



기본 사항 학습

Setup and administration

NetApp
February 02, 2026

목차

기본 사항 학습	1
NetApp Workload Factory에 대해 알아보세요	1
피처	1
지원되는 클라우드 공급자	2
보안	2
비용	2
Workload Factory 작동 방식	2
NetApp Workload Factory를 사용하는 도구	4
콘솔 환경	5
NetApp 콘솔에서 Workload Factory에 액세스	5
Workload Factory 콘솔에서 Workload Factory에 액세스하세요	5
NetApp Workload Factory에 대한 권한	6
사용 권한을 사용하는 이유	6
워크로드별 권한	6
변경 로그	51

기본 사항 학습

NetApp Workload Factory에 대해 알아보세요

NetApp Workload Factory는 Amazon FSx for NetApp ONTAP 파일 시스템을 사용하여 워크로드를 최적화하는 데 도움이 되도록 설계된 강력한 수명 주기 관리 플랫폼입니다.

Workload Factory와 FSx for ONTAP 사용하여 간소화할 수 있는 워크로드로는 데이터베이스, VMware Cloud on AWS로의 VMware 마이그레이션, AI 챗봇 등이 있습니다.

워크로드란 비즈니스 목표를 달성하기 위해 설계된 리소스, 코드, 서비스 또는 애플리케이션의 조합을 의미합니다. 이는 고객 대면 애플리케이션부터 백엔드 프로세스에 이르기까지 무엇이든 될 수 있습니다. 워크로드는 단일 AWS 계정 내의 리소스 일부를 사용하거나 여러 계정에 걸쳐 리소스를 사용할 수 있습니다.

Amazon FSx for NetApp ONTAP 미션 크리티컬 애플리케이션, 데이터베이스, 컨테이너, VMware Cloud 데이터 저장소 및 사용자 파일을 위한 완전 관리형 AWS 기반 NFS, SMB/CIFS 및 iSCSI 스토리지 볼륨을 제공합니다. Workload Factory와 기본 AWS 관리 도구를 사용하여 FSx for ONTAP 을 관리할 수 있습니다.

피처

Workload Factory 플랫폼은 다음과 같은 주요 기능을 제공합니다.

유연하고 저렴한 스토리지

클라우드에서 Amazon FSx for NetApp ONTAP 파일 시스템을 검색, 배포 및 관리합니다. FSx for ONTAP은 일관된 하이브리드 클라우드 경험을 제공하는 네이티브 AWS 관리형 서비스에 ONTAP의 모든 기능을 제공합니다.

온프레미스 vSphere 환경을 AWS의 VMware Cloud로 마이그레이션합니다

VMware Cloud on AWS 마이그레이션 어드바이저를 사용하면 온프레미스 vSphere 환경에서 현재 가상 머신 구성을 분석하고 권장 VM 레이아웃을 AWS 기반 VMware Cloud에 배포하고 맞춤형 Amazon FSx for NetApp ONTAP 파일 시스템을 외부 데이터 저장소로 사용할 수 있습니다.

데이터베이스 라이프사이클 관리

Amazon FSx for NetApp ONTAP를 사용하여 데이터베이스 워크로드를 검색하고 비용 절감 효과를 분석, SQL 서버 데이터베이스를 FSx for ONTAP 스토리지로 마이그레이션할 때 스토리지 및 애플리케이션의 이점을 활용하고, 공급업체 모범 사례를 구현하는 SQL 서버, 데이터베이스, 데이터베이스 클론을 배포하고, 인프라를 코드 공동 파일럿으로 사용하여 운영을 자동화하고, SQL 서버 환경을 지속적으로 모니터링 및 최적화하여 성능, 가용성, 보호, 비용 효율성을 개선합니다.

AI 챗봇 개발

FSx for ONTAP 파일 시스템을 활용하여 조직의 챗봇 소스 및 AI Engine 데이터베이스를 저장합니다. 이를 통해 조직의 비정형 데이터를 엔터프라이즈 챗봇 애플리케이션에 포함할 수 있습니다.

비용 절감을 위한 절약 계산기

Amazon EBS(Elastic Block Store) 또는 EFS(Elastic File System) 스토리지 또는 Amazon FSx for Windows File Server를 사용하는 현재 배포를 분석하여 Amazon FSx for NetApp ONTAP으로 전환할 경우 절감할 수 있는 비용을 확인하십시오. 또한 계산기를 사용하여 계획 중인 향후 배포를 위한 "가상" 시나리오를 수행할 수도 있습니다.

자동화를 촉진하기 위한 서비스 계정

서비스 계정을 사용하여 NetApp Workload Factory 작업을 안전하고 안정적으로 자동화하세요. 서비스 계정은

사용자 관리 제한 없이 안정적이고 오래 지속되는 자동화를 제공하며 API 액세스만 제공하므로 보안이 더욱 강화되었습니다.

Ask Me AI 비서

AI 비서에게 FSx for ONTAP 파일 시스템을 관리하고 운영하는 방법에 대해 질문해 보세요. Ask Me는 MCP(Model Context Protocol)를 사용하여 외부 환경과 안전하게 인터페이스하고 API 도구를 쿼리하여 특정 스토리지 환경에 맞춤형 응답을 제공합니다.

지원되는 클라우드 공급자

Workload Factory를 사용하면 Amazon Web Services에서 클라우드 스토리지를 관리하고 워크로드 기능을 사용할 수 있습니다.

보안

NetApp Workload Factory의 보안은 NetApp에게 최우선 과제입니다. Workload Factory의 모든 워크로드는 Amazon FSx for NetApp ONTAP에서 실행됩니다. 이 모든 것 외에도 ["AWS 보안 기능"](#) NetApp Workload Factory 인증을 받았습니다. ["SOC2 1종 규정 준수, SOC2 2종 규정 준수 및 HIPAA 규정 준수"](#).

NetApp Workload Factory Amazon FSx for NetApp ONTAP는 ["엔터프라이즈 앱 배포를 위한 AWS 솔루션"](#) 잘 설계된 모범 사례를 염두에 두고 만들어졌습니다.

비용

Workload Factory는 무료로 사용할 수 있습니다. Amazon Web Services(AWS)에 지불하는 비용은 배포하려는 스토리지 및 워크로드 서비스에 따라 달라집니다. 여기에는 Amazon FSx for NetApp ONTAP, AWS 인프라의 VMware Cloud, AWS 서비스 등의 비용이 포함됩니다.

Workload Factory 작동 방식

Workload Factory에는 SaaS 계층을 통해 제공되는 웹 기반 콘솔, 계정, 클라우드 자산에 대한 액세스를 제어하는 운영 모드, Workload Factory와 AWS 계정 간에 분리된 연결을 제공하는 링크 등이 포함되어 있습니다.

