 생성하여 시작할 수 있습니다. 예를 들어 Amazon EC2 인스턴스를 시작할 수 있습니다.

### 전제 조건

사이트에 Outpost가 설치되어 있어야 합니다. 자세한 내용은 [Outpost를 생성하고 Outpost 용량을 주문합니다](#). 단원을 참조하세요.

## Tasks

- [1단계: 서브넷 생성](#)
- [2단계: Outpost에서 인스턴스 시작](#)
- [3단계: 연결 구성](#)
- [4단계: 연결 테스트](#)

## 1단계: 서브넷 생성

Outpost 서브넷은 Outpost의 AWS 지역 VPC 내 어느 곳이나 추가할 수 있습니다. 이렇게 하면 아웃포스트 VPC 전체에도 적용됩니다. 자세한 내용은 [네트워크 구성 요소](#) 단원을 참조하십시오.

### Note

다른 AWS 계정사람이 공유한 Outpost 서브넷에서 인스턴스를 시작하는 경우 으로 건너뛰십시오. [2단계: Outpost에서 인스턴스 시작](#)

Outpost 서브넷을 생성하려면 다음과 같이 하세요.

1. 에서 콘솔을 여십시오. AWS Outposts <https://console.aws.amazon.com/outposts/>
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 서브넷 생성을 선택합니다. Amazon VPC 콘솔에서 서브넷을 생성하도록 리디렉션됩니다. Outpost와 Outpost가 위치한 가용성 영역을 선택합니다.
4. a를 VPC 선택하고 서브넷의 IP 주소 범위를 지정합니다.
5. 생성(Create)을 선택합니다.
6. 서브넷을 생성한 후에는 로컬 네트워크 인터페이스용 서브넷을 활성화해야 합니다. AWS CLI의 [modify-subnet-attribute](#) 명령을 사용합니다. 장치 인덱스에서 네트워크 인터페이스의 위치를 지정해야 합니다. 활성화된 Outpost 서브넷에서 실행되는 모든 인스턴스는 로컬 네트워크 인터페이스에 이 장치 위치를 사용합니다. 다음 예에서는 값 1을 사용하여 보조 네트워크 인터페이스를 지정합니다.

```
aws ec2 modify-subnet-attribute \  
  --subnet-id subnet-1a2b3c4d \  
  --local-ipv6-addresses 1
```

```
--enable-lni-at-device-index 1
```

## 2단계: Outpost에서 인스턴스 시작

생성한 Outpost 서브넷 또는 공유된 Outpost 서브넷에서 EC2 인스턴스를 시작할 수 있습니다. 보안 그룹은 가용 영역 서브넷의 인스턴스와 마찬가지로 Outpost 서브넷의 인스턴스에 대한 인바운드 및 아웃바운드 VPC 트래픽을 제어합니다. Outpost 서브넷의 EC2 인스턴스에 연결하려면 가용 영역 서브넷의 인스턴스와 마찬가지로 인스턴스를 시작할 때 키 페어를 지정하면 됩니다.

### 고려 사항

- Outposts 서버의 인스턴스에는 인스턴스 스토어 볼륨이 포함되지만 볼륨은 포함되지 않습니다. EBS. 애플리케이션의 요구 사항을 충족하기에 충분한 인스턴스 스토리지가 있는 인스턴스 크기를 선택하십시오. 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 스토어 볼륨](#) 및 [인스턴스 스토어 지원 AMI 생성](#)을 참조하십시오.
- 단일 AMI EBS 스냅샷과 함께 Amazon EBS 기반 플랫폼을 사용해야 합니다. AMIs 두 개 이상의 EBS 스냅샷은 지원되지 않습니다.
- 인스턴스 스토어 볼륨의 데이터는 인스턴스 재부팅 후에도 유지되지만 인스턴스 종료 후에는 지속되지 않습니다. 인스턴스 수명 기간이 지난 후에도 인스턴스 스토어 볼륨에 장기 데이터를 유지하려면 Amazon S3 버킷이나 온 프레미스 네트워크의 네트워크 스토리지 장치와 같은 영구 스토리지에 데이터를 백업해야 합니다.
- Outpost 서브넷의 인스턴스를 온프레미스 네트워크에 연결하려면 다음 절차에 설명된 대로 [로컬 네트워크 인터페이스](#)를 추가해야 합니다.

Outpost 서브넷에서 인스턴스를 시작하려면 다음과 같이 하세요.

1. 에서 AWS Outposts 콘솔을 <https://console.aws.amazon.com/outposts/>여십시오.
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 인스턴트 시작을 선택합니다. Amazon EC2 콘솔의 인스턴스 시작 마법사로 리디렉션됩니다. Outpost 서브넷을 선택하여 Outposts 서버에서 지원하는 인스턴스 유형만 보여줍니다.
5. Outposts 서버에서 지원하는 인스턴스 유형을 선택합니다.
6. (선택 사항) 로컬 네트워크 인터페이스는 지금 또는 인스턴스를 생성한 후에 추가할 수 있습니다. 지금 추가하려면 고급 네트워크 구성을 확장하고 네트워크 인터페이스 추가를 선택합니다.

Outpost 서브넷을 선택합니다. 그러면 장치 인덱스 1을 사용하는 인스턴스용 네트워크 인터페이스가 생성됩니다. Outpost 서브넷의 로컬 네트워크 인터페이스 디바이스 인덱스로 1을 지정한 경우 이 네트워크 인터페이스는 인스턴스의 로컬 네트워크 인터페이스입니다. 또는 나중에 추가하려면 을 참조하십시오. [로컬 네트워크 인터페이스 추가](#)

7. 마법사를 완료하여 Outpost 서브넷에서 인스턴스를 시작합니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 [인스턴스 시작](#)을 참조하십시오.

### 3단계: 연결 구성

인스턴스 시작 중에 로컬 네트워크 인터페이스를 인스턴스에 추가하지 않았다면 지금 추가해야 합니다. 자세한 내용은 [로컬 네트워크 인터페이스 추가](#) 단원을 참조하십시오.

로컬 네트워크의 IP 주소를 사용하여 인스턴스의 로컬 네트워크 인터페이스를 구성해야 합니다. 일반적으로 다음을 사용하여 이 작업을 수행합니다DHCP. 자세한 내용은 인스턴스에서 실행되는 운영 체제의 설명서를 참조하세요. 추가 네트워크 인터페이스 및 보조 IP 주소 구성 정보를 검색합니다.

### 4단계: 연결 테스트

적절한 사용 사례를 사용하여 연결을 테스트할 수 있습니다.

로컬 네트워크에서 Outpost로의 연결을 테스트합니다.

로컬 네트워크의 컴퓨터에서 Outpost 인스턴스의 로컬 네트워크 인터페이스 IP 주소로 ping 명령을 실행합니다.

```
ping 10.0.3.128
```

출력의 예시는 다음과 같습니다.

```
Pinging 10.0.3.128

Reply from 10.0.3.128: bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128: bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128: bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets: Sent = 3, Received = 3, Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Outpost 인스턴스와 로컬 네트워크 간의 연결을 테스트합니다.

운영 체제에 따라 ssh 또는 rdp를 사용하여 Outpost 인스턴스의 프라이빗 IP 주소에 연결합니다. EC2 인스턴스 연결에 대한 자세한 내용은 Amazon EC2 사용 설명서의 EC2 [인스턴스에 연결](#)을 참조하십시오.

인스턴스가 실행된 후 로컬 네트워크에 있는 컴퓨터의 IP 주소로 ping 명령을 실행합니다. 다음 예제에서 IP 주소는 172.16.0.130입니다.

```
ping 172.16.0.130
```

출력의 예시는 다음과 같습니다.

```
Pinging 172.16.0.130

Reply from 172.16.0.130: bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130: bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130: bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets: Sent = 3, Received = 3, Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## AWS 지역과 Outpost 간의 연결성 테스트

지역의 서브넷에서 AWS 인스턴스를 시작합니다. 예를 들면 [run-instances](#) 명령을 실행합니다.

```
aws ec2 run-instances \  
  --image-id ami-abcdefghi1234567898 \  
  --instance-type c5.large \  
  --key-name MyKeyPair \  
  --security-group-ids sg-1a2b3c4d123456787 \  
  --subnet-id subnet-6e7f829e123445678
```

인스턴스가 실행된 후 다음 작업을 수행합니다.

1. AWS 지역 내 인스턴스의 프라이빗 IP 주소를 가져옵니다. 이 정보는 Amazon EC2 콘솔의 인스턴스 세부 정보 페이지에서 확인할 수 있습니다.

2. 운영 체제에 따라 Outpost 인스턴스의 프라이빗 IP 주소로 연결하는 데 ssh 또는 rdp을(를) 사용합니다.
3. Outpost 인스턴스에서 ping 명령을 실행하여 AWS 지역 내 인스턴스의 IP 주소를 지정합니다.

```
ping 10.0.1.5
```