서비스형 소프트웨어

Workload Factory는 다음을 통해 액세스할 수 있습니다. ["NetApp Workload Factory 콘솔"](#) 그리고 ["NetApp 콘솔"](#). 이러한 SaaS 환경을 사용하면 최신 기능이 출시되면 자동으로 액세스할 수 있으며 Workload Factory 계정과 링크 간에 쉽게 전환할 수 있습니다.


["다양한 콘솔 경험에 대해 자세히 알아보세요"](#)

계정

처음으로 Workload Factory에 로그인하면 계정을 만들라는 메시지가 표시됩니다. 이 계정을 사용하면 자격 증명을 사용하여 조직의 리소스, 워크로드 및 워크로드 액세스를 구성할 수 있습니다.

Hello Richard,

Let's get started by creating an account.



An account is the top-level element in NetApp's identity platform. It enables you to add and manage permissions and credentials.

[Learn more about accounts.](#)

Account name

To help us organize menu options that best suit your objectives, we suggest that you provide us with some background about your job.

My job description Optional

계정을 만들면 해당 계정의 single_account admin_user가 됩니다.

조직에서 추가 계정 또는 사용자 관리가 필요한 경우 제품 내 채팅을 사용하여 문의하십시오.



NetApp 콘솔을 사용하는 경우 Workload Factory가 NetApp 계정을 활용하므로 이미 계정에 속해 있습니다.

서비스 계정

서비스 계정은 자동화 목적으로 NetApp Workload Factory에 승인된 API 호출을 할 수 있는 "사용자" 역할을 합니다. 이렇게 하면 언제든지 회사를 떠날 수 있는 실제 사람의 사용자 계정을 기반으로 자동화 스크립트를 작성할 필요가 없으므로 자동화를 관리하기가 더 쉬워집니다. Workload Factory의 모든 계정 소유자는 계정 관리자로 간주됩니다. 계정 관리자는 여러 개의 서비스 계정을 만들고 삭제할 수 있습니다.

["서비스 계정을 관리하는 방법에 대해 알아봅니다"](#)

권한

Workload Factory는 클라우드 자산에 대한 액세스를 신중하게 제어하고 IT 정책에 따라 Workload Factory에 점진적인 신뢰를 할당할 수 있는 유연한 권한 정책을 제공합니다.

["Workload Factory 권한 정책에 대해 자세히 알아보세요."](#)

연결 링크

Workload Factory 링크는 Workload Factory와 하나 이상의 FSx for ONTAP 파일 시스템 간에 신뢰 관계와 연결을 생성합니다. 이를 통해 Amazon FSx for ONTAP API를 통해서만 사용할 수 없는 특정 파일 시스템 기능을 ONTAP REST API 호출에서 직접 모니터링하고 관리할 수 있습니다.

Workload Factory를 시작하는 데는 링크가 필요하지 않지만, 어떤 경우에는 모든 Workload Factory 기능과 워크로드 기능을 잠금 해제하려면 링크를 만들어야 합니다.

현재 링크에서는 AWS Lambda를 활용하고 있습니다.

["링크에 대해 자세히 알아보십시오"](#)

코드박스 자동화

Codebox는 개발자와 DevOps 엔지니어가 Workload Factory에서 지원하는 모든 작업을 실행하는 데 필요한 코드를 생성하는 데 도움이 되는 Infrastructure as Code(IaC) 파일럿입니다. 코드 형식에는 Workload Factory REST API, AWS CLI, AWS CloudFormation이 포함됩니다.

Codebox는 Workload Factory 운영 모드(기본, 읽기 전용, 읽기/쓰기)에 맞춰 조정되며 실행 준비를 위한 명확한 경로와 빠른 향후 재사용을 위한 자동화 카탈로그를 설정합니다.

코드박스 창에는 특정 작업 흐름 작업에 의해 생성되고 그래픽 마법사 또는 대화 채팅 인터페이스에 의해 일치하는 IAC가 표시됩니다. Codebox는 손쉬운 탐색 및 분석을 위한 색상 코딩 및 검색을 지원하지만 편집은 허용되지 않습니다. 자동화 카탈로그에는 복사하거나 저장할 수만 있습니다.

"Codebox에 대해 자세히 알아보십시오"

비용 절감 계산기

Workload Factory는 스토리지 환경, 데이터베이스 또는 VMware 워크로드의 비용을 FSx for ONTAP 파일 시스템에서 다른 Amazon 서비스와 비교할 수 있도록 비용 절감 계산기를 제공합니다. 저장 용량 요구 사항에 따라 FSx for ONTAP 파일 시스템이 가장 비용 효율적인 옵션이 될 수 있습니다.

- ["스토리지 환경의 비용 절감 방법을 알아보십시오"](#)
- ["데이터베이스 워크로드 비용 절감 방법을 알아보십시오"](#)
- ["VMware 워크로드 비용 절감 방법을 알아보세요."](#)

잘 설계된 워크로드

Workload Factory는 AWS Well-Architected Framework에 부합하는 안정적이고 안전하며 효율적이고 비용 효율적인 스토리지 및 데이터베이스 구성을 유지 관리하고 운영할 수 있도록 지원합니다. Workload Factory는 FSx에서 ONTAP 파일 시스템, SQL Server 및 Oracle 데이터베이스 배포를 매일 검사하여 잠재적인 구성 오류에 대한 정보를 제공하고 문제를 해결하기 위한 수동 또는 자동 조치를 권장합니다.

"잘 설계된 워크로드에 대해 자세히 알아보세요."

NetApp Workload Factory를 사용하는 도구

다음 도구와 함께 NetApp Workload Factory를 사용할 수 있습니다.

- **Workload Factory 콘솔:** Workload Factory 콘솔은 애플리케이션과 프로젝트에 대한 시각적이고 전체적인 보기를 제공합니다.
- *** NetApp 콘솔:** NetApp 콘솔은 Workload Factory를 다른 NetApp 데이터 서비스와 함께 사용할 수 있도록 하이브리드 인터페이스 환경을 제공합니다.
- **질문하기:** Workload Factory 콘솔을 벗어나지 않고도 Ask me AI 도우미를 사용하여 질문을 하고 Workload Factory에 대해 자세히 알아보세요. Workload Factory 도움말 메뉴에서 Ask me에 액세스하세요.
- **CloudShell CLI:** Workload Factory에는 단일 브라우저 기반 CLI를 통해 여러 계정의 AWS 및 NetApp 환경을 관리하고 운영할 수 있는 CloudShell CLI가 포함되어 있습니다. Workload Factory 콘솔의 상단 표시줄에서 CloudShell에 액세스합니다.
- **REST API:** Workload Factory REST API를 사용하여 FSx for ONTAP 파일 시스템 및 기타 AWS 리소스를 배포하고 관리합니다.

- **CloudFormation**: AWS CloudFormation 코드를 사용하여 Workload Factory 콘솔에서 정의한 작업을 수행하여 AWS 계정의 CloudFormation 스택에서 AWS 및 타사 리소스를 모델링, 프로비저닝 및 관리합니다.
- **Terraform NetApp Workload Factory** 공급자: Terraform을 사용하여 Workload Factory 콘솔에서 생성된 인프라 워크플로를 구축하고 관리합니다.

REST API

Workload Factory를 사용하면 특정 워크로드에 맞게 FSx for ONTAP 파일 시스템을 최적화, 자동화하고 운영할 수 있습니다. 각 워크로드는 연관된 REST API를 노출합니다. 이러한 워크로드와 API를 합치면 FSx for ONTAP 파일 시스템을 관리하는 데 사용할 수 있는 유연하고 확장 가능한 개발 플랫폼이 형성됩니다.

Workload Factory REST API를 사용하면 다음과 같은 여러 가지 이점이 있습니다.

- API는 REST 기술과 최신 모범 사례를 기반으로 설계되었습니다. 핵심 기술로는 HTTP와 JSON이 있습니다.
- Workload Factory 인증은 OAuth2 표준을 기반으로 합니다. NetApp Auth0 서비스 구현에 의존합니다.
- Workload Factory 웹 기반 콘솔은 동일한 핵심 REST API를 사용하므로 두 액세스 경로 간에 일관성이 유지됩니다.

["Workload Factory REST API 문서 보기"](#)

콘솔 환경

NetApp Workload Factory는 두 개의 웹 기반 콘솔을 통해 접근할 수 있습니다. Workload Factory 콘솔과 NetApp 콘솔을 사용하여 Workload Factory에 액세스하는 방법을 알아보세요.

- * NetApp 콘솔*: Amazon FSx for NetApp ONTAP for ONTAP 파일 시스템과 워크로드를 동일한 장소에서 관리할 수 있는 하이브리드 환경을 제공합니다.
- **Workload Factory** 콘솔: Amazon FSx for NetApp ONTAP 에서 실행되는 워크로드에 중점을 둔 전용 Workload Factory 환경을 제공합니다.

NetApp 콘솔에서 Workload Factory에 액세스

NetApp Console 에서 Workload Factory에 액세스할 수 있습니다. AWS 스토리지 및 워크로드 기능에 Workload Factory를 사용하는 것 외에도 NetApp Copy and Sync 등의 다른 데이터 서비스에도 액세스할 수 있습니다.

단계

1. 에 로그인하세요["NetApp 콘솔"](#) .
2. NetApp 콘솔 메뉴에서 *워크로드*를 선택한 다음 *개요*를 선택합니다.

Workload Factory 콘솔에서 Workload Factory에 액세스하세요

Workload Factory 콘솔에서 Workload Factory에 액세스할 수 있습니다.

단계

1. 에 로그인하세요["워크로드 팩토리 콘솔"](#) .

NetApp Workload Factory에 대한 권한

NetApp Workload Factory 기능과 서비스를 사용하려면 Workload Factory가 클라우드 환경에서 작업을 수행할 수 있도록 권한을 제공해야 합니다.

사용 권한을 사용하는 이유

권한을 제공하면 Workload Factory는 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있는 권한이 있는 정책을 인스턴스에 연결합니다. 이를 통해 Workload Factory는 스토리지 환경 검색부터 스토리지 관리의 파일 시스템이나 GenAI 워크로드의 지식 기반과 같은 AWS 리소스 배포까지 다양한 작업을 실행할 수 있습니다.

예를 들어 데이터베이스 워크로드의 경우 Workload Factory에 필요한 권한이 부여되면 지정된 계정 및 지역의 모든 EC2 인스턴스를 스캔하고 모든 Windows 기반 머신을 필터링합니다. AWS Systems Manager(SSM) 에이전트가 호스트에 설치되어 실행 중이고 System Manager 네트워킹이 올바르게 구성된 경우 Workload Factory는 Windows 머신에 액세스하여 SQL Server 소프트웨어가 설치되었는지 확인할 수 있습니다.

워크로드별 권한

각 워크로드는 Workload Factory에서 특정 작업을 수행하기 위해 권한을 사용합니다. 권한은 설정된 권한 정책에 묶여 있습니다. 권한 정책, 권한 정책에 대한 복사 가능한 JSON, 모든 권한, 권한의 목적, 사용 위치, 권한을 지원하는 권한 정책이 나열된 표에 대해 자세히 알아보려면 사용하는 작업으로 스크롤하세요.

저장소 사용 권한

Storage에 사용할 수 있는 IAM 정책은 Workload Factory가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하는데 필요한 권한을 제공합니다.

저장소에는 다음과 같은 권한 정책 중에서 선택할 수 있습니다.

- 보기, 계획 및 분석: FSx for ONTAP 파일 시스템을 보고, 시스템 상태에 대해 알아보고, 시스템에 맞게 잘 설계된 분석을 받고, 절감 방안을 살펴보세요.
- 운영 및 수정: 파일 시스템 용량을 조정하고 파일 시스템 구성에 대한 문제를 해결하는 등의 운영 작업을 수행합니다.
- 파일 시스템 생성 및 삭제: FSx for ONTAP 파일 시스템과 스토리지 VM을 생성하고 삭제합니다.

필요한 IAM 정책을 확인하세요.



보기, 계획 및 분석

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeSharedVpcConfiguration",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "ce:GetCostAndUsage",
        "ce:GetTags",
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

운영 및 개선

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolume",
        "fsx>DeleteVolume",
        "fsx:UpdateFileSystem",

```

```

    "fsx:UpdateStorageVirtualMachine",
    "fsx:UpdateVolume",
    "fsx:CreateBackup",
    "fsx:CreateVolumeFromBackup",
    "fsx:DeleteBackup",
    "fsx:TagResource",
    "fsx:UntagResource",
    "fsx:CreateAndAttachS3AccessPoint",
    "fsx:DetachAndDeleteS3AccessPoint",
    "s3:CreateAccessPoint",
    "s3:DeleteAccessPoint",
    "s3:GetObjectTagging",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:InvokeModel",
    "bedrock:ListInferenceProfiles",
    "bedrock:GetInferenceProfile",
    "s3tables:CreateTableBucket",
    "s3tables:ListTables",
    "s3tables:GetTable",
    "s3tables:GetTableMetadataLocation",
    "s3tables:CreateTable",
    "s3tables:GetNamespace",
    "s3tables:PutTableData",
    "s3tables:CreateNamespace",
    "s3tables:GetTableData",
    "s3tables:ListNamespaces",
    "s3tables:ListTableBuckets",
    "s3tables:GetTableBucket",
    "s3tables:UpdateTableMetadataLocation",
    "s3tables:ListTagsForResource",
    "s3tables:TagResource",
    "s3:GetObjectTagging",
    "s3:ListBucket"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "iam:SimulatePrincipalPolicy"
  ],
  "Resource": "*"
}
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx>DeleteFileSystem",
        "fsx>DeleteStorageVirtualMachine",
        "fsx:TagResource",
        "fsx:UntagResource",
        "kms:CreateGrant",
        "iam:CreateServiceLinkedRole",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumeStatus",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2>DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    }
  ],

```