출력의 예시는 다음과 같습니다.

```
Pinging 10.0.1.5
```

```
Reply from 10.0.1.5: bytes=32 time=<1ms TTL=128
```

```
Reply from 10.0.1.5: bytes=32 time=<1ms TTL=128
```

```
Reply from 10.0.1.5: bytes=32 time=<1ms TTL=128
```

```
Ping statistics for 10.0.1.5
```

```
Packets: Sent = 3, Received = 3, Lost = 0 (0% lost)
```

```
Approximate round trip time in milliseconds
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

# AWS Outposts AWS 지역과의 연결성

AWS Outposts 서비스 링크 연결을 통해 광역 네트워크 (WAN) 연결을 지원합니다.

## Note

Outposts 서버를 AWS 지역 또는 AWS Outposts 홈 지역에 연결하는 서비스 링크 연결에는 비공개 연결을 사용할 수 없습니다.

## 내용

- [서비스 링크를 통한 연결](#)
- [업데이트 및 서비스 링크](#)
- [중복 인터넷 연결](#)

## 서비스 링크를 통한 연결

AWS Outposts 프로비저닝 중에 Outpost를 선택한 AWS 지역 또는 AWS Outposts 거주 지역으로 다시 연결하는 서비스 링크 연결을 만들거나 AWS 생성합니다. 서비스 링크는 Outpost가 선택한 거주 지역과 통신할 때마다 사용되는 암호화된 VPN 연결 세트입니다. 가상 LAN (VLAN) 을 사용하여 서비스 링크의 트래픽을 분류합니다. 서비스 링크를 VLAN 사용하면 전초 기지 관리와 AWS 지역 및 전초 기지 간의 내부 VPC 트래픽 관리를 위한 전초 기지와 AWS 지역 간의 통신이 가능합니다.

전초 기지는 공공 AWS 지역 연결을 통해 해당 지역으로 VPN 다시 연결되는 서비스 링크를 만들 수 있습니다. 이를 위해 Outpost는 공용 인터넷 또는 AWS Direct Connect 공용 가상 인터페이스를 통해 AWS 해당 지역의 공용 IP 범위에 연결해야 합니다. 이 연결은 서비스 링크의 특정 경로를 통하거나 기본 VLAN 경로인 0.0.0.0/0을 통해 이루어질 수 있습니다. AWS의 공용 범위에 대한 자세한 내용은 [AWS IP 주소 범위](#)를 참조하세요.

서비스 링크가 설정되면 Outpost가 서비스 중이며 에서 관리합니다. AWS 서비스 링크는 다음 트래픽에 사용됩니다.

- 내부 컨트롤 플레인 트래픽, 내부 리소스 모니터링, 펌웨어 및 소프트웨어 업데이트를 포함하여 서비스 링크를 통해 Outpost로 전달되는 관리 트래픽.
- Outpost와 고객 데이터 플레인 트래픽을 VPCs 포함한 모든 관련 기관 간의 트래픽.

## 서비스 링크 최대 전송 단위 (MTU) 요구 사항

네트워크 연결의 최대 전송 단위 (MTU) 는 연결을 통해 전달될 수 있는 최대 허용 패킷의 크기 (바이트) 입니다. 네트워크는 상위 지역의 Outpost와 서비스 링크 엔드포인트 MTU 사이에서 1500바이트를 지원해야 합니다. AWS 서비스 링크를 통해 Outpost의 인스턴스와 AWS 지역 내 인스턴스 MTU 사이에 필요한 [사항에 대한 자세한 내용은 Amazon EC2사용 설명서의 Amazon EC2 인스턴스의 네트워크 최대 전송 단위 \(MTU\) 를 참조하십시오.](#)

## 서비스 링크 대역폭 권장 사항

최적의 경험과 탄력성을 AWS 위해서는 지역에 대한 서비스 링크 연결에 최소 500Mbps의 중복 연결과 최대 175ms의 왕복 지연 시간을 사용해야 합니다. AWS 각 Outposts 서버의 최대 사용률은 500Mbps 입니다. 연결 속도를 높이려면 여러 Outposts 서버를 사용하십시오. 예를 들어 AWS Outposts 서버가 세 대인 경우 최대 연결 속도는 1.5Gbps(1,500Mbps)로 빨라집니다. 자세한 내용은 [서버의 서비스 링크 트래픽을 참조하십시오.](#)

AWS Outposts 서비스 링크 대역폭 요구 사항은 AMI 크기, 애플리케이션 탄력성, 버스트 속도 요구 사항, 지역으로의 Amazon VPC 트래픽과 같은 워크로드 특성에 따라 달라집니다. 단, AWS Outposts 서버는 AMIs 캐싱되지 않습니다. AMIs 인스턴스가 시작될 때마다 지역에서 다운로드됩니다.

요구 사항에 필요한 서비스 링크 대역폭에 대한 맞춤 권장 사항을 받으려면 AWS 영업 담당자 또는 APN 파트너에게 문의하십시오.

## 방화벽 및 서비스 링크

이 섹션에서는 방화벽 구성 및 서비스 링크 연결에 대해 설명합니다.

다음 다이어그램에서 구성은 Amazon을 AWS 지역에서 VPC Outpost로 확장합니다. AWS Direct Connect 퍼블릭 가상 인터페이스는 서비스 링크 연결입니다. 다음 트래픽은 서비스 링크와 AWS Direct Connect 연결을 거칩니다.

- 서비스 링크를 통해 Outpost로 유입되는 관리 트래픽
- Outpost와 관련 기관 간의 트래픽 VPCs

인터넷 연결과 함께 상태 저장 방화벽을 사용하여 공용 인터넷에서 서비스 VLAN 링크로의 연결을 제한하는 경우 인터넷에서 시작되는 모든 인바운드 연결을 차단할 수 있습니다. 이는 서비스 링크가 전초 기지에서 해당 지역으로만 VPN 시작되고 지역에서 전초 기지로는 시작되지 않기 때문입니다.

방화벽을 사용하여 서비스 VLAN 링크의 연결을 제한하는 경우 모든 인바운드 연결을 차단할 수 있습니다. 다음 표에 따라 AWS 지역에서 Outpost로의 아웃바운드 연결을 다시 허용해야 합니다. 방화벽이 상태 저장 상태인 경우 Outpost에서 허용된 아웃바운드 연결, 즉 Outpost에서 시작된 연결은 다시 인바운드로 허용되어야 합니다.

프로토콜	소스 포트	소스 주소	대상 포트	대상 주소
UDP	1024~65535	서비스 링크 IP	53	DHCP제공된 DNS 서버
UDP	443, 1024-65535	서비스 링크 IP	443	AWS Outposts 서비스 링크 엔드포인트
TCP	1024~65535	서비스 링크 IP	443	AWS Outposts 등록 엔드포인트

#### Note

Outpost의 인스턴스는 서비스 링크를 사용하여 다른 Outposts의 인스턴스와 통신할 수 없습니다. 로컬 게이트웨이 또는 로컬 네트워크 인터페이스를 통한 라우팅을 활용하여 Outpost 간에 통신할 수 있습니다.

## 업데이트 및 서비스 링크

AWS Outposts 서버와 상위 AWS 지역 간의 보안 네트워크 연결을 유지합니다. 서비스 링크라고 하는 이 네트워크 연결은 Outpost와 지역 간에 내부 VPC 트래픽을 제공하여 Outpost를 관리하는 데 필수적입니다. AWS [AWS Well-Architected](#) 모범 사례에서는 액티브-액티브 디자인을 사용하여 서로 다른 가용 영역의 부모인 두 Outposts에 애플리케이션을 배포할 것을 권장합니다. [자세한 내용은고가용성 설계 및 아키텍처 고려 사항을 참조하십시오AWS Outposts](#).

서비스 링크는 운영 품질 및 성능을 유지하기 위해 정기적으로 업데이트됩니다. 유지 관리 중에 이 네트워크에서 짧은 기간의 지연 시간 및 패킷 손실이 발생하여 지역 내 호스팅되는 VPC 리소스와의 연결에 따라 달라지는 워크로드에 영향을 미칠 수 있습니다. 하지만 [로컬 네트워크 인터페이스 \(LNI\)](#)를 통과하는 트래픽은 영향을 받지 않습니다. [AWS Well-Architected](#) 모범 사례를 따르고 단일 Outposts 서

버에 영향을 미치는 장애 또는 유지 관리 활동에 대해 애플리케이션이 [복원되도록](#) 하면 애플리케이션에 미치는 영향을 피할 수 있습니다.

## 중복 인터넷 연결

Outpost에서 AWS 지역으로 연결을 구축할 때는 가용성과 복원력을 높이기 위해 여러 연결을 만드는 것이 좋습니다. 자세한 내용은 [AWS Direct Connect 복원력 권장 사항](#)을 참조하세요.

공용 인터넷에 연결해야 하는 경우, 기존 온프레미스 워크로드와 마찬가지로 중복 인터넷 연결과 다양한 인터넷 공급자를 사용할 수 있습니다.

# Outposts 서버 반납

서버에서 결함이 AWS Outposts 발견되면 알려 드리고 교체 프로세스를 시작하여 새 서버를 보내고 콘솔을 통해 배송 라벨을 제공합니다. AWS Outposts 시작하려면 다음 단계를 완료하세요.

## Tasks

- [1단계: 서버 반품 준비](#)
- [2단계: 반품 배송 라벨 받기](#)
- [3단계: 서버 포장](#)
- [4단계: 택배를 통해 서버 반송](#)

서버가 계약 기간이 만료되었거나 다른 이유로 인해 서버를 반품하려면 [AWS Support 센터에](#) 문의하세요.

## 1단계: 서버 반품 준비

반환을 위해 서버를 준비하려면 리소스 공유를 해제하고, 데이터를 백업하고, 로컬 네트워크 인터페이스를 삭제하고, 활성 인스턴스를 종료하세요.

1. Outpost의 리소스를 공유하는 경우 해당 리소스의 공유를 해제해야 합니다.

다음 방법 중 하나로 공유 Outpost 리소스의 공유를 취소할 수 있습니다.

- AWS RAM 콘솔을 사용하세요. 자세한 내용은 AWS RAM 사용 설명서에서 [리소스 공유 업데이트](#)를 참조하세요.
- 를 AWS CLI 사용하여 [disassociate-resource-share](#) 명령을 실행합니다.

공유할 수 있는 Outpost 리소스 목록은 [공유 가능한 Outpost 리소스](#)를 참조하세요.

2. AWS Outposts 서버에서 실행되는 Amazon EC2 인스턴스의 인스턴스 스토리지에 저장된 데이터의 백업을 생성합니다.
3. 서버에서 실행 중인 인스턴스와 연결된 로컬 네트워크 인터페이스를 삭제합니다.
4. Outpost의 서브넷과 연결된 활성 인스턴스를 종료하세요. 인스턴스를 종료하려면 Amazon 사용 EC2 설명서의 [인스턴스 종료](#)에 있는 지침을 따르십시오.

## 2단계: 반품 배송 라벨 받기

### Important

제공된 배송 라벨만 사용해야 AWS 합니다. 배송 라벨을 직접 만들지 마세요.

반환 사유에 따라 배송 라벨을 받으세요.

Shipping label for a server that is being replaced

1. 에서 AWS Outposts 콘솔을 <https://console.aws.amazon.com/outposts/> 여십시오.
2. 탐색 창에서 주문을 선택합니다.
3. 교체 주문 요약에서 반환 라벨 인쇄를 선택하고 반환하려는 서버의 구성 ID를 선택합니다.

Shipping label for a server that is not being replaced

1. [AWS Support 센터](#)로 문의하세요.
2. 반환하려는 서버의 배송 라벨을 요청하세요.

## 3단계: 서버 포장

서버를 포장하려면 서버가 원래 들어 있던 상자와 포장재를 사용합니다. 교체 서버가 들어 있는 상자를 사용할 수도 있습니다. 또는 [AWS Support 센터](#)에 문의하여 박스를 요청하세요. 서버를 포장한 후 AWS 제공된 배송 라벨을 부착합니다.

## 4단계: 택배를 통해 서버 반송

해당 국가의 지정된 택배사를 통해 서버를 반환해야 합니다. 택배사에 서버를 배송하거나 택배사가 서버를 픽업하도록 원하는 날짜 및 시간을 예약할 수 있습니다. 제공된 배송 라벨에는 서버를 반품하기 위한 올바른 주소가 포함되어 있습니다. AWS

다음 표에는 배송 대상 국가의 연락처 정보가 나와 있습니다.

국가	연락처
아르헨티나	<p><a href="#">AWS Support 센터</a>로 문의하세요. 요청 시 다음 정보를 제공합니다.</p> <ul style="list-style-type: none"> <li>• AWS제공된 배송 라벨에 있는 추적 번호</li> <li>• 택배사가 서버를 픽업하기를 원하는 날짜 및 시간</li> <li>• 담당자 이름</li> <li>• 전화번호</li> <li>• 이메일 주소</li> </ul>
바레인	
브라질	
브루나이	
캐나다	
칠레	
콜롬비아	
홍콩	
인도	
인도네시아	
일본	
말레이시아	
나이지리아	
오만	
파나마	
페루	
필리핀	
세르비아	
싱가포르	
남아프리카공화국	

국가	연락처
대한민국	
대만	
태국	
아랍 에미리트 연합국	
베트남	
30	<p>연락처 <a href="#">UPS</a>.</p> <p>다음과 같은 방법으로 서버를 반환할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 사이트에서 정기적으로 UPS 픽업하는 동안 서버를 반납하십시오.</li> <li>• 서버를 특정 <a href="#">UPS위치에</a> 반납하십시오.</li> <li>• 원하는 날짜와 시간으로 <a href="#">픽업</a>을 예약하세요. 무료 배송을 위해 AWS제공된 배송 라벨의 추적 번호를 입력하십시오.</li> </ul>

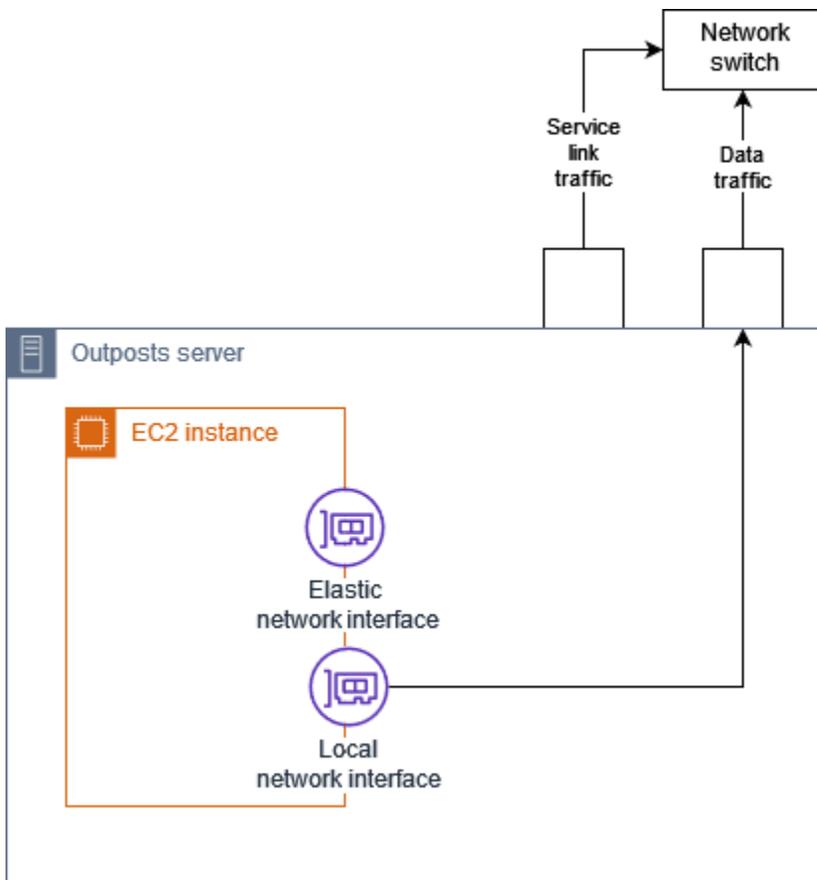
국가	연락처
기타 모든 국가	<p>연락처 <a href="#">DHL</a>.</p> <p>다음과 같은 방법으로 서버를 반환할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 서버를 특정 <a href="#">DHL위치에</a> 반납하십시오.</li> <li>• 원하는 날짜와 시간으로 <a href="#">픽업</a>을 예약하세요. 무료 배송을 DHL 받으려면 AWS제공된 배송 라벨의 운송장 번호를 입력하십시오.</li> </ul> <p>다음 오류 Courier pickup can't be scheduled for an import shipment(이)가 발생하는 경우, 일반적으로 선택한 픽업 국가가 반환 배송 라벨의 픽업 국가와 일치하지 않는다는 의미입니다. 배송지 국가를 선택하고 다시 시도하십시오.</p>

## Outposts 서버를 위한 로컬 네트워크 인터페이스

Outposts 서버에서 로컬 네트워크 인터페이스는 Outposts 서브넷의 Amazon EC2 인스턴스를 온프레미스 네트워크에 연결하는 논리적 네트워킹 구성 요소입니다.

로컬 네트워크 인터페이스는 근거리 통신망에서 직접 실행됩니다. 이러한 유형의 로컬 연결을 사용하면 온프레미스 장비와 통신하는 데 라우터나 게이트웨이가 필요하지 않습니다. 로컬 네트워크 인터페이스의 이름은 네트워크 인터페이스 또는 탄력적 네트워크 인터페이스와 비슷합니다. 로컬 네트워크 인터페이스를 참고할 때는 항상 로컬을 사용하여 두 인터페이스를 구분합니다.

Outpost 서브넷에서 로컬 네트워크 인터페이스를 활성화한 후, Elastic 네트워크 인터페이스 외에 로컬 네트워크 인터페이스를 포함하도록 Outpost 서브넷의 EC2 인스턴스를 구성할 수 있습니다. 로컬 네트워크 인터페이스는 온프레미스 네트워크에 연결되고 네트워크 인터페이스는 온프레미스 네트워크에 연결됩니다. VPC 다음 다이어그램은 Elastic Network 인터페이스와 로컬 네트워크 인터페이스를 모두 갖춘 Outposts 서버의 EC2 인스턴스를 보여줍니다.



다른 온프레미스 장비와 마찬가지로 로컬 네트워크 인터페이스가 근거리 통신망에서 통신할 수 있도록 운영 체제를 구성해야 합니다. 로컬 네트워크 인터페이스는 근거리 통신망에서 실행되므로 a의 DHCP 옵션 세트를 사용하여 로컬 네트워크 인터페이스를 구성할 수 없습니다. VPC

탄력적 네트워크 인터페이스는 가용 영역 서브넷의 인스턴스와 동일하게 작동합니다. 예를 들어, VPC 네트워크 연결을 사용하여 공용 지역 엔드포인트에 액세스하거나 인터페이스 VPC 엔드포인트를 사용하여 액세스할 AWS 서비스 수 있습니다. AWS 서비스 AWS PrivateLink 자세한 내용은 [AWS Outposts AWS 지역과의 연결성](#) 단원을 참조하십시오.

## 내용

- [로컬 네트워크 인터페이스 기본 사항](#)
- [Outposts 서브넷의 EC2 인스턴스에 로컬 네트워크 인터페이스 추가](#)
- [Outposts 서버를 위한 로컬 네트워크 연결](#)

## 로컬 네트워크 인터페이스 기본 사항

로컬 네트워크 인터페이스는 물리적 계층 2 네트워크에 대한 액세스를 제공합니다. A는 가상화된 레이어 3 VPC 네트워크입니다. 로컬 네트워크 인터페이스는 네트워킹 구성 요소를 지원하지 VPC 않습니다. 이러한 구성 요소에는 보안 그룹, 네트워크 액세스 제어 목록, 가상화된 라우터 또는 라우팅 테이블, 플로우 로그가 포함됩니다. 로컬 네트워크 인터페이스는 Outposts 서버에 VPC 계층 3 흐름에 대한 가시성을 제공하지 않습니다. 인스턴스의 호스트 운영 체제는 물리적 네트워크의 프레임을 완벽하게 파악할 수 있습니다. 이러한 프레임 내의 정보에 표준 방화벽 로직을 적용할 수 있습니다. 하지만 이러한 통신은 인스턴스 내부에서 이루어지지만 가상화된 구조의 범위 밖에서는 이루어집니다.

## 고려 사항

- 로컬 네트워크 인터페이스 지원 ARP 및 프로토콜. DHCP 일반 L2 브로드캐스트 메시지는 지원하지 않습니다.
- 로컬 네트워크 인터페이스 할당량은 네트워크 인터페이스 할당량에서 차감됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 [네트워크 인터페이스 할당량](#)을 참조하십시오.
- 각 EC2 인스턴스는 하나의 로컬 네트워크 인터페이스를 가질 수 있습니다.
- 로컬 네트워크 인터페이스는 인스턴스의 기본 네트워크 인터페이스를 사용할 수 없습니다.
- Outposts 서버는 각각 로컬 네트워크 인터페이스를 가진 여러 EC2 인스턴스를 호스팅할 수 있습니다.

**Note**

EC2동일한 서버 내의 인스턴스는 Outposts 서버 외부로 데이터를 보내지 않고 직접 통신할 수 있습니다. 이 통신에는 로컬 네트워크 인터페이스 또는 탄력적 네트워크 인터페이스를 통한 트래픽이 포함됩니다.

- 로컬 네트워크 인터페이스는 Outposts 서버의 Outposts 서브넷에서 실행되는 인스턴스에만 사용할 수 있습니다.
- 로컬 네트워크 인터페이스는 프로미스큐어스 모드 또는 주소 스푸핑을 지원하지 않습니다. MAC

## 성능

각 인스턴스 크기의 로컬 네트워크 인터페이스는 물리적 10GbE 가용 대역폭의 일부를 제공합니다. 다음 표에는 각 인스턴스 유형의 네트워크 성능이 나와 있습니다.

인스턴스 유형	기준 대역폭(Gbps)	버스트 대역폭(Gbps)
c6id.large	0.15625	2.5
c6id.xlarge	0.3125	2.5
c6id.2xlarge	0.625	2.5
c6id.4xlarge	1.25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3.75	3.75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10
c6gd.medium	0.15625	4
c6gd.large	0.3125	4

인스턴스 유형	기준 대역폭(Gbps)	버스트 대역폭(Gbps)
c6gd.xlarge	0.625	4
c6gd.2xlarge	1.25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

## 보안 그룹

로컬 네트워크 인터페이스는 설계상 사용자의 VPC 보안 그룹을 사용하지 않습니다. 보안 그룹은 인바운드 및 아웃바운드 VPC 트래픽을 제어합니다. 로컬 네트워크 인터페이스가 에 연결되어 있지 않습니다. VPC 로컬 네트워크 인터페이스는 로컬 네트워크에 연결됩니다. 로컬 네트워크 인터페이스의 인바운드 및 아웃바운드 트래픽을 제어하려면 온프레미스 장비의 나머지 부분과 마찬가지로 방화벽이나 유사한 전략을 사용합니다.

## 모니터링

CloudWatch 메트릭은 엘라스틱 네트워크 인터페이스와 마찬가지로 각 로컬 네트워크 인터페이스에 대해 생성됩니다. 자세한 내용은 Amazon EC2 사용 설명서의 EC2 [인스턴스 ENA 설정에 대한 네트워크 성능 모니터링](#)을 참조하십시오.

## MAC주소

AWS 로컬 네트워크 인터페이스의 MAC 주소를 제공합니다. 로컬 네트워크 인터페이스는 해당 MAC 주소로 로컬에서 관리되는 주소 (LAA) 를 사용합니다. 로컬 네트워크 인터페이스는 인터페이스를 삭제할 때까지 동일한 MAC 주소를 사용합니다. 로컬 네트워크 인터페이스를 삭제한 후에는 로컬 구성에서 MAC 주소를 제거합니다. AWS 더 이상 사용하지 않는 MAC 주소를 재사용할 수 있습니다.

# Outposts 서브넷의 EC2 인스턴스에 로컬 네트워크 인터페이스 추가

시작 도중 또는 이후에 Outposts 서브넷의 Amazon EC2 인스턴스에 로컬 네트워크 인터페이스를 추가할 수 있습니다. 로컬 네트워크 인터페이스용 Outpost 서브넷을 활성화할 때 지정한 장치 인덱스를 사용하여 인스턴스에 보조 네트워크 인터페이스를 추가하면 됩니다.

## 고려 사항

콘솔을 사용하여 보조 네트워크 인터페이스를 지정하면 장치 인덱스 1을 사용하여 네트워크 인터페이스가 생성됩니다. 로컬 네트워크 인터페이스용 Outpost 서브넷을 활성화할 때 지정한 디바이스 인덱스가 이 인덱스가 아닌 경우, 또는 를 대신 사용하여 올바른 디바이스 인덱스를 지정할 수 있습니다. AWS CLI AWS SDK 예를 들어, AWS CLI: [create-network-interface](#) 및 에서 다음 명령을 사용하십시오. [attach-network-interface](#)

인스턴스를 시작한 후 다음 절차를 사용하여 로컬 네트워크 인터페이스를 추가합니다. 인스턴스 시작 시 인스턴스 추가에 대한 자세한 내용은 [Outpost에서 인스턴스 시작](#)을 참조하십시오.

## 인스턴스에 EC2 로컬 네트워크 인터페이스 추가하기

1. 에서 Amazon EC2 콘솔을 엽니다 <https://console.aws.amazon.com/ec2/>.
2. 탐색 창에서 네트워크 및 보안 네트워크 인터페이스를 선택합니다.
3. 네트워크 인터페이스 생성
  - a. 네트워크 인터페이스 생성을 선택합니다.
  - b. 인스턴스와 동일한 Outpost 서브넷을 선택합니다.
  - c. 개인 IPv4 주소가 자동 할당으로 설정되어 있는지 확인합니다.
  - d. 보안 그룹을 선택합니다. 보안 그룹은 로컬 네트워크 인터페이스에 적용되지 않으므로 선택한 보안 그룹은 관련이 없습니다.
  - e. 네트워크 인터페이스 생성을 선택합니다.
4. 인스턴스에 네트워크 인터페이스 연결
  - a. 새로 생성한 네트워크 인터페이스의 확인란을 선택합니다.
  - b. 작업], 연결을 선택합니다.
  - c. 인스턴스를 선택합니다.
  - d. 연결을 선택합니다. 네트워크 인터페이스는 장치 인덱스 1에 연결됩니다. Outpost 서브넷의 로컬 네트워크 인터페이스에 대한 장치 인덱스로 1을 지정한 경우 이 네트워크 인터페이스는 인스턴스의 로컬 네트워크 인터페이스입니다.

## 로컬 네트워크 인터페이스 보기

인스턴스가 실행 상태인 동안 Amazon EC2 콘솔을 사용하여 Outpost 서브넷에 있는 인스턴스의 Elastic network 인터페이스와 로컬 네트워크 인터페이스를 모두 볼 수 있습니다. 인스턴스를 선택하고 네트워킹 탭을 선택합니다.

콘솔에는 서브넷의 로컬 네트워크 인터페이스 전용 IPv4 주소가 표시됩니다. CIDR 이 주소는 로컬 네트워크 인터페이스의 IP 주소가 아니므로 사용할 수 없습니다. 하지만 이 주소는 서브넷에서 할당되므로 서브넷 CIDR 크기를 조정할 때 이 주소를 고려해야 합니다. 게스트 운영 체제 내에서 로컬 네트워크 인터페이스의 IP 주소를 정적으로 설정하거나 서버를 통해 설정해야 합니다. DHCP

## 운영 체제 구성

로컬 네트워크 인터페이스를 활성화하면 Amazon EC2 인스턴스는 두 개의 네트워크 인터페이스를 갖게 되며, 그 중 하나는 로컬 네트워크 인터페이스입니다. 시작하는 Amazon EC2 인스턴스의 운영 체제가 멀티홈 네트워킹 구성을 지원하도록 구성해야 합니다.

## Outposts 서버를 위한 로컬 네트워크 연결

이 항목을 사용하면 Outposts 서버를 호스팅하기 위한 네트워크 케이블 연결 및 토폴로지 요구 사항을 이해할 수 있습니다. 자세한 내용은 [Outposts 서버를 위한 로컬 네트워크 인터페이스](#) 단원을 참조하십시오.

### 콘텐츠

- [네트워크의 서버 토폴로지](#)
- [서버 물리적 연결](#)
- [서버의 서비스 링크 트래픽](#)
- [로컬 네트워크 인터페이스 링크 트래픽](#)
- [서버 IP 주소 할당](#)
- [서버 등록](#)

## 네트워크의 서버 토폴로지

Outposts 서버에는 네트워킹 장비에 대한 두 개의 개별 연결이 필요합니다. 각 연결은 서로 다른 케이블을 사용하며 서로 다른 유형의 트래픽을 전달합니다. 여러 케이블은 트래픽 등급 격리용이며 이중화 용은 아닙니다. 두 케이블을 공통 네트워크에 연결할 필요는 없습니다.

다음 표에서는 Outposts 서버 트래픽 유형 및 레이블에 대해 설명합니다.

트래픽 라벨	설명
2	서비스 링크 트래픽 — 이 트래픽을 통해 전초 기지 관리 및 AWS 지역과 전초 기지 간의 내부 VPC 트래픽 모두를 위한 전초 기지와 AWS 지역 간의 통신이 가능합니다. 서비스 링크 트래픽에는 Outpost에서 리전으로의 서비스 링크 연결이 포함됩니다. 서비스 링크는 사용자 지정 VPN 링크이거나 전초 VPNs 기지에서 해당 지역으로 연결되는 링크입니다. Outpost는 구매 시 선택한 리전의 가용 영역에 연결됩니다.
1	로컬 네트워크 인터페이스 링크 트래픽 — 이 트래픽을 통해 로컬 네트워크 인터페이스를 LAN 통해 사용자와 로컬 간에 VPC 통신할 수 있습니다. 로컬 링크 트래픽에는 온프레미스 네트워크와 통신하는 Outpost에서 실행되는 인스턴스가 포함됩니다. 로컬 링크 트래픽에는 온프레미스 네트워크를 통해 인터넷과 통신하는 인스턴스가 포함될 수 있습니다.

## 서버 물리적 연결

각 Outposts 서버에는 중복되지 않은 물리적 업링크 포함되어 있습니다. 포트에는 다음과 같은 자체 속도 및 커넥터 요구 사항이 있습니다.

- 10GbE — 커넥터 유형 + QSFP

### QSFP+ 케이블

QSFP+ 케이블에는 Outposts 서버의 포트 3에 연결하는 커넥터가 있습니다. QSFP+ 케이블의 반대쪽 끝에는 스위치에 연결하는 4개의 SFP + 인터페이스가 있습니다. 스위치 측 인터페이스 중 2개는 1과 (와) 2이(가) 레이블로 지정되어 있습니다. Outposts 서버가 작동하려면 두 인터페이스가 모두 필요합니다. 2인터페이스는 서비스 링크 트래픽에 사용하고 인터페이스는 로컬 네트워크 1 인터페이스 링크 트래픽에 사용합니다. 나머지 인터페이스는 사용되지 않습니다.

## 서버의 서비스 링크 트래픽

스위치의 서비스 링크 포트를 게이트웨이가 있는 a에 대한 태그가 지정되지 않은 액세스 포트 및 다음 지역 엔드포인트로 연결되는 VLAN 경로로 구성하십시오.

- 서비스 링크 엔드포인트
- Outpost 등록 엔드포인트

Outpost가 해당 지역의 등록 엔드포인트를 검색하려면 서비스 링크 연결을 공용으로 DNS 사용할 수 있어야 합니다. AWS 연결에는 Outposts 서버와 등록 엔드포인트 사이에 NAT 장치가 있을 수 있습니다. 퍼블릭 주소 범위에 대한 AWS자세한 내용은 Amazon VPC 사용 설명서의 [AWS IP 주소 범위와 AWS Outposts 엔드포인트 및 할당량을](#) 참조하십시오. AWS 일반 참조

서버를 등록하려면 다음 네트워크 포트를 엽니다.

- TCP443
- UDP443
- UDP53

### 업링크 속도

각 Outposts 서버는 해당 지역에 대한 최소 20Mbps의 업링크 속도를 요구합니다. AWS

로컬 네트워크 인터페이스 링크 및 서비스 링크 사용률에 따라 더 빠른 업링크가 필요할 수 있습니다. 자세한 내용은 [서비스 링크에 대한 대역폭 권장 사항](#)을 참조하세요.

## 로컬 네트워크 인터페이스 링크 트래픽

업스트림 네트워크 디바이스의 로컬 네트워크 인터페이스 링크 포트를 로컬 네트워크의 VLAN a에 대한 표준 액세스 포트 구성합니다. 둘 VLAN 이상의 포트가 있는 경우 업스트림 네트워크 장치의 모든 포트를 트렁크 포트 구성하십시오. 여러 MAC 주소를 예상하도록 업스트림 네트워크 디바이스의 포트를 구성하십시오. 서버에서 실행되는 각 인스턴스는 MAC 주소를 사용합니다. 일부 네트워크 디바이스는 여러 MAC 주소를 보고하는 포트를 종료하는 포트 보안 기능을 제공합니다.

### Note

AWS Outposts 서버는 트래픽에 태그를 VLAN 지정하지 않습니다. 로컬 네트워크 인터페이스를 트렁크로 구성하는 경우 OS가 VLAN 트래픽에 태그를 지정했는지 확인해야 합니다.

다음 예제는 Amazon Linux 2023에서 로컬 네트워크 인터페이스에 대한 VLAN 태깅을 구성하는 방법을 보여줍니다. 다른 Linux 배포판을 사용하는 경우 Linux 배포판의 VLAN 태깅 구성 설명서를 참조하십시오.

예: 아마존 리눅스 2023과 아마존 리눅스 2에서 로컬 네트워크 인터페이스에 대한 VLAN 태깅을 구성하려면

1. 8021q 모듈이 커널에 로드되었는지 확인합니다. 그렇지 않은 경우 modprobe 명령을 사용하여 로드합니다.