```
{
  "Effect": "Allow",
  "Action": [
    "iam:SimulatePrincipalPolicy"
  ],
  "Resource": "*"
}
```

다음 표에는 스토리지에 대한 사용 권한이 나와 있습니다.

목적	조치	사용된 위치	허가 정책
FSx for ONTAP 파일 시스템을 생성합니다	FSX:CreateFileSystem 을 참조하십시오	구축	파일 시스템 생성 및 삭제
FSx for ONTAP 파일 시스템에 대한 보안 그룹을 생성합니다	EC2:CreateSecurityGroup입니다	구축	파일 시스템 생성 및 삭제
FSx for ONTAP 파일 시스템의 보안 그룹에 태그를 추가합니다	EC2: CreateTags(태그 생성)	구축	파일 시스템 생성 및 삭제
FSx for ONTAP 파일 시스템에 대한 보안 그룹 송신 및 수신 권한을 부여합니다	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	파일 시스템 생성 및 삭제
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	파일 시스템 생성 및 삭제
허가된 역할은 FSx for ONTAP과 다른 AWS 서비스 간에 통신을 제공합니다	IAM: CreateServiceLinkedRole	구축	파일 시스템 생성 및 삭제
FSx for ONTAP 파일 시스템 배포 양식을 작성하는 방법에 대해 자세히 알아보십시오	EC2: 설명	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제
	EC2: DescribeSubnet	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제
	EC2: DescribeSecurityGroups	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제
	EC2: 설명표	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제
	EC2: DescribeNetworkInterfaces를 참조하십시오	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제
	EC2: VolumeStatus를 설명합니다	<ul style="list-style-type: none"> • 구축 • 비용 절감 효과를 	파일 시스템 생성 및 삭제

목적	조치	사용된 위치	허가 정책
KMS 키 세부 정보를 얻고 FSx for ONTAP 암호화를 사용합니다	KMS: CreateGrant	구축	파일 시스템 생성 및 삭제
	KMS: 설명키	구축	파일 시스템 생성 및 삭제
	KMS: ListKeys	구축	파일 시스템 생성 및 삭제
	KMS: ListAliases	구축	파일 시스템 생성 및 삭제
EC2 인스턴스의 볼륨 세부 정보를 가져옵니다	EC2: 설명 볼륨을 참조하십시오	<ul style="list-style-type: none"> 인벤토리 비용 절감 효과를 	보기, 계획 및 분석
EC2 인스턴스에 대한 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	비용 절감 효과를	보기, 계획 및 분석
비용 절감 계산기에 Elastic File System에 대해 설명하십시오	Elasticfilesystem:DescribeFileSystems	비용 절감 효과를	보기, 계획 및 분석
FSx for ONTAP 리소스의 태그를 나열합니다	FSX:ListTagsForResource.를 참조하십시오	인벤토리	보기, 계획 및 분석
FSx for ONTAP 파일 시스템에 대한 보안 그룹 송신 및 수신을 관리합니다	EC2: RevokeSecurityGroupIngress 를 참조하십시오	관리 운영	파일 시스템 생성 및 삭제
	ec2: 보안 그룹 탈퇴 취소	관리 운영	파일 시스템 생성 및 삭제
	EC2: DeleteSecurityGroup	관리 운영	파일 시스템 생성 및 삭제

목적	조치	사용된 위치	허가 정책
FSx for ONTAP 파일 시스템 리소스를 생성, 확인, 관리합니다	FSX:CreateVolume 을 참조하십시오	관리 운영	운영 및 개선
	FSX:태그 리소스	관리 운영	운영 및 개선
	FSx:CreateStorageVirtualMachine	관리 운영	파일 시스템 생성 및 삭제
	fsx:파일 시스템 삭제	관리 운영	파일 시스템 생성 및 삭제
	fsx:저장소 가상 머신 삭제	관리 운영	보기, 계획 및 분석
	FSx:파일 시스템 설명	인벤토리	보기, 계획 및 분석
	FSX:DescribeStorageVirtualMachines를 참조하십시오	인벤토리	보기, 계획 및 분석
	fsx:공유Vpc구성 설명	인벤토리	보기, 계획 및 분석
	fsx:파일 시스템 업데이트	관리 운영	운영 및 개선
	fsx:업데이트 스토리지 가상 머신	관리 운영	운영 및 개선
	FSx:볼륨 설명	인벤토리	보기, 계획 및 분석
	FSX:UpdateVolume을 참조하십시오	관리 운영	운영 및 개선
	fsx:볼륨 삭제	관리 운영	운영 및 개선
	FSx:UntagResource	관리 운영	운영 및 개선
	FSX:백업 설명	관리 운영	보기, 계획 및 분석
	fsx:백업 생성	관리 운영	운영 및 개선
	fsx:백업에서볼륨생성	관리 운영	운영 및 개선
	fsx:백업 삭제	관리 운영	운영 및 개선
파일 시스템 및 볼륨 메트릭을 가져옵니다	CloudWatch: GetMetricData	관리 운영	보기, 계획 및 분석
	CloudWatch: GetMetricStatistics	관리 운영	보기, 계획 및 분석
워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축	모두

목적	조치	사용된 위치	허가 정책
ONTAP EMS 이벤트에 대한 FSx에 AI 기반 인사이트를 제공합니다.	Bedrock: ListInferenceProfiles 를 참조하십시오	ONTAP EMS 분석을 위한 FSx	운영 및 개선
	기본암: GetInferenceProfile	ONTAP EMS 분석을 위한 FSx	운영 및 개선
	기본암: InvokeModelWithResponseStream	ONTAP EMS 분석을 위한 FSx	운영 및 개선
	Bedrock: InvokeModel 을 참조하십시오	ONTAP EMS 분석을 위한 FSx	운영 및 개선
AWS Cost Explorer에서 FSx for ONTAP 파일 시스템에 대한 비용 및 사용 데이터를 가져옵니다.	ce:GetCostAndUsage	비용 및 사용량 분석	보기, 계획 및 분석
	ce:GetTags	비용 및 사용량 분석	보기, 계획 및 분석
S3 액세스 포인트를 생성하고 이를 FSx for ONTAP 파일 시스템에 연결합니다.	fsx:CreateAndAttachS3AccessPoint	S3 액세스 포인트 관리	운영 및 개선
FSx for ONTAP 파일 시스템에서 S3 액세스 포인트를 분리하고 삭제합니다	fsx:DetachAndDeleteS3AccessPoint	S3 액세스 포인트 관리	운영 및 개선
간소화된 버킷 액세스 관리를 위한 S3 액세스 포인트 생성	s3:CreateAccessPoint	S3 액세스 포인트 관리	운영 및 개선
S3 액세스 포인트를 삭제합니다	s3:DeleteAccessPoint	S3 액세스 포인트 관리	운영 및 개선
S3 액세스 포인트에 태그 추가	s3:TagResource	S3 액세스 포인트 관리	운영 및 개선
S3 액세스 포인트의 태그 나열 및 보기	s3:ListTagsForResource	S3 액세스 포인트 관리	운영 및 개선
S3 액세스 포인트에서 태그 제거	s3:UntagResource	S3 액세스 포인트 관리	운영 및 개선
S3 액세스 포인트 버킷에서 객체 검색	s3:ListBucket	S3 버킷 작업	운영 및 개선
S3 테이블 버킷 나열, 생성 및 설명	s3tables:ListTableBuckets s3tables:CreateTableBucket s3tables:GetTableBucket	S3 table bucket 관리	운영 및 개선
S3 테이블 나열, 생성 및 검색	s3tables:ListTables s3tables:CreateTable s3tables:GetTable	S3 테이블 작업	운영 및 개선
테이블 메타데이터 위치 읽기	s3tables:GetTableMetadataLocation	S3 테이블 메타데이터 작업	운영 및 개선
테이블 metadata 위치 업데이트	s3tables:UpdateTableMetadataLocation	S3 테이블 메타데이터 작업	운영 및 개선

목적	조치	사용된 위치	허가 정책
테이블 네임스페이스를 나열, 생성 및 조회합니다	s3tables:ListNamespaces s3tables:CreateNamespace s3tables:GetNamespace	S3 네임스페이스 작업	운영 및 개선
테이블 데이터 읽기(select, scan)	s3tables:GetTableData	S3 테이블 데이터 작업	운영 및 개선
테이블 데이터 쓰기(삽입)	s3tables:PutTableData	S3 테이블 데이터 작업	운영 및 개선
인벤토리 테이블의 태그 나열(FSx for ONTAP, 스토리지 VM, 볼륨 ID 가져오기)	s3tables:ListTagsForResource	S3 테이블 태그 작업	운영 및 개선
Workload Factory 조회를 위한 인벤토리 테이블에 태그를 지정합니다	s3tables:TagResource	S3 테이블 태그 작업	운영 및 개선
액세스 포인트를 통해 객체 태깅 검색	s3:GetObjectTagging	S3 객체 작업	운영 및 개선

데이터베이스 워크로드에 대한 권한

데이터베이스 워크로드에 사용할 수 있는 IAM 정책은 Workload Factory가 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다.

데이터베이스에는 다음과 같은 권한 정책이 선택 가능합니다.

- 보기, 계획 및 분석: 데이터베이스 리소스 인벤토리를 보고, 리소스 상태를 파악하고, 데이터베이스 구성에 맞게 잘 설계된 분석을 검토하고, 절감 효과를 알아보고, 오류 로그 분석을 받고, 절감 효과를 살펴봅니다.
- 운영 및 수정: 데이터베이스 리소스에 대한 운영 작업을 수행하고 데이터베이스 구성과 기본 FSx for ONTAP 파일 시스템 스토리지에 대한 문제를 해결합니다.
- 데이터베이스 호스트 생성: 모범 사례에 따라 데이터베이스 호스트와 기본 FSx for ONTAP 파일 시스템 스토리지를 배포합니다.

필요한 IAM 정책을 보려면 운영 모드를 선택하십시오.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CommonGroup",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sns:ListTopics",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAddresses",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:DescribeKey",
        "cloudformation:ListStacks",
        "cloudformation:DescribeAccountLimits",
        "ds:DescribeDirectories",
        "fsx:DescribeVolumes",
        "fsx:DescribeBackups",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeFileSystems",
        "servicequotas:ListServiceQuotas",
        "ssm:GetParametersByPath",
        "ssm:GetCommandInvocation",
        "ssm:SendCommand",
        "ssm:GetConnectionStatus",
        "ssm:DescribePatchBaselines",
        "ssm:DescribeInstancePatchStates",
        "ssm:ListCommands",