```
modinfo 8021q
modprobe --first-time 8021q
```

2. VLAN 디바이스를 생성하십시오. 이 예제에서는 다음이 적용됩니다.

- 로컬 네트워크 인터페이스의 인터페이스 이름은 다음과 같습니다. ens6
- VLANID는 59
- VLAN 디바이스에 할당된 이름은 다음과 같습니다. ens6.59

```
ip link add link ens6 name ens6.59 type vlan id 59
```

3. 선택 사항입니다. IP를 수동으로 할당하려면 이 단계를 완료합니다. 이 예에서는 IP 192.168.59.205를 할당하고 있습니다. 여기서 서브넷은 192.168.59.0/24입니다. CIDR

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. 링크를 활성화합니다.

```
ip link set dev ens6.59 up
```

OS 수준에서 네트워크 인터페이스를 구성하고 태그 지정 변경을 영구적으로 적용하려면 다음 리소스를 참조하십시오. VLAN

- Amazon Linux 2를 사용하는 경우 Amazon 사용 설명서의 [Amazon Linux용 ec2-net-utils를 사용하여 네트워크 인터페이스 구성](#)을 참조하십시오. EC2
- Amazon Linux 2023을 사용하는 경우, Amazon Linux 2023 사용 설명서의 [네트워킹 서비스](#)를 참조하세요.

## 서버 IP 주소 할당

Outposts 서버에는 퍼블릭 IP 주소를 할당할 필요가 없습니다.

동적 호스트 제어 프로토콜 (DHCP) 은 IP 네트워크에서 장치를 구성하는 프로세스를 자동화하는 데 사용되는 네트워크 관리 프로토콜입니다. Outposts 서버에서는 다음 DHCP 두 가지 방법을 사용할 수 있습니다.

- 서버의 네트워크 카드
- 인스턴스의 로컬 네트워크 인터페이스

서비스 링크의 경우 Outposts 서버는 로컬 네트워크에 연결하는 DHCP 데 . DHCPDNS네임 서버와 기본 게이트웨이를 반환해야 합니다. Outposts 서버는 서비스 링크의 고정 IP 할당을 지원하지 않습니다.

로컬 네트워크 인터페이스 링크의 경우 로컬 네트워크에 연결할 인스턴스를 구성하는 데 사용합니다 DHCP. 자세한 내용은 [the section called “운영 체제 구성”](#) 단원을 참조하십시오.

### Note

Outposts 서버에 안정적인 IP 주소를 사용해야 합니다. IP 주소 변경으로 인해 Outpost 서브넷에서 일시적인 서비스 중단이 발생할 수 있습니다.

## 서버 등록

Outposts 서버는 로컬 네트워크에 연결을 설정하면 서비스 링크 연결을 사용하여 Outpost 등록 엔드포인트에 연결하고 스스로를 등록합니다. 등록하려면 공개가 필요합니다. DNS 서버가 등록하면 해당 리전의 서비스 링크 엔드포인트에 보안 터널을 생성합니다. Outposts 서버는 TCP 포트 443을 사용하여 공용 인터넷을 통해 지역과의 통신을 용이하게 합니다. Outposts 서버는 프라이빗 연결을 지원하지 않습니다. VPC

# AWS Outposts 리소스 공유하기

Outpost 공유를 통해 Outpost 소유자는 Outpost 사이트 및 서브넷을 포함한 Outposts 및 Outpost 리소스를 동일한 조직의 다른 계정과 공유할 수 있습니다. AWS Outpost 소유자는 Outpost 리소스를 중앙에서 생성 및 관리하고 조직 내 여러 계정에서 리소스를 공유할 수 있습니다. 이를 통해 다른 소비자가 Outpost 사이트를 사용하고 공유 Outpost에서 인스턴스를 구성VPCs, 시작 및 실행할 수 있습니다.

이 모델에서는 Outpost 리소스를 소유한 AWS 계정 (소유자) 이 동일한 조직의 다른 AWS 계정 (소비자) 과 리소스를 공유합니다. 소비자는 자신의 계정으로 생성하는 Outpost에서 동일한 방식으로 공유된 Outpost의 리소스를 생성할 수 있습니다. 소유자는 생성한 Outpost의 관리 및 리소스를 관리할 책임이 있습니다. 소유자는 언제든지 공유 액세스를 변경하거나 취소할 수 있습니다. 용량 예약을 사용하는 인스턴스를 제외하고, 소유자는 소비자가 공유 Outpost에서 생성하는 리소스를 보고 수정하고 삭제할 수 있습니다. 소유자는 소비자가 공유한 용량 예약으로 시작한 인스턴스를 수정할 수 없습니다.

소비자는 용량 예약을 소비하는 리소스를 포함하여 공유된 Outpost의 리소스를 관리할 책임이 있습니다. 소비자는 다른 소비자 또는 용량 예약 소유자가 소유한 인스턴스를 보거나 수정할 수 없습니다. 또한 공유된 Outpost를 수정할 수 없습니다.

Outpost 소유자는 다음과 같이 Outpost 리소스를 공유할 수 있습니다.

- 조직 내 특정 AWS 계정 AWS Organizations.
- AWS Organizations내 조직 내부의 조직 단위
- AWS Organizations의 전체 조직.

## 내용

- [공유 가능한 Outpost 리소스](#)
- [Outpost의 리소스 공유를 위한 사전 조건](#)
- [관련 서비스](#)
- [가용 영역 공유](#)
- [Outpost 리소스 공유](#)
- [공유된 Outpost 리소스 공유 해제](#)
- [공유 Outpost 리소스 식별](#)
- [공유 Outpost 리소스 권한](#)

- [결제 및 측정](#)
- [제한 사항](#)

## 공유 가능한 Outpost 리소스

Outpost 소유주는 이 섹션에 나열된 Outpost 자원을 소비자와 공유할 수 있습니다.

Outposts 서버에 사용할 수 있는 리소스는 다음과 같습니다. Outposts 랙 리소스의 경우 Outposts 랙 AWS Outposts 사용 설명서의 [공유 AWS Outposts 리소스](#) 사용을 참조하십시오.

- 할당된 전용 호스트 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 전용 호스트에서 EC2 인스턴스를 시작하고 실행합니다.
- Outpost – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - Outpost에서 서브넷을 생성하고 관리합니다.
  - 를 사용하여 Outpost에 대한 정보를 볼 수 있습니다. AWS Outposts API
- 사이트 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 사이트에서 Outpost를 생성하고, 관리하고, 제어합니다.
- 서브넷 – 이 리소스에 액세스할 수 있는 소비자는 다음을 수행할 수 있습니다.
  - 서브넷에 대한 정보 보기
  - 서브넷에서 EC2 인스턴스를 시작하고 실행합니다.

Amazon VPC 콘솔을 사용하여 Outpost 서브넷을 공유할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 [서브넷 공유](#)를 참조하십시오.

## Outpost의 리소스 공유를 위한 사전 조건

- 의 조직 또는 조직 구성 단위와 Outpost 리소스를 공유하려면 공유를 활성화해야 합니다. AWS Organizations AWS Organizations 자세한 내용은 AWS RAM 사용 설명서의 [AWS Organizations과 \(와\) 공유 활성화](#)를 참조하세요.
- Outpost 리소스를 공유하려면 AWS 계정에서 해당 리소스를 소유해야 합니다. 공유된 Outpost 리소스는 공유할 수 없습니다.
- Outpost 리소스를 공유하려면 조직 내 계정과 공유해야 합니다.

## 관련 서비스

Outpost 리소스 공유는 () 와 AWS Resource Access Manager 통합됩니다. AWS RAM AWS RAM 모든 AWS 계정과 또는 계정을 통해 AWS 리소스를 공유할 수 있는 서비스입니다. AWS Organizations AWS RAM을 사용하여 리소스 공유로 생성한 사용자 소유 리소스를 공유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. 소비자는 개별 AWS 계정, 조직 단위 또는 전체 조직일 수 있습니다.

에 대한 AWS RAM 자세한 내용은 [AWS RAM 사용 설명서](#)를 참조하십시오.

## 가용 영역 공유

리전의 가용 영역에 걸쳐 리소스가 배포될 수 있도록 각 계정의 이름에 가용 영역을 독립적으로 매핑합니다. 이로 인해 계정 전체에서 가용 영역 이름의 차이가 발생할 수 있습니다. 예를 들어 계정의 us-east-1a 가용 영역의 위치가 다른 AWS 계정의 us-east-1a 가용 영역과 동일하지 않을 수 있습니다.

계정과 관련된 Outpost 리소스의 위치를 확인하려면 가용 영역 ID(AZ ID)를 사용해야 합니다. AZ ID는 모든 AWS 계정의 가용 영역을 나타내는 고유하고 일관된 식별자입니다. 예를 들어 use1-az1 는 us-east-1 해당 지역의 AZ ID이며 모든 AWS 계정에서 동일한 위치에 있습니다.

계정의 IDs 가용 영역에 대한 AZ를 보려면

1. <https://console.aws.amazon.com/ram>에서 **AWS RAM** 콘솔을 엽니다.
2. 현재 지역의 IDs AZ는 화면 오른쪽에 있는 내 AZ ID 패널에 표시됩니다.

### Note

로컬 게이트웨이 라우팅 테이블은 Outpost와 동일한 AZ에 있으므로 라우팅 테이블에 AZ ID를 지정할 필요가 없습니다.

## Outpost 리소스 공유

소유주가 소비자와 Outpost를 공유하는 경우, 소비자는 자신의 계정으로 Outpost에 리소스를 생성하는 것과 동일한 방식으로 Outpost에서 리소스를 생성할 수 있습니다. 공유 로컬 게이트웨이 라우팅 테이블에 액세스할 수 있는 소비자는 VPC 연결을 생성하고 관리할 수 있습니다. 자세한 내용은 [공유 가능한 Outpost 리소스](#) 단원을 참조하십시오.

Outpost 리소스를 공유하려면 리소스 공유에 추가해야 합니다. 리소스 공유는 AWS 계정 간에 AWS RAM 리소스를 공유할 수 있는 리소스입니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. AWS Outposts 콘솔을 사용하여 Outpost 리소스를 공유하면 기존 리소스 공유에 추가합니다. 새 리소스 공유에 Outpost 리소스를 추가하려면, 우선 [AWS RAM 콘솔](#)을 사용해 리소스 공유를 생성해야 합니다.

조직의 일원이고 조직 내 공유가 활성화된 경우 AWS RAM 콘솔에서 공유 Outpost 리소스에 대한 액세스 권한을 조직의 소비자에게 부여할 수 있습니다. AWS Organizations 그렇지 않으면 소비자는 리소스 공유에 가입하라는 초대장을 받고 초대를 수락한 후 공유된 리소스의 액세스 권한을 받습니다.

AWS Outposts 콘솔, AWS RAM 콘솔 또는 `aws` 를 사용하여 소유한 Outpost 리소스를 공유할 수 있습니다. AWS CLI

콘솔을 사용하여 소유한 Outpost를 공유하려면 AWS Outposts

1. 에서 AWS Outposts 콘솔을 여세요. <https://console.aws.amazon.com/outposts/>
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 리소스 공유를 선택합니다.
5. 리소스 공유 생성을 선택합니다.

다음 절차를 사용하면 AWS RAM 콘솔로 리디렉션되어 Outpost 공유를 완료할 수 있습니다. 소유한 로컬 게이트웨이 라우팅 테이블을 공유하려면 다음 절차도 사용합니다.

콘솔을 사용하여 소유한 Outpost 또는 로컬 게이트웨이 라우팅 테이블을 공유하려면 AWS RAM

AWS RAM 사용 설명서의 [리소스 공유 생성](#)을 참조하세요.

`aws` 를 사용하여 소유한 Outpost 또는 로컬 게이트웨이 라우팅 테이블을 공유하려면 AWS CLI

[create-resource-share](#) 명령을 사용하세요.

## 공유된 Outpost 리소스 공유 해제

공유 전초 기지가 공유되지 않으면 소비자는 콘솔에서 더 이상 전초 기지를 볼 수 없습니다. AWS Outposts Outpost에서 새 서브넷을 만들거나 Outpost에 새 EBS 볼륨을 만들거나 콘솔 또는 `aws` 를 사용하여 Outpost 세부 정보 및 인스턴스 유형을 볼 수 없습니다. AWS Outposts AWS CLI 소비자가 만든 기

존 서브넷, 볼륨 또는 인스턴스는 삭제되지 않습니다. 소비자가 Outpost에서 생성한 기존 서브넷은 여전히 새 인스턴스를 시작하는 데 사용할 수 있습니다.

공유된 로컬 게이트웨이 라우팅 테이블이 공유되지 않으면 소비자는 더 이상 새 연결을 생성할 수 없습니다. VPC 소비자가 생성한 기존 VPC 연결은 모두 라우팅 테이블과 연결된 상태로 유지됩니다. 이러한 리소스는 트래픽을 로컬 게이트웨이로 계속 라우팅할 VPCs 수 있습니다.

소유하고 있는 공유 Outpost 리소스의 공유를 해제하려면 리소스 공유에서 제거해야 합니다. AWS RAM 콘솔이나 `aws` 를 사용하여 이 작업을 수행할 수 있습니다.

콘솔을 사용하여 소유하고 있는 공유 Outpost 리소스의 공유를 취소하려면 AWS RAM

AWS RAM 사용 설명서에서 [리소스 공유 업데이트](#)를 참조하세요.

`aws` 를 사용하여 소유하고 있는 공유 Outpost 리소스의 공유를 취소하려면 AWS CLI

명령어를 사용하세요. [disassociate-resource-share](#)

## 공유 Outpost 리소스 식별

소유자와 소비자는 AWS Outposts 콘솔 및 `aws` 를 사용하여 공유 Outposts를 식별할 수 있습니다. AWS CLI `aws` 을(를) 사용하여 공유 로컬 게이트웨이 라우팅 테이블을 식별할 수 있습니다.

콘솔을 사용하여 공유 전초 기지를 식별하려면 AWS Outposts

1. 에서 AWS Outposts <https://console.aws.amazon.com/outposts/> 콘솔을 여십시오.
2. 탐색 창에서 Outposts를 선택합니다.
3. Outpost를 선택한 다음 작업, 세부 정보 보기를 선택합니다.
4. Outpost 요약 페이지에서 소유자 ID를 확인하여 Outpost 소유자의 AWS 계정 ID를 식별할 수 있습니다.

다음은 사용하여 공유 아웃포스트 리소스를 식별하려면 AWS CLI

[리스트-아웃포스트와 -tables 명령을 사용하세요. describe-local-gateway-route](#) 이 명령은 사용자가 소유한 Outpost 리소스 및 사용자와 공유하는 Outpost 리소스를 반환합니다. `OwnerId`은(는) Outpost 소유자의 AWS 계정 ID를 보여줍니다.

## 공유 Outpost 리소스 권한

### 소유자에 대한 권한

소유자는 Outpost의 관리 및 자원을 관리할 책임이 있습니다. 소유자는 언제든지 공유 액세스를 변경하거나 취소할 수 있습니다. AWS Organizations 이를 사용하여 소비자가 공유 Outposts에서 생성한 리소스를 보고, 수정하고, 삭제할 수 있습니다.

### 소비자에 대한 권한

소비자는 자신의 계정으로 생성하는 Outpost에서 동일한 방식으로 공유된 Outpost의 리소스를 생성할 수 있습니다. 소비자는 공유된 Outpost에서 시작된 리소스를 관리할 책임이 있습니다. 소비자는 다른 소비자나 Outpost 소유자가 소유한 인스턴스를 보거나 수정할 수 없으며 공유된 Outpost를 수정할 수 없습니다.

## 결제 및 측정

공유하는 Outpost의 리소스에 대한 비용이 소유자에게 청구됩니다. 또한 해당 지역에서 들어오는 Outpost의 서비스 링크 VPN 트래픽과 관련된 모든 데이터 전송 요금도 청구됩니다. AWS

로컬 게이트웨이 라우팅 테이블 공유에 대한 추가 비용은 없습니다. 공유 서브넷의 경우 연결, NAT 게이트웨이, 사설 링크 AWS Direct Connect VPN 연결과 같은 VPC 수준 리소스에 대한 요금이 VPC 소유자에게 청구됩니다.

소비자는 로드 밸런서 및 RDS Amazon 데이터베이스와 같은 공유 Outposts에서 생성한 애플리케이션 리소스에 대해 요금이 청구됩니다. 또한 소비자는 해당 지역에서 데이터를 전송할 때 요금이 청구됩니다. AWS

## 제한 사항

AWS Outposts 공유 작업에는 다음과 같은 제한이 적용됩니다.

- 공유 서브넷 제한은 AWS Outposts 공유 작업에 적용됩니다. VPC공유 한도에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [제한](#)을 참조하십시오.
- 서비스 할당량은 개별 계정별로 적용됩니다.

## 보안 내부 AWS Outposts

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

보안은 기업과 기업 간의 AWS 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

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

의 보안 및 규정 준수에 대한 AWS Outposts 자세한 내용은 [서버를](#) 참조하십시오 FAQ.

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

### 내용

- [데이터 보호: AWS Outposts](#)
- [ID 및 액세스 관리 \(\) 에 대한 IAM AWS Outposts](#)
- [의 인프라 보안 AWS Outposts](#)
- [탄력성: AWS Outposts](#)
- [규정 준수 검증: AWS Outposts](#)

## 데이터 보호: AWS Outposts

AWS [공동 책임 모델](#) 의 데이터 보호에 적용됩니다 AWS Outposts. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 AWS 서비스 사용하는 보안 구성 및 관리 작업 이 포함됩니다.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 개별 사용자를 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM) 로 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다.

데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시를 참조하십시오](#) FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 [AWS 공동 책임 모델 및 AWS 보안 GDPR 블로그의 블로그 게시물](#)을 참조하십시오.

## 저장 중 암호화

AWS Outposts를 사용하면 저장된 모든 데이터가 암호화됩니다. 키 자료는 이동식 장치에 저장된 외부 키인 Nitro 보안 키 (NSK) 에 래핑됩니다.

## 전송 중 암호화

AWS Outpost와 해당 지역 간의 전송 데이터를 암호화합니다. AWS 자세한 내용은 [서비스 링크를 통한 연결](#) 단원을 참조하십시오.

## 데이터 삭제

인스턴스를 종료하면 새 EC2 인스턴스에 할당되기 전에 하이퍼바이저가 해당 인스턴스에 할당된 메모리를 스크러빙 (0으로 설정) 하고 모든 스토리지 블록이 재설정됩니다.

Nitro 보안 키를 파괴하면 Outpost의 데이터가 암호적으로 파괴됩니다. 자세한 내용은 [암호화 방식으로 파쇄된 서버 데이터](#) 섹션을 참조하세요.

## ID 및 액세스 관리 () 에 대한 IAM AWS Outposts

AWS Identity and Access Management (IAM) 는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 도와주는 AWS 서비스입니다. IAM관리자는 AWS Outposts 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. 추가 비용 없이 IAM 사용할 수 있습니다.

### 내용

- [AWS Outposts와 함께 작동하는 방식 IAM](#)
- [AWS Outposts 정책 예제](#)
- [서비스 연결 역할: AWS Outposts](#)

- [AWS Outposts에 대한 관리형 정책](#)

## AWS Outposts와 함께 작동하는 방식 IAM

IAM Outposts를 사용하여 액세스를 관리하기 전에 AWS Outposts에서 사용할 수 있는 IAM 기능에 대해 알아보십시오. AWS

IAM AWS Outposts와 함께 사용할 수 있는 기능

IAM기능	AWS Outposts 지원
<a href="#">ID 기반 정책</a>	예
<a href="#">리소스 기반 정책</a>	아니요
<a href="#">정책 작업</a>	예
<a href="#">정책 리소스</a>	예
<a href="#">정책 조건 키(서비스별)</a>	예
<a href="#">ACLs</a>	아니요
<a href="#">ABAC(정책의 태그)</a>	예
<a href="#">임시 보안 인증</a>	예
<a href="#">보안 주체 권한</a>	예
<a href="#">서비스 역할</a>	아니요
<a href="#">서비스 링크 역할</a>	예

## Outposts에 대한 ID 기반 정책 AWS

ID 기반 정책 지원: 예

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

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

Outposts를 위한 ID 기반 정책 예제 AWS

AWS Outposts ID 기반 정책의 예를 보려면 [을 참조하십시오. AWS Outposts 정책 예제](#)

Outposts 내의 리소스 기반 정책 AWS

리소스 기반 정책 지원: 아니요

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

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

AWS Outposts를 위한 정책 조치

정책 작업 지원: 예

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

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

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

AWS Outposts 작업 목록을 보려면 서비스 권한 부여 AWS Outposts [참조에 정의된 작업을](#) 참조하십시오.

AWS Outposts의 정책 조치는 조치 앞에 다음 접두사를 사용합니다.