```

```

        "ssm:DescribeInstanceInformation",
        "fsx:ListTagsForResource",
        "logs:DescribeLogGroups",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "SSMParameterStore",
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:DeleteParameters"
    ],
    "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
},
{
    "Sid": "SSMResponseCloudWatch",
    "Effect": "Allow",
    "Action": [
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
}
]
}

```

운영 및 개선

```
[
  {
    "Sid": "FSxRemediation",
    "Effect": "Allow",
    "Action": [
      "fsx:UpdateFileSystem",
      "fsx:UpdateVolume"
    ],
    "Resource": "*"
  },
  {
    "Sid": "EC2Remediation",
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:StopInstances"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/aws:cloudformation:stack-name":
"WLMDB*"
      }
    }
  }
]
```

데이터베이스 호스트 생성

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2TagGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",

```

```

        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVolume",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTags",
        "ec2>DeleteVolume",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVolume",
        "ec2:DisassociateAddress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolume",
        "ec2:ModifyVolumeAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
        }
    }
},
{
    "Sid": "FSxNGroup",
    "Effect": "Allow",
    "Action": [
        "fsx:TagResource"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
        }
    }
}

```

```

    }
  },
  {
    "Sid": "CreationGroup",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStacks",
      "cloudformation:ValidateTemplate",
      "ec2:CreateLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2:CreateTags",
      "ec2:CreateVpcEndpoint",
      "ec2:RunInstances",
      "ec2:DescribeTags",
      "ec2:DescribeLaunchTemplates",
      "ec2:ModifyVpcAttribute",
      "fsx:CreateFileSystem",
      "fsx:CreateStorageVirtualMachine",
      "fsx:CreateVolume",
      "fsx:DescribeFileSystemAliases",
      "kms:CreateGrant",
      "kms:DescribeCustomKeyStores",
      "kms:GenerateDataKey",
      "kms:Decrypt",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:GetLogGroupFields",
      "logs:GetLogRecord",
      "logs:ListLogDeliveries",
      "logs:PutLogEvents",
      "logs:TagResource",
      "sns:Publish",
      "ssm:PutComplianceItems",
      "ssm:PutConfigurePackageResult",
      "ssm:PutInventory",
      "ssm:UpdateAssociationStatus",
      "ssm:UpdateInstanceAssociationStatus",
      "ssm:UpdateInstanceInformation",
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",

```