```
outposts
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
  "outposts:action1",
  "outposts:action2"
]
```

와일드카드(\*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, List라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "outposts:List*"
```

## AWS Outposts를 위한 정책 리소스

정책 리소스 지원: 예

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

ResourceJSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. [Amazon 리소스 이름 \(ARN\)](#) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

```
"Resource": "*"

```

일부 AWS Outposts API 액션은 여러 리소스를 지원합니다. 명령문 하나에 여러 리소스를 지정하려면 ARNs 쉼표로 구분하십시오.

```
"Resource": [

```

```
"resource1",
"resource2"
]
```

AWS Outposts 리소스 유형 및 해당 ARNs 유형의 목록을 보려면 서비스 권한 부여 AWS Outposts [참조에 정의된 리소스 유형](#)을 참조하십시오. 각 리소스의 어떤 작업을 지정할 수 있는지 알아보려면 [정의된 AWS Outposts 작업](#)을 참조하십시오. ARN

## AWS Outposts의 정책 조건 키

서비스별 정책 조건 키 지원: 예

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

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

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

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

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS [글로벌 조건 컨텍스트 키](#)를 참조하십시오.

AWS Outposts 조건 키 목록을 보려면 서비스 권한 부여 참조의 [조건 키를 참조하십시오 AWS Outposts](#). 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 [작업 정의 기준](#)을 참조하십시오. AWS Outposts

AWS Outposts ID 기반 정책의 예를 보려면 을 참조하십시오. [AWS Outposts 정책 예제](#)

## ACLs AWS Outposts에서

지원ACLs: 아니요

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

## ABAC AWS Outposts와 함께

지원 ABAC (정책의 태그): 예

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

ABAC 빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에도 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

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

에 대한 자세한 내용은 [What is ABAC?](#) 를 참조하십시오. ABAC IAM 사용 설명서에서, 설정 ABAC 단계가 포함된 자습서를 보려면 [사용 IAM 설명서의 속성 기반 액세스 제어 사용 \(ABAC\)](#) 을 참조하십시오.

## AWS Outposts에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 AWS 서비스 방법을 비롯한 추가 정보는 IAM 사용 설명서의 [AWS 서비스 해당](#) 자격 증명을 참조하십시오. IAM

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

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 AWS API 있습니다. 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS 있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자

격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 [임시 보안 자격 증명을 참조하십시오.](#)  
[IAM](#)

## Outposts에 대한 AWS 서비스 간 사용자 권한

순방향 액세스 세션 지원 (FAS): 예

에서 IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS 경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 를 호출하는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 [전달 액세스 세션을 참조하십시오.](#)

## AWS Outpost의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 [IAM 역할입니다.](#) IAM 관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 [역할 만들기를 참조하여 권한을 위임하십시오](#) IAM. AWS 서비스

## Outposts의 서비스 연계 역할 AWS

서비스 링크 역할 지원: 예

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

AWS Outposts 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오.  
[서비스 연결 역할: AWS Outposts](#)

## AWS Outposts 정책 예제

기본적으로 사용자 및 역할에는 AWS Outposts 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API 를 사용하여 작업을 수행할 수도 없습니다. IAM 관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수

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

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 [사용 IAM 설명서](#)에서 IAM [정책 생성](#)을 참조하십시오.

각 리소스 유형의 형식을 포함하여 AWS Outposts에서 정의한 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 권한 부여 참조의 [작업, 리소스 및 조건 키](#)를 참조하십시오.

## 내용

- [정책 모범 사례](#)
- [예제: 리소스 수준 권한 사용](#)

## 정책 모범 사례

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

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

되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 [IAMAccess Analyzer 정책 검증을](#) 참조하십시오. IAM

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

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 [보안 모범 사례를](#) 참조하십시오. IAM

### 예제: 리소스 수준 권한 사용

다음 예에서는 리소스 수준 권한을 사용하여 지정된 Outpost에 대한 정보를 가져올 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

다음 예제에서는 리소스 수준 권한을 사용하여 지정된 사이트에 대한 정보를 가져올 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

## 서비스 연결 역할: AWS Outposts

AWS Outposts 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결된 서비스 역할 유형입니다. AWS Outposts 서비스 연결 역할을 정의하며 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS Outposts 보다 효율적으로 설정할 수 있습니다. AWS Outposts 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 역할만 맡을 AWS Outposts 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 링크 역할을 삭제할 수 있습니다. 이렇게 하면 AWS Outposts 리소스 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

### 에 대한 서비스 연결 역할 권한 AWS Outposts

AWS Outposts \_라는 서비스 연결 역할을 사용합니다. `AWSServiceRoleForOutposts OutpostID`—Outposts가 사용자 대신 개인 연결을 위한 AWS 리소스에 액세스할 수 있도록 허용합니다. 이 서비스 링크 역할은 프라이빗 연결 구성을 허용하고, 네트워크 인터페이스를 생성하고, 이를 서비스 링크 엔드포인트 인스턴스에 연결합니다.

\_ `AWSServiceRoleForOutpostsOutpostID` 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수입합니다.

- `outposts.amazonaws.com`

\_ `AWSServiceRoleForOutpostsOutpostID` 서비스 연결 역할에는 다음 정책이 포함됩니다.

- `AWSOutpostsServiceRolePolicy`
- `AWSOutpostsPrivateConnectivityPolicy_OutpostID`

`AWSOutpostsServiceRolePolicy` 정책은 에서 관리하는 리소스에 액세스할 수 있도록 하는 서비스 연결 역할 정책입니다. AWS Outposts

이 정책을 통해 지정된 리소스에서 다음 작업을 AWS Outposts 완료할 수 있습니다.

- 작업: all AWS resources에 대한 `ec2:DescribeNetworkInterfaces`
- 작업: all AWS resources에 대한 `ec2:DescribeSecurityGroups`

- 작업: all AWS resources에 대한 ec2:CreateSecurityGroup
- 작업: all AWS resources에 대한 ec2:CreateNetworkInterface

AWSOutpostsPrivateConnectivityPolicy\_ **OutpostID** 정책을 통해 지정된 리소스에서 다음 작업을 AWS Outposts 완료할 수 있습니다.

- 작업: all AWS resources that match the following Condition:에 대한 ec2:AuthorizeSecurityGroupIngress

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" : "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: all AWS resources that match the following Condition:에 대한 ec2:AuthorizeSecurityGroupEgress

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" : "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: all AWS resources that match the following Condition:에 대한 ec2:CreateNetworkInterfacePermission

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" : "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 작업: all AWS resources that match the following Condition:에 대한 ec2:CreateTags