```

        "ssmmessages:OpenDataChannel",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:PutRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser"
    ],
    "Resource": "*"
},
{
    "Sid": "ArnGroup",
    "Effect": "Allow",
    "Action": [
        "cloudformation:SignalResource"
    ],
    "Resource": [
        "arn:aws:cloudformation:*:*:stack/WLMDB*",
        "arn:aws:logs:*:*:log-group:WLMDB*"
    ]
},
{
    "Sid": "IAMGroup1",
    "Effect": "Allow",
    "Action": [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": [
        "arn:aws:iam:*:*:instance-profile/*",
        "arn:aws:iam:*:*:role/WLMDB*"
    ]
},
{
    "Sid": "IAMGroup2",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",

```

```

    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/WLMDB*"
    ],
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "IAMGroup3",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/WLMDB*"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "IAMGroup4",
    "Effect": "Allow",
    "Action": "iam:CreateRole",
    "Resource": "arn:aws:iam::*:role/WLMDB*"
}
]
}

```

다음 표에는 데이터베이스 워크로드에 대한 사용 권한이 나와 있습니다.

목적	조치	사용된 위치	허가 정책
FSx for ONTAP, EBS 및 FSx for Windows File Server에 대한 메트릭 통계를 얻고 컴퓨팅 최적화 권장 사항을 확인하세요.	CloudWatch: GetMetricStatistics	<ul style="list-style-type: none"> 인벤토리 비용 절감 효과를 	보기, 계획 및 분석
등록된 SQL 노드에서 Amazon CloudWatch에 저장된 성능 지표를 수집합니다. 데이터는 등록된 SQL 인스턴스의 인스턴스 관리 화면에서 성능 추세 차트로 생성됩니다.	CloudWatch: GetMetricData	인벤토리	보기, 계획 및 분석
EC2 인스턴스에 대한 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	<ul style="list-style-type: none"> 인벤토리 비용 절감 효과를 	보기, 계획 및 분석
	EC2: 설명	구축	보기, 계획 및 분석
	EC2: DescribeNetworkInterfaces를 참조하십시오	구축	보기, 계획 및 분석
	EC2:DescribeInstanceTypes를 참조하십시오	<ul style="list-style-type: none"> 구축 비용 절감 효과를 	보기, 계획 및 분석
FSx for ONTAP 배포 양식을 작성하는 방법에 대해 자세히 알아보십시오	EC2: 설명	<ul style="list-style-type: none"> 구축 인벤토리 	보기, 계획 및 분석
	EC2: DescribeSubnet	<ul style="list-style-type: none"> 구축 인벤토리 	보기, 계획 및 분석
	EC2: DescribeSecurityGroups	구축	보기, 계획 및 분석
	EC2: DescribeImages(설명 영상)	구축	보기, 계획 및 분석
	EC2: 설명	구축	보기, 계획 및 분석
	EC2: 설명표	<ul style="list-style-type: none"> 구축 인벤토리 	보기, 계획 및 분석
기존 VPC 엔드포인트를 가져와 구축 전에 새 엔드포인트를 생성해야 하는지 여부를 결정합니다	EC2: DescribeVpcEndpoints	<ul style="list-style-type: none"> 구축 인벤토리 	보기, 계획 및 분석

목적	조치	사용된 위치	허가 정책
EC2 인스턴스의 공용 네트워크 연결과 상관없이 필요한 서비스에 VPC 엔드포인트가 없으면 생성합니다	EC2: CreateVpcEndpoint입니다	구축	데이터베이스 호스트 생성
유효성 검사 노드 (t2.micro/t3.micro)에 대해 지역에서 사용할 수 있는 인스턴스 유형 가져오기	EC2: InstanceTypeOfferings를 설명합니다	구축	보기, 계획 및 분석
가격 책정 및 절감 효과를 위해 연결된 각 EBS 볼륨의 스냅샷 세부 정보를 확인합니다	EC2: 설명	비용 절감 효과를	보기, 계획 및 분석
가격 책정 및 절감 예상 비용을 위해 연결된 각 EBS 볼륨의 세부 정보를 봅니다	EC2: 설명 볼륨을 참조하십시오	<ul style="list-style-type: none"> 인벤토리 비용 절감 효과를 	보기, 계획 및 분석
FSx for ONTAP 파일 시스템 암호화에 대한 KMS 키 세부 정보를 확인하십시오	KMS: ListAliases	구축	보기, 계획 및 분석
	KMS: ListKeys	구축	보기, 계획 및 분석
	KMS: 설명키	구축	보기, 계획 및 분석
환경에서 실행 중인 CloudFormation 스택 목록을 확인하여 할당량 제한을 확인합니다	CloudFormation: ListStacks	구축	보기, 계획 및 분석
배포를 트리거하기 전에 리소스에 대한 계정 제한을 확인하십시오	CloudFormation: DescribeAccountLimits 를 참조하십시오	구축	보기, 계획 및 분석
해당 지역에서 AWS에서 관리하는 Active Directory 목록을 가져옵니다	DS:설명 디렉토리	구축	보기, 계획 및 분석

목적	조치	사용된 위치	허가 정책
볼륨, 백업, SVM, AZ의 파일 시스템, FSx for ONTAP 파일 시스템용 태그의 목록과 세부 정보를 확인할 수 있습니다	FSx:볼륨 설명	<ul style="list-style-type: none"> 인벤토리 비용 절감 살펴보기 	보기, 계획 및 분석
	FSX:백업 설명	<ul style="list-style-type: none"> 인벤토리 비용 절감 살펴보기 	보기, 계획 및 분석
	FSX:DescribeStorageVirtualMachines를 참조하십시오	<ul style="list-style-type: none"> 구축 관리 운영 인벤토리 	보기, 계획 및 분석
	FSx:파일 시스템 설명	<ul style="list-style-type: none"> 구축 관리 운영 인벤토리 비용 절감 효과를 	보기, 계획 및 분석
	FSX:ListTagsForResource.를 참조하십시오	관리 운영	보기, 계획 및 분석
CloudFormation 및 VPC에 대한 서비스 할당량 한도 가져오기 / SQL, 도메인 및 FSx for ONTAP 에 제공된 자격 증명에 대한 사용자 계정에서 비밀 만들기	servicequotas:ListServiceQuotas 입니다	구축	보기, 계획 및 분석
SSM 기반 쿼리를 사용하여 ONTAP용 FSx 지원 지역의 업데이트된 목록을 확인하십시오	SSM:GetParametersByPath 입니다	구축	보기, 계획 및 분석
배포 후 관리 작업을 위한 명령을 전송한 후 SSM 응답을 폴링합니다	SSM: GetCommandInvocation 을 참조하십시오	<ul style="list-style-type: none"> 관리 운영 인벤토리 비용 절감 효과를 최적화 	보기, 계획 및 분석
SSM을 통해 EC2 인스턴스에 명령을 보내 검색 및 관리	SSM: SendCommand 를 참조하십시오	<ul style="list-style-type: none"> 관리 운영 인벤토리 비용 절감 효과를 최적화 	보기, 계획 및 분석

목적	조치	사용된 위치	허가 정책
배포 후 인스턴스의 SSM 연결 상태를 가져옵니다	SSM: GetConnectionStatus 를 참조하십시오	<ul style="list-style-type: none"> • 관리 운영 • 인벤토리 • 최적화 	보기, 계획 및 분석
관리되는 EC2 인스턴스 그룹(SQL 노드)에 대한 SSM 연결 상태 가져오기	SSM: DescribeInstanceInformation을 참조하십시오	인벤토리	보기, 계획 및 분석
운영 체제 패치 평가에 사용할 수 있는 패치 기준 목록을 가져옵니다	SSM: PatchBaseline 설명	최적화	보기, 계획 및 분석
운영 체제 패치 평가를 위해 Windows EC2 인스턴스의 패치 상태를 가져옵니다	SSM: InstancePatchStates 설명	최적화	보기, 계획 및 분석
운영 체제 패치 관리를 위해 EC2 인스턴스에서 AWS Patch Manager가 실행한 명령을 나열합니다	SSM: ListCommands 를 참조하십시오	최적화	보기, 계획 및 분석
계정이 AWS Compute Optimizer에 등록되었는지 확인합니다	계산 최적화 프로그램: GetEnrollmentStatus	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성
AWS Compute Optimizer에서 기존 권장 사항 기본 설정을 업데이트하여 SQL Server 워크로드에 대한 제안을 조정합니다	컴퓨팅 최적화 프로그램: 권장 사항 권장 사항 기본 설정	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성
AWS Compute Optimizer에서 특정 리소스에 적용되는 권장 사항 기본 설정을 확인합니다	Compute-Optimizer: GetEffective권장 사항 기본 설정	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성
AWS Compute Optimizer가 Amazon EC2(Amazon Elastic Compute Cloud) 인스턴스에 대해 생성하는 권장 사항을 가져옵니다	컴퓨팅 최적화: GetEC2InstanceRecommendations 를 참조하십시오	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성
자동 크기 조정 그룹에 대한 인스턴스 연결을 확인합니다	자동 크기 조정: AutoScalingGroup 설명	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성
	자동 크기 조정:자동 크기 조정 설명	<ul style="list-style-type: none"> • 비용 절감 효과를 • 최적화 	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
배포 또는 AWS 계정에서 관리되는 AD, FSx for ONTAP 및 SQL 사용자 자격 증명에 대한 SSM 매개 변수를 가져오고 나열하고 생성하고 삭제합니다	SSM: GetParameter(GetParameter	<ul style="list-style-type: none"> • 구축 • 관리 운영 • 인벤토리 	보기, 계획 및 분석
	SSM: GetParameters(GetParameters	<ul style="list-style-type: none"> • 구축 • 관리 운영 • 인벤토리 	보기, 계획 및 분석
	SSM: PutParameter 1	<ul style="list-style-type: none"> • 구축 • 관리 운영 	보기, 계획 및 분석
	SSM: 매개 변수 삭제	<ul style="list-style-type: none"> • 구축 • 관리 운영 	보기, 계획 및 분석
네트워크 리소스를 SQL 노드 및 유효성 검사 노드에 연결하고 SQL 노드에 보조 IP를 추가합니다	EC2: AllocateAddress(주소 1)	구축	데이터베이스 호스트 생성
	EC2: AllocateHosts(호스트 1)	구축	데이터베이스 호스트 생성
	2:1:1:1(주소 지정)	구축	데이터베이스 호스트 생성
	EC2: 연관 주소 1	구축	데이터베이스 호스트 생성
	2:1(2)	구축	데이터베이스 호스트 생성
	EC2: AssociateSubnetCidrBlock(연결	구축	데이터베이스 호스트 생성
	2:1:1:1:1:1:1:1:1:1:1:1:1:1:1	구축	데이터베이스 호스트 생성
	(영어): AttachInternetGateway (영어	구축	데이터베이스 호스트 생성
	(영어) - 어댑터 네트워크 인터페이스 (영어	구축	데이터베이스 호스트 생성
구축을 위해 필요한 EBS 볼륨을 SQL 노드에 연결	EC2: AttachVolume	구축	데이터베이스 호스트 생성
보안 그룹을 연결하고 프로비저닝된 EC2 인스턴스에 규칙을 수정합니다.	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	데이터베이스 호스트 생성
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
구축을 위해 SQL 노드에 필요한 EBS 볼륨을 생성합니다	EC2: CreateVolume	구축	데이터베이스 호스트 생성
t2.micro 유형으로 생성된 임시 유효성 검사 노드를 제거하고 실패한 EC2 SQL 노드의 롤백 또는 재시도를 위해 제거합니다	EC2: DeleteNetworkInterface	구축	데이터베이스 호스트 생성
	EC2: DeleteSecurityGroup	구축	데이터베이스 호스트 생성
	EC2: 삭제 태그	구축	데이터베이스 호스트 생성
	EC2: DeleteVolume(삭제 볼륨)	구축	데이터베이스 호스트 생성
	EC2: 분리 네트워크 인터페이스	구축	데이터베이스 호스트 생성
	EC2: DetachVolume(분리 볼륨)	구축	데이터베이스 호스트 생성
	EC2: 연결 해제 주소	구축	데이터베이스 호스트 생성
	EC2: DiscassociateIamInstanceProfile 을 참조하십시오	구축	데이터베이스 호스트 생성
	EC2: 연결 해제 라우팅 테이블	구축	데이터베이스 호스트 생성
	EC2: 연결 해제 SubnetCidrBlock	구축	데이터베이스 호스트 생성
	EC2: 연결 해제 VpcCidrBlock	구축	데이터베이스 호스트 생성
생성된 SQL 인스턴스의 특성을 수정합니다. WLMDDB로 시작하는 이름에만 적용됩니다.	EC2: ModifyInstanceAttribute	구축	운영 및 개선
	EC2: ModifyInstancePlacement	구축	데이터베이스 호스트 생성
	EC2: ModifyNetworkInterfaceAttribute 입니다	구축	데이터베이스 호스트 생성
	EC2: ModifySubnetAttribute 를 사용합니다	구축	데이터베이스 호스트 생성
	EC2: ModifyVolume(수정 볼륨)	구축	데이터베이스 호스트 생성
	EC2: ModifyVolumeAttribute	구축	데이터베이스 호스트 생성