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" : "[*]OutpostId"} }
```

IAM 엔티티 (예: 사용자, 그룹 또는 역할) 가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하십시오. IAM

에 대한 서비스 연결 역할을 생성하십시오. AWS Outposts

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 Outpost의 비공개 연결을 구성하면 서비스 연결 AWS Outposts 역할이 자동으로 생성됩니다. AWS Management Console

## 에 대한 서비스 연결 역할을 편집하십시오. AWS Outposts

AWS Outposts \_를 편집할 수 없습니다. AWSServiceRoleForOutposts *OutpostID* 서비스 연결 역할. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 를 사용하여 역할에 대한 설명을 편집할 수 있습니다. IAM 자세한 내용은 IAM사용 설명서의 [서비스 연결 역할 업데이트](#)를 참조하십시오.

## 에 대한 서비스 연결 역할 삭제 AWS Outposts

서비스 링크 역할이 필요한 기능이나 서비스가 더 이상 필요하지 않으면 그 역할을 삭제하는 것이 좋습니다. 이렇게 하면 적극적으로 모니터링되거나 유지 관리되지 않는 미사용 개체를 피할 수 있습니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

AWS Outposts 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

\_를 삭제하려면 먼저 Outpost를 삭제해야 합니다. AWSServiceRoleForOutposts *OutpostID* 서비스 연계 역할.

시작하기 전에 Outpost가 () 를 사용하여 AWS Resource Access Manager 공유되고 있는지 확인하세요. AWS RAM 자세한 내용은 [공유된 Outpost 리소스 공유 해제](#) 단원을 참조하십시오.

\_에서 사용하는 AWS Outposts 리소스를 삭제하려면 AWSServiceRoleForOutposts *OutpostID*

Outpost를 삭제하려면 AWS 기업 지원팀에 문의하세요.

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

자세한 내용은 사용 설명서의 [서비스 연결 역할 삭제](#)를 참조하십시오. IAM

## 서비스 연결 역할이 지원되는 AWS Outposts 지역

AWS Outposts 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할을 사용할 수 있습니다. [자세한 내용은 Outposts 랙 FAQs 및 Outposts 서버용을 참조하십시오.](#)

## AWSAWS Outposts에 대한 관리형 정책

AWS 관리형 정책은 에서 만들고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS 관리형 정책에 정의된 권한을 업데이트 하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 정책이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM사용 설명서의 [AWS 관리형 정책](#)을 참조하십시오.

### AWS 관리형 정책: AWSOutpostsServiceRolePolicy

이 정책은 AWS Outposts가 사용자를 대신하여 작업을 수행하도록 허용하는 서비스 연결 역할에 연결됩니다. 자세한 내용은 [서비스 연결 역할](#) 단원을 참조하십시오.

### AWS 관리형 정책: AWSOutpostsPrivateConnectivityPolicy

이 정책은 AWS Outposts가 사용자를 대신하여 작업을 수행하도록 허용하는 서비스 연결 역할에 연결됩니다. 자세한 내용은 [서비스 연결 역할](#) 단원을 참조하십시오.

### AWS 관리형 정책: AWSOutpostsAuthorizeServerPolicy

이 정책을 사용하면 온프레미스 네트워크에서 Outposts 서버 하드웨어를 승인하는 데 필요한 권한을 부여할 수 있습니다.

이 정책에는 다음 권한이 포함되어 있습니다.

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

## AWS 관리형 정책에 대한 업데이트를 AWS Outposts

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS Outposts의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오.

변경 사항	설명	날짜
<a href="#">AWSOutpostsAuthorizeServerPolicy</a> - 새 정책	AWS Outposts는 온프레미스 네트워크에서 Outposts 서버 하드웨어에 권한을 부여하는 정책을 추가했습니다.	2023년 1월 4일
AWS Outposts는 변경 사항을 추적하기 시작했습니다	AWS Outposts는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2019년 12월 3일

## 의 인프라 보안 AWS Outposts

관리형 서비스인 AWS Outposts는 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 [AWS 클라우드 보안을](#) 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 [인프라 보호](#)를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS Outposts에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

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

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

Outpost에서 실행되는 EC2 인스턴스 및 EBS 볼륨에 제공되는 인프라 보안에 대한 자세한 내용은 [EC2Amazon의 인프라 보안을](#) 참조하십시오.

VPC플로우 로그는 AWS 지역에서와 동일한 방식으로 작동합니다. 즉, 분석을 GuardDuty 위해 CloudWatch 로그, Amazon S3 또는 Amazon에 게시할 수 있습니다. Outpost가 연결이 끊긴 상태일 때는 데이터를 다른 서비스에서 CloudWatch 볼 수 없도록 이러한 서비스에 게시하려면 해당 지역으로 데이터를 다시 보내야 합니다.

## 탄력성: AWS Outposts

고가용성을 위해, 추가 Outpost 서버를 주문할 수 있습니다. Outpost 용량 구성은 프로덕션 환경에서 작동하도록 설계되었으며, 용량을 프로비저닝하면 각 인스턴스 패밀리에 대해 N+1 인스턴스를 지원 합니다. AWS 은(는) 기본 호스트 문제가 있는 경우 복구 및 장애 조치를 수행할 수 있도록 미션 크리티컬 애플리케이션에 충분한 추가 용량을 할당할 것을 권장합니다. Amazon CloudWatch 용량 가용성 지표를 사용하고 경보를 설정하여 애플리케이션 상태를 모니터링하고, 자동 복구 옵션을 구성하는 CloudWatch 작업을 생성하고, 시간 경과에 따른 Outposts의 용량 사용률을 모니터링할 수 있습니다.

Outpost를 생성할 때는 지역에서 가용 영역을 선택합니다. AWS 이 가용 영역은 API 통화 응답, Outpost 모니터링, Outpost 업데이트와 같은 컨트롤 플레인 작업을 지원합니다. 가용 영역이 제공하는 복원력을 활용하려면 각각 다른 가용 영역에 연결된 여러 Outpost에 애플리케이션을 배포할 수 있습니다. 이를 통해 추가 애플리케이션 복원력을 구축하고 단일 가용 영역에 대한 의존성을 피할 수 있습니다. 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

Outposts 서버는 인스턴스 스토어 볼륨을 포함하지만 Amazon EBS 볼륨은 지원하지 않습니다. 인스턴스 스토어 볼륨의 데이터는 인스턴스 재부팅 후에도 유지되지만 인스턴스 종료 후에는 지속되지 않습니다. 인스턴스 수명 기간이 지난 후에도 인스턴스 스토어 볼륨에 장기 데이터를 유지하려면 Amazon S3 버킷이나 온 프레미스 네트워크의 네트워크 스토리지 장치와 같은 영구 스토리지에 데이터를 백업해야 합니다.

## 규정 준수 검증: AWS Outposts

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면 AWS 서비스 규정 준수 [프로그램의 AWS 서비스 범위별, 규정](#) 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 [AWS 규정 준수 프로그램 AWS 보증 프로그램 규정 AWS](#) 참조하십시오.

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

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

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

**Note**

모든 AWS 서비스 사람이 자격이 있는 것은 아닙니다. HIPAA 자세한 내용은 [HIPAA적격서 비스 참조를](#) 참조하십시오.

- [AWS 규정AWS 준수 리소스](#) — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- [AWS 고객 규정 준수 가이드](#) — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 ()) 를 포함한PCI) 전반의 보안 제어에 대한 지침을 매핑합니다. ISO
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#)— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하십시오.
- [Amazon GuardDuty](#) — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하는 PCI DSS 등 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- [AWS Audit Manager](#)— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위협을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

AWS Outposts 모니터링 및 로깅 기능을 제공하는 다음 서비스와 통합됩니다.

### CloudWatch 지표

CloudWatch Amazon을 사용하면 Outposts 서버의 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 집합으로 가져올 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 [CloudWatch](#) 단원을 참조하십시오.

### CloudTrail 로그

AWS CloudTrail 걸려온 통화에 대한 세부 정보를 캡처하는 데 사용합니다 AWS APIs. Amazon S3에 이러한 호출을 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하여 어떤 전화를 걸었는지, 전화를 건 소스 IP 주소, 전화를 건 사람, 언제 전화를 걸었는지 등의 정보를 확인할 수 있습니다.

CloudTrail 로그에는 클릭 유도 문안에 대한 정보가 API 들어 AWS Outposts 있습니다. 또한 Amazon EC2 EBS 및 Amazon과 같은 Outpost에 API 있는 서비스로부터 오는 클릭 유도 문안에 대한 정보도 포함되어 있습니다. 자세한 내용은 [다음을 사용하여 API 통화를 기록합니다. CloudTrail](#) 단원을 참조하십시오.

### VPC 흐름 로그

VPC 흐름 로그를 사용하여 전초 기지와 전초 기지 내에서 들어오고 나가는 트래픽에 대한 자세한 정보를 캡처할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC [흐름 로그](#)를 참조하십시오.

### 트래픽 미러링

트래픽 미러링을 사용하여 랙 서버의 네트워크 트래픽을 복사하여 보안 및 모니터링 out-of-band 어플라이언스로 전달할 수 있습니다. 미러링된 트래픽을 콘텐츠 검사, 위협 모니터링 또는 문제 해결에 사용할 수 있습니다. 자세한 내용은 [Amazon VPC 트래픽 미러링 가이드](#)를 참조하십시오.

### AWS Health Dashboard

리소스 상태의 변화에 따라 시작되는 정보와 알림을 AWS Health Dashboard 표시합니다. AWS 이 정보는 최근 이벤트와 예정된 이벤트를 카테고리별로 보여주는 대시보드와 지난 90일간의 모든 이벤트를 보여주는 전체 이벤트 로그의 두 가지 방법으로 표시됩니다. 예를 들어 서비스 링크의 연결 문제가 발생하면 대시보드와 이벤트 로그에 나타나는 이벤트가 시작되고 이벤트 로그에 90일 동안 남아 있게 됩니다. 이 AWS Health 서비스의 일부는 설정이 AWS Health Dashboard 필요 없으며 계정에서 인증된 모든 사용자가 볼 수 있습니다. 자세한 내용은 [AWS Health Dashboard 시작하기](#)를 참조하세요.

# CloudWatch

AWS Outposts Outposts를 CloudWatch 위해 Amazon에 데이터 포인트를 게시합니다. CloudWatch 이러한 데이터 포인트에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 예를 들어, 지정된 기간 동안 Outpost에 사용 가능한 인스턴스 용량을 모니터링할 수 있습니다. 각 데이터 포인트에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어, ConnectedStatus 지표를 모니터링하는 CloudWatch 경보를 만들 수 있습니다. 평균 지표가 다음보다 1 작으면 이메일 주소로 알림을 보내는 등의 작업을 시작할 CloudWatch 수 있습니다. 그런 다음 Outpost 운영에 영향을 미칠 수 있는 잠재적인 온프레미스 또는 업링크 네트워킹 문제를 조사할 수 있습니다. 일반적인 문제로는 방화벽과 NAT 규칙에 대한 최근의 온-프레미스 네트워크 구성 변경 또는 인터넷 연결 문제 등이 있습니다. ConnectedStatus문제의 경우 온-프레미스 네트워크 내에서 AWS 지역 연결을 확인하고 문제가 지속되면 AWS Support에 문의하는 것이 좋습니다.

CloudWatch 경보 생성에 대한 자세한 내용은 Amazon 사용 설명서의 [Amazon CloudWatch Alarms 사용](#)을 참조하십시오. CloudWatch에 대한 CloudWatch 자세한 내용은 [Amazon CloudWatch 사용 설명서](#)를 참조하십시오.

## 내용

- [지표](#)
- [미터식 치수](#)
- 

## 지표

AWS/Outposts 네임스페이스에 포함된 지표는 다음과 같습니다.

### ConnectedStatus

Outpost의 서비스 링크 연결 상태. 평균 통계가 1 이하이면 연결이 손상된 것입니다.

단위: 수

최대 해상도: 1분

통계: 가장 유용한 통계는 Average입니다.

차원: OutpostId

### CapacityExceptions

인스턴스 시작에 대한 용량 부족 오류 수입니다.

단위: 수

최대 해상도: 5분

통계: 가장 유용한 통계는 Maximum 및 Minimum입니다.

치수: InstanceType 및 OutpostId

### InstanceFamilyCapacityAvailability

사용 가능한 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

치수: 및 InstanceFamily OutpostId

### InstanceFamilyCapacityUtilization

사용 중인 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

차원: Account, InstanceFamily, OutpostId

### InstanceTypeCapacityAvailability

사용 가능한 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

치수: InstanceType 및 OutpostId

#### InstanceTypeCapacityUtilization

사용 중인 인스턴스 용량의 백분율. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 백분율

최대 해상도: 5분

통계: 가장 유용한 통계는 Average 및 pNN.NN입니다(백분위수).

차원: Account, InstanceType, OutpostId

#### UsedInstanceType\_Count

Amazon Relational Database Service (RDSAmazon) 또는 Application Load Balancer와 같은 관리형 서비스에서 사용하는 모든 인스턴스 유형을 포함하여 현재 사용 중인 인스턴스 유형의 수입니다. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 수

최대 해상도: 5분

차원: Account, InstanceType, OutpostId

#### AvailableInstanceType\_Count

사용 가능한 인스턴스 유형 수. 이 지표에는 Outpost에 구성된 전용 호스트의 용량이 포함되지 않습니다.

단위: 수

최대 해상도: 5분

크기: 및 InstanceType OutpostId

#### AvailableReservedInstances

[용량 예약](#)을 사용하여 예약된 컴퓨팅 파워로 시작할 수 있는 인스턴스의 수입니다. 이 지표에는 Amazon EC2 예약 인스턴스가 포함되지 않습니다.

단위: 수

최대 해상도: 5분

크기: InstanceType 및 OutpostId

#### UsedReservedInstances

[용량 예약](#)을 사용하여 예약된 컴퓨팅 파워에서 실행 중인 인스턴스의 수입입니다. 이 지표에는 Amazon EC2 예약 인스턴스가 포함되지 않습니다.

단위: 수

최대 해상도: 5분

크기: InstanceType 및 OutpostId

#### TotalReservedInstances

실행 중이고 시작할 수 있는 총 인스턴스 수로, [용량 예약](#)을 사용하여 예약한 컴퓨팅 파워로 제공됩니다. 이 지표에는 Amazon EC2 예약 인스턴스가 포함되지 않습니다.

단위: 수

최대 해상도: 5분

크기: InstanceType 및 OutpostId

## 미터식 치수

Outpost의 지표를 필터링하려면 다음 차원을 사용합니다.

측정기준	설명
Account	용량을 사용하는 계정 또는 서비스.
InstanceFamily	인스턴스 패밀리.
InstanceType	인스턴스 유형.
OutpostId	Outpost의 ID.

측정기준	설명
VolumeType	EBS볼륨 유형.
VirtualInterfaceId	로컬 게이트웨이 또는 서비스 링크 가상 인터페이스 (VIF) 의 ID.
VirtualInterfaceGroupId	로컬 게이트웨이 가상 인터페이스 (VIF) 의 가상 인터페이스 그룹 ID.

콘솔을 사용하여 Outposts 서버의 CloudWatch 메트릭을 볼 수 있습니다. CloudWatch

콘솔을 CloudWatch 사용하여 지표를 보려면

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. 탐색 창에서 지표를 선택합니다.
3. Outpost네임스페이스를 선택합니다.
4. (선택 사항) 모든 측정기준의 지표를 보려면 검색 필드에 이름을 입력합니다.

를 사용하여 지표를 보려면 AWS CLI

사용 가능한 지표의 목록을 표시하려면 다음 [list-metrics](#) 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

를 사용하여 지표에 대한 통계를 가져오려면 AWS CLI

다음 [get-metric-statistics](#) 명령을 사용하여 지정된 지표 및 차원에 대한 통계를 가져올 수 있습니다. CloudWatch 고유한 차원 조합을 각각 별도의 지표로 취급합니다. 특별 게시가 되지 않은 차원의 조합을 사용해 통계를 검색할 수는 없습니다. 지표 생성 시 사용한 것과 동일하게 차원을 지정해야 합니다.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef \
Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

## 다음을 사용하여 AWS Outposts API 통화를 기록합니다. AWS CloudTrail

AWS Outposts 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다. CloudTrail AWS Outposts AS 이벤트의 API 호출을 캡처합니다. 캡처된 호출에는 AWS Outposts 콘솔에서의 호출 및 AWS Outposts API 작업에 대한 코드 호출이 포함됩니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Outposts, 요청한 IP 주소, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

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

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

CloudTrail 계정을 만들 때 AWS 계정에서 활성화되며 자동으로 CloudTrail 이벤트 기록에 액세스할 수 있습니다. CloudTrail 이벤트 기록은 지난 90일간의 기록된 관리 이벤트를 보고, 검색하고, 다운로드할 수 있고, 변경할 수 없는 기록을 제공합니다. AWS 리전자세한 내용은 사용 설명서의 [CloudTrail 이벤트 기록 사용](#)을 참조하십시오. AWS CloudTrail 이벤트 기록 조회에는 CloudTrail 요금이 부과되지 않습니다.

AWS 계정 지난 90일 동안 진행 중인 이벤트 기록을 보려면 트레일 또는 [CloudTrail호수](#) 이벤트 데이터 저장소를 생성하세요.

### CloudTrail 트레일

트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 를 사용하여 생성된 모든 트레일은 멀티 AWS Management Console 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정의 모든 활동을 기록할 수 있으므로 멀티 리전 트레일을 생성하는 것이 좋습니다 AWS 리전 . 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [Creating a trail for your AWS 계정](#) 및 [Creating a trail for an organization](#)을 참조하세요.

트레일을 CloudTrail 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수 있지만 Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은

[AWS CloudTrail 요금](#)을 참조하십시오. Amazon S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

## CloudTrail 레이크 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대한 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail [Lake](#)는 [행 기반 JSON 형식의 기존 이벤트를 Apache 형식으로 변환합니다.](#) [ORC](#) ORC데이터를 빠르게 검색하는 데 최적화된 컬럼형 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 [고급 이벤트 선택기](#)를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 [사용 안내서의 AWS CloudTrail Lake 사용](#)을 참조하십시오. AWS CloudTrail

CloudTrail Lake 이벤트 데이터 저장 및 쿼리로 인해 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## AWS Outposts 의 관리 이벤트 CloudTrail

[관리 이벤트](#)는 내 리소스에 대해 수행되는 관리 작업에 대한 정보를 제공합니다 AWS 계정. 이를 제어 영역 작업이라고도 합니다. 기본적으로 관리 이벤트를 CloudTrail 기록합니다.

AWS Outposts는 모든 AWS Outposts 컨트롤 플레인 작업을 관리 이벤트로 기록합니다. [Outposts가 기록하는 AWS Outposts 컨트롤 플레인 작업 목록은 AWS Outposts 레퍼런스를 CloudTrail 참조하십시오.](#) [AWS API](#)

## AWS Outposts 이벤트 예제

다음 예제는 SetSiteAddress 작업을 보여주는 CloudTrail 이벤트를 보여줍니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE:jd0e",
    "arn": "arn:aws:sts::111122223333:assumed-role/example/jd0e",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
```

```
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AKIAIOSFODNN7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:role/example",
      "accountId": "111122223333",
      "userName": "example"
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2020-08-14T16:28:16Z"
    }
  }
},
"eventTime": "2020-08-14T16:32:23Z",
"eventSource": "outposts.amazonaws.com",
"eventName": "SetSiteAddress",
"awsRegion": "us-west-2",
"sourceIPAddress": "XXX.XXX.XXX.XXX",
"userAgent": "userAgent",
"requestParameters": {
  "SiteId": "os-123ab4c56789de01f",
  "Address": "****"
},
"responseElements": {
  "Address": "****",
  "SiteId": "os-123ab4c56789de01f"
},
"requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
"eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

# Outposts

[공동 책임 모델](#) 하에서는 AWS AWS 서비스를 실행하는 하드웨어와 소프트웨어를 담당합니다. 이는 AWS 지역과 AWS Outposts 마찬가지로 예도 적용됩니다. 예를 들어, 보안 패치를 AWS 관리하고, 펌웨어를 업데이트하고, Outpost 장비를 유지 관리합니다. AWS 또한 Outposts 서버의 성능, 상태 및 메트릭을 모니터링하고 유지 관리가 필요한지 여부를 결정합니다.

## Warning

기본 디스크 드라이브에 장애가 발생하거나 인스턴스가 종료되면 인스턴스 스토어 볼륨의 데이터가 손실됩니다. 데이터 손실을 방지하려면 인스턴스 스토어 볼륨의 장기 데이터를 Amazon S3 버킷 또는 온프레미스 네트워크의 네트워크 스토리지 디바이스와 같은 영구 스토리지에 백업하는 것이 좋습니다.

## 내용

- [하드웨어 유지 관리](#)
- [펌웨어 업데이트](#)
- [전력 및 네트워크 이벤트에 대한 모범 사례](#)
- [암호화 방식으로 파쇄된 서버 데이터](#)

## 하드웨어 유지 관리

서버 프로비저닝 프로세스 중에 또는 Outposts 서버에서 EC2 실행되는 Amazon 인스턴스를 호스팅하는 동안 복구할 수 없는 하드웨어 문제가 AWS 감지되면 Outpost 소유자와 인스턴스 소유자 모두에게 영향을 받는 인스턴스가 사용 중지될 예정임을 알립니다. 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 종료](#)를 참조하십시오.

AWS 인스턴스 사용 중지 날짜에 영향을 받는 인스턴스를 종료합니다. 인스턴스 스토어 볼륨의 데이터는 인스턴스 종료 후에 유지되지 않습니다. 따라서 인스턴스 만료 날짜 전에 작업을 수행하는 것이 중요합니다. 먼저, 영향을 받는 각 인스턴스의 인스턴스 스토어 볼륨에서 Amazon S3 버킷 또는 네트워크의 네트워크 스토리지 장치와 같은 영구 스토리지로 장기 데이터를 전송합니다.

대체 서버가 Outpost 사이트로 배송됩니다. 이어서 다음을 수행합니다.

- 복구할 수 없는 서버에서 네트워크 및 전원 케이블을 분리하고 필요한 경우 랙에서 분리합니다.

- 교체 서버를 같은 위치에 설치합니다. [Outposts 서버 설치](#)의 설치 지침을 따르십시오.
- 수리할 수 없는 서버를 교체 서버가 도착했던 것과 동일한 포장에 포장하십시오. AWS
- 주문 구성 세부 정보 또는 교체 서버 주문에 첨부된 콘솔에 있는 선불 반송 배송 라벨을 사용합니다.
- 서버를 에 반납하십시오. AWS자세한 내용은 [AWS Outposts 서버 반송](#)을 참조하세요.

## 펌웨어 업데이트

Outpost 펌웨어 업데이트는 일반적으로 Outpost의 인스턴스에는 영향을 주지 않습니다. 업데이트를 설치하기 위해 Outpost 장비를 재부팅해야 하는 드문 경우에는 해당 용량으로 실행되는 모든 인스턴스에 대해 인스턴스 사용 중지 통지를 받게 됩니다.

## 전력 및 네트워크 이벤트에 대한 모범 사례

AWS Outposts 고객 [AWS 서비스 약관에](#) 명시된 바와 같이 Outposts 장비가 위치한 시설은 Outposts 장비의 설치, 유지 관리 및 사용을 지원하기 위한 최소 [전력](#) 및 [네트워크](#) 요구 사항을 충족해야 합니다. Outposts 서버는 전원 및 네트워크 연결이 중단되지 않는 경우에만 제대로 작동할 수 있습니다.

### 전력 이벤트

정전이 완전히 중단되면 AWS Outposts 리소스가 자동으로 서비스 상태로 돌아가지 않을 수 있는 위험이 내재되어 있습니다. 중복 전원 및 백업 전원 솔루션을 배포하는 것 외에도 다음과 같은 작업을 미리 수행하여 일부 최악의 시나리오의 영향을 완화하는 것이 좋습니다.

- DNS기반 또는 랙 외부 로드 밸런싱 변경을 사용하여 통제된 방식으로 Outposts 장비 외부로 서비스와 애플리케이션을 이동하십시오.
- 컨테이너, 인스턴스, 데이터베이스를 순서대로 증분 방식으로 중지하고 복원 시 역순으로 사용합니다.
- 서비스의 통제된 이동 또는 중지에 대한 계획을 테스트합니다.
- 중요한 데이터와 구성을 백업하고 Outpost 외부에 저장합니다.
- 전력 가동 중지 시간을 최소화합니다.
- 유지 관리 중에는 전원 공급 장치 () off-on-off-on 를 반복해서 전환하지 마십시오.
- 유지 관리 기간 내에 예상치 못한 상황에 대처할 수 있도록 여분의 시간을 할애합니다.
- 일반적으로 필요한 것보다 더 넓은 유지 관리 기간을 전달하여 사용자와 고객의 기대치를 관리합니다.

## 네트워크 연결 이벤트

Outpost와 AWS 지역 또는 Outposts 홈 지역 간의 [서비스 링크 연결](#)은 일반적으로 네트워크 유지 관리가 완료되면 업스트림 회사 네트워크 장치 또는 타사 연결 공급자의 네트워크에서 발생할 수 있는 네트워크 중단이나 문제로부터 자동으로 복구됩니다. 서비스 링크 연결이 끊기는 동안에는 Outpost 작업이 로컬 네트워크 활동으로 제한됩니다.

Outposts 서버의 Amazon EC2 인스턴스, LNI 네트워킹 및 인스턴스 스토리지 볼륨은 계속해서 정상적으로 작동하며 로컬 네트워크를 통해 로컬로 액세스할 수 있습니다. LNI 마찬가지로 Amazon ECS 작업자 노드와 같은 AWS 서비스 리소스는 로컬에서 계속 실행됩니다. 하지만 API 가용성은 저하될 것입니다. 예를 들어 실행, 시작, 중지 및 종료가 작동하지 APIs 않을 수 있습니다. 인스턴스 지표와 로그는 몇 시간 동안 로컬에 계속 캐시되며, 연결이 다시 시작되면 AWS 해당 지역으로 푸시됩니다. 그러나 몇 시간 이상 연결이 끊기면 지표와 로그가 손실될 수 있습니다.

현장 전원 문제 또는 네트워크 연결 손실로 인해 서비스 링크가 중단된 경우 Outposts를 소유한 계정으로 알림을 AWS Health Dashboard 보냅니다. 서비스 링크 중단이 예상되더라도 사용자나 사용자 모두 서비스 링크 중단 알림을 표시하지 않을 AWS 수 없습니다. 자세한 내용은 AWS Health 사용 설명서의 [AWS Health Dashboard 시작하기](#)를 참조하세요.

계획된 서비스 유지 관리가 네트워크 연결에 영향을 미칠 경우 다음과 같은 사전 조치를 취하여 잠재적인 문제 시나리오의 영향을 제한합니다.

- 네트워크 유지 관리를 관리할 수 있는 경우 서비스 링크의 가동 중지 시간을 제한합니다. 네트워크가 복구되었는지 확인하는 단계를 유지 관리 프로세스에 포함시킵니다.
- 네트워크 유지 관리를 관리할 수 없는 경우, 공지된 유지 관리 기간과 관련하여 서비스 링크 다운타임을 모니터링하고 공지된 유지 관리 기간이 끝나도 서비스 링크가 백업되지 않으면 계획된 네트워크 유지 관리 담당자에게 조기에 에스컬레이션합니다.

## 리소스

다음은 계획된 또는 예상치 못한 전력 또는 네트워크 사고 이후 Outposts가 정상적으로 작동하고 있는지 확인할 수 있는 몇 가지 모니터링 관련 리소스입니다.

- AWS 블로그 [모니터링 모범 사례에서는 Outposts와](#) 관련된 오퍼버빌리티 및 이벤트 관리 모범 사례를 AWS Outposts 다룹니다.
- [Amazon의 네트워크 연결을 위한 AWS 블로그 디버깅 도구에서는 AWSSupport-SetupIPMonitoring From](#) 도구에 VPC 대해 설명합니다. VPC 이 도구는 사용자가 지정한 서브넷에 Amazon EC2

Monitor 인스턴스를 생성하고 대상 IP 주소를 모니터링하는 AWS Systems Manager SSM 문서 (문서)입니다. 이 문서는 핑MTR, TCP 추적 경로 및 경로 추적 진단 테스트를 실행하고 결과를 Amazon CloudWatch Logs에 저장하며 CloudWatch 대시보드에서 시각화할 수 있습니다 (예: 지연 시간, 패킷 손실). Outposts 모니터링의 경우 Monitor 인스턴스는 상위 AWS 지역의 한 서브넷에 있어야 하며 해당 프라이빗 IP를 사용하여 하나 이상의 Outpost 인스턴스를 모니터링하도록 구성해야 합니다. 그러면 상위 지역 간의 AWS Outposts 패킷 손실 그래프와 지연 시간이 제공됩니다. AWS

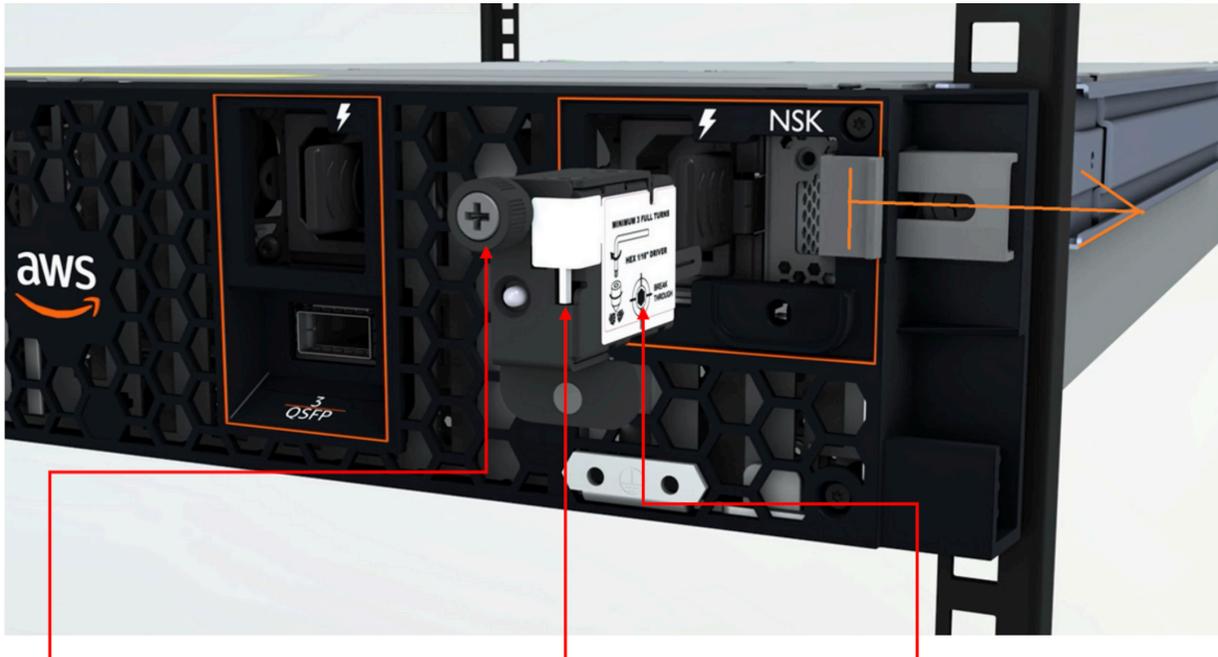
- [AWS Outposts 사용을 위한 자동 Amazon CloudWatch 대시보드 배포 AWS 블로그](#)에서는 자동화된 대시보드 배포와 관련된 단계를 AWS CDK 설명합니다.
- 질문이 있거나 자세한 정보가 필요한 경우, AWS 지원 사용 설명서의 [지원 사례 생성](#)을 참조하세요.

## 암호화 방식으로 파쇄된 서버 데이터

서버의 데이터를 해독하려면 Nitro 보안 키 (NSK) 가 필요합니다. 서버를 교체하거나 서비스를 중단하기 위해 AWS 서버를 다시 서버로 되돌리면 NSK 파기하여 서버의 데이터를 암호적으로 파쇄할 수 있습니다.

서버의 데이터를 암호화 방식으로 파쇄하려면 다음과 같이 하세요.

1. 서버를 다시 NSK 배송하기 전에 서버에서 제거하십시오. AWS
2. 서버와 함께 제공된 올바른 NSK 제품을 가지고 있는지 확인하십시오.
3. 스티커 아래에 있는 소형 육각 도구 및 육각 렌치를 제거합니다.
4. 육각 도구를 사용하여 스티커 아래에 있는 작은 나사를 세 바퀴 완전히 돌립니다. 이 작업을 수행하면 서버의 모든 데이터가 NSK 삭제되고 암호화된 방식으로 파기됩니다.



NSK thumbscrew

HEX tool included with NSK

Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

## Outposts 서버 옵션 end-of-term

AWS Outposts 학기가 끝나면 다음 옵션 중에서 선택해야 합니다.

- [구독을 갱신하고](#) 기존 Outposts 서버를 유지하세요.
- [구독을 종료하고](#) Outposts 서버를 반납하세요.
- [month-to-month 구독으로 전환하고](#) 기존 Outposts 서버를 유지하세요.

### 구독 갱신

Outposts 서버의 현재 구독이 종료되기 최소 30일 전에 다음 단계를 완료해야 합니다.

구독을 갱신하고 기존 Outposts 서버를 유지하려면

1. [AWS Support 센터](#) 콘솔로 로그인합니다.
2. 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 서비스에서 결제를 선택합니다.
5. 카테고리에서 기타 결제 질문을 선택합니다.
6. 심각도에서 중요 질문을 선택합니다.
7. 다음 단계: 추가 정보를 선택합니다
8. 추가 정보 페이지의 제목에 **Renew my Outpost subscription** 다음과 같이 갱신 요청을 입력합니다.
9. 설명에 다음 결제 옵션 중 하나를 입력합니다.
  - 선수금 없음
  - 부분 선결제
  - 전체 선결제

가격은 [AWS Outposts 서버 가격](#)을 참조하세요. 가격 견적을 요청할 수도 있습니다.

10. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.
11. 문의처 페이지에서 선호하는 언어를 선택합니다.
12. 선호하는 연락 방법을 선택합니다.

13. 사례 세부 정보를 검토한 다음 제출을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.

AWS 고객 지원 부서에서 구독 갱신 프로세스를 시작합니다. 새 구독은 현재 구독이 종료된 다음 날에 시작됩니다.

구독을 갱신하거나 Outposts 서버를 반환하겠다는 의사를 표시하지 않으면 자동으로 구독으로 전환됩니다. month-to-month Outpost는 구성에 해당하는 선결제 없음 결제 옵션의 비율로 월 단위로 갱신됩니다. AWS Outposts 새 월별 구독은 현재 구독이 종료된 다음 날에 시작됩니다.

## 구독을 종료하고 서버를 반환하세요.

Outposts 서버의 현재 구독이 종료되기 최소 30일 전에 다음 단계를 완료해야 합니다. AWS 그렇게 하기 전까지는 반품 절차를 시작할 수 없습니다.

### Important

AWS 지원 케이스를 열어 구독을 종료한 후에는 반품 프로세스를 중단할 수 없습니다.

구독을 종료하려면

1. [AWS Support 센터](#) 콘솔로 로그인합니다.
2. 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 서비스에서 결제를 선택합니다.
5. 카테고리에서 기타 결제 질문을 선택합니다.
6. 심각도에서 중요 질문을 선택합니다.
7. 다음 단계: 추가 정보를 선택합니다
8. 추가 정보 페이지에서, 제목에 **End my Outpost subscription**와(과) 같이 명백한 요청을 입력합니다.
9. 설명에 구독을 종료하려는 날짜를 입력합니다.
10. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.
11. 문의처 페이지에서 선호하는 언어를 선택합니다.
12. 선호하는 연락 방법을 선택합니다.
13. 필요한 경우 서버에 있는 모든 인스턴스와 인스턴스 데이터를 백업하십시오.

14. 서버에서 시작된 인스턴스를 종료합니다.
15. 사례 세부 정보를 검토한 다음 제출을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.
16. 지원 사례에서 지시할 때까지 NOT 전원을 끄거나 네트워크 연결을 끊으십시오.

서버를 반납하려면 AWS Outposts 서버 [반납](#) 절차를 따르십시오. AWS Outposts

## month-to-month 구독으로 전환하기

month-to-month 구독으로 전환하고 기존 Outposts 서버를 유지하려면 별도의 조치가 필요하지 않습니다. 궁금한 점은 청구 지원 사례를 여세요.

Outpost는 구성에 해당하는 선결제 없음 결제 옵션의 비율로 월 단위로 갱신됩니다. AWS Outposts 새 월간 구독은 현재 구독이 종료된 다음 날부터 시작됩니다.

## AWS Outposts에 대한 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 모든 할당량에 대한 증가를 요청할 수 없습니다.

AWS Outposts에 대한 할당량을 보려면 [Service Quotas 콘솔](#)을 엽니다. 탐색 창에서 AWS 서비스를 (를) 선택한 다음 AWS Outposts을(를) 선택합니다.

할당량 증가를 요청하려면 [Service Quotas 사용 설명서](#)의 할당량 증가 요청을 참조하십시오.

AWS 계정에는 AWS Outposts와 관련하여 다음과 같은 할당량이 있습니다.

리소스	기본값	조정 가능	설명
Outpost 사이트	100	<a href="#">예</a>	<p>Outpost 사이트는 Outpost 장비에 전원을 공급하고 네트워크에 연결하는 고객이 관리하는 물리적 건물입니다.</p> <p>AWS 계정의 각 리전에는 100개의 Outpost 사이트를 만들 수 있습니다.</p>
사이트당 Outpost	10	<a href="#">예</a>	<p>AWS Outposts은(는) Outpost라고 하는 하드웨어 및 가상 리소스를 포함합니다. 이 할당량은 Outpost 가상 리소스를 제한합니다.</p> <p>각 Outpost 내에 10개의 Outpost를 생성할 수 있습니다.</p>

## AWS Outposts 그리고 다른 서비스에 대한 할당량

AWS Outposts은(는) 다른 서비스의 리소스에 의존하며 해당 서비스에는 자체 기본 할당량이 있을 수 있습니다. 예를 들어, 로컬 네트워크 인터페이스의 할당량은 네트워크 인터페이스의 Amazon VPC 할당량에서 나옵니다.

다음 표에서는 Outposts 서버의 설명서 업데이트에 대해 설명합니다.

변경 사항	설명	날짜
<a href="#">용량 관리</a>	새 Outposts 주문에 대한 기본 용량 구성을 수정할 수 있습니다.	2024년 4월 16일
<a href="#">서버를 위한 E 옵션 on-demand AWS Outposts</a>	AWS Outposts 기간이 만료되면 구독을 갱신, 종료 또는 전환할 수 있습니다.	2023년 8월 1일
<a href="#">AWS Outposts Outposts 서버를 위한 사용자 가이드 작성</a>	AWS Outposts 사용자 가이드는 랙과 서버에 대한 별도의 가이드로 구성되었습니다.	2022년 9월 14일
<a href="#">플레이스먼트 그룹: AWS Outposts</a>	분산 전략을 사용하는 배치 그룹은 호스트 전반에서 인스턴스를 분산할 수 있습니다.	2022년 6월 30일
<a href="#">전용 호스팅 커짐 AWS Outposts</a>	이제 Outposts의 전용 호스트를 사용할 수 있습니다.	2022년 5월 31일
<a href="#">Outposts 서버 소개</a>	새로운 AWS Outposts 폼 팩터인 Outposts 서버를 추가했습니다.	2021년 11월 30일

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