	EC2: ModifyVpcAttribute 를 사용합니다	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
유효성 검사 인스턴스의 연결을 끊고 제거합니다	EC2: ReleaseAddress(릴리스 주소)	구축	데이터베이스 호스트 생성
	EC2: ReplaceRoute	구축	데이터베이스 호스트 생성
	EC2: ReplaceRouteTableAssociation 을 참조하십시오	구축	데이터베이스 호스트 생성
	EC2: RevokeSecurityGroupEgress	구축	데이터베이스 호스트 생성
	EC2: RevokeSecurityGroupIngress 를 참조하십시오	구축	데이터베이스 호스트 생성
배포된 인스턴스를 시작합니다	EC2: StartInstances(시작 인스턴스)	구축	운영 및 개선
배포된 인스턴스를 중지합니다	EC2: StopInstances(중지 인스턴스)	구축	운영 및 개선
WLMDDB에서 생성한 Amazon FSx for NetApp ONTAP 리소스에 대한 사용자 지정 값에 태그를 지정하여 리소스 관리 중에 청구 세부 정보를 가져옵니다	자유무역협정(FSX)	<ul style="list-style-type: none"> 구축 관리 운영 	데이터베이스 호스트 생성
배포할 CloudFormation 템플릿을 만들고 유효성을 검사합니다	CloudFormation:CreateStack	구축	데이터베이스 호스트 생성
	CloudFormation: DescribeStackEvents	구축	데이터베이스 호스트 생성
	CloudFormation: DescribeStacks	구축	데이터베이스 호스트 생성
	CloudFormation: ListStacks	구축	보기, 계획 및 분석
	CloudFormation:ValidateTemplate 을 참조하십시오	구축	데이터베이스 호스트 생성
재시도 및 롤백을 위해 중첩된 스택 템플릿을 생성합니다	EC2:CreateLaunchTemplate	구축	데이터베이스 호스트 생성
	EC2: CreateLaunchTemplateVersion	구축	데이터베이스 호스트 생성
생성된 인스턴스에서 태그 및 네트워크 보안을 관리합니다	EC2: CreateNetworkInterface입니다	구축	데이터베이스 호스트 생성
	EC2:CreateSecurityGroup입니다	구축	데이터베이스 호스트 생성
	EC2: CreateTags(태그 생성)	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
프로비저닝을 위한 인스턴스 세부 정보를 가져옵니다	ec2:주소 설명	구축	보기, 계획 및 분석
	ec2:DescribeLaunchTemplates	구축	보기, 계획 및 분석
생성된 인스턴스를 시작합니다	EC2: 런인스턴스	구축	데이터베이스 호스트 생성
프로비저닝에 필요한 FSx for ONTAP 리소스를 생성합니다. 기존 FSx for ONTAP 시스템의 경우 SQL 볼륨을 호스팅하는 새로운 SVM이 생성됩니다.	FSX:CreateFileSystem 을 참조하십시오	구축	데이터베이스 호스트 생성
	FSx:CreateStorageVirtualMachine	구축	데이터베이스 호스트 생성
	FSX:CreateVolume 을 참조하십시오	<ul style="list-style-type: none"> 구축 관리 운영 	데이터베이스 호스트 생성
FSx for ONTAP 정보를 확인하십시오	fsx:파일 시스템 별칭 설명	구축	데이터베이스 호스트 생성
파일 시스템 여유 공간을 해결하기 위해 FSx for ONTAP 파일 시스템의 크기를 조정합니다	FSx:UpdateFilesystem입니다	최적화	운영 및 개선
로그 및 TempDB 드라이브 크기를 수정하기 위해 볼륨 크기를 조정합니다	FSX:UpdateVolume을 참조하십시오	최적화	운영 및 개선
KMS 키 세부 정보를 얻고 FSx for ONTAP 암호화를 사용합니다	KMS: CreateGrant	구축	데이터베이스 호스트 생성
	kms:사용자 정의 키 저장소 설명	구축	데이터베이스 호스트 생성
	KMS : GenerateDataKey	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
EC2 인스턴스에서 실행되는 검증 및 프로비저닝 스크립트를 위한 CloudWatch 로그를 생성합니다	로그:CreateLogGroup	구축	데이터베이스 호스트 생성
	로그: CreateLogStream	구축	데이터베이스 호스트 생성
	로그:GetLogGroupFields	구축	데이터베이스 호스트 생성
	로그:GetLogRecord	구축	데이터베이스 호스트 생성
	로그:ListLogDeliveries입니다	구축	데이터베이스 호스트 생성
	로그: PutLogEvents	<ul style="list-style-type: none"> • 구축 • 관리 운영 	데이터베이스 호스트 생성
	로그:TagResource	구축	데이터베이스 호스트 생성
SSM 출력 잘림이 발생하면 Workload Factory가 SQL 인스턴스에 대한 Amazon CloudWatch 로그로 전환됩니다.	로그:GetLogEvents	<ul style="list-style-type: none"> • 스토리지 평가(최적화) • 인벤토리 	보기, 계획 및 분석
Workload Factory가 현재 로그 그룹을 가져오고 Workload Factory에서 생성한 로그 그룹에 대한 보존이 설정되었는지 확인하도록 허용합니다.	로그:DescribeLogGroups	<ul style="list-style-type: none"> • 스토리지 평가(최적화) • 인벤토리 	보기, 계획 및 분석
SSM 명령 출력에 대한 로그 스트림의 불필요한 누적을 방지하기 위해 Workload Factory에서 생성된 로그 그룹에 대해 1일 보존 정책을 설정하도록 Workload Factory에 허용합니다.	로그: PutRetentionPolicy	<ul style="list-style-type: none"> • 스토리지 평가(최적화) • 인벤토리 	보기, 계획 및 분석
고객 SNS 항목을 나열하고 WLMDb 백엔드 SNS 및 고객 SNS에 게시합니다(선택한 경우)	SNS: ListTopics 를 참조하십시오	구축	보기, 계획 및 분석
	SNS: 게시	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
프로비저닝된 SQL 인스턴스에서 검색 스크립트를 실행하고 FSx for ONTAP 지원 AWS 지역의 최신 목록을 가져오려면 SSM 권한이 필요합니다.	SSM: PutComplianceItems 를 참조하십시오	구축	데이터베이스 호스트 생성
	SSM: PutConfigurePackageResult 를 참조하십시오	구축	데이터베이스 호스트 생성
	SSM: 재고 입고	구축	데이터베이스 호스트 생성
	SSM: 업데이트 연결 상태	구축	데이터베이스 호스트 생성
	SSM: UpdateInstanceAssociationStatus 를 참조하십시오	구축	데이터베이스 호스트 생성
	SSM: UpdateInstanceInformation 을 참조하십시오	구축	데이터베이스 호스트 생성
	ssmmessages:CreateControlChannel	구축	데이터베이스 호스트 생성
	ssmmessages:CreateDataChannel	구축	데이터베이스 호스트 생성
	ssmmessages:OpenControlChannel	구축	데이터베이스 호스트 생성
	ssmmessages:오픈데이터채널	구축	데이터베이스 호스트 생성
성공 또는 실패에 대한 신호 CloudFormation 스택.	이 부분의 본문은 서명자입니다	구축	데이터베이스 호스트 생성
템플릿으로 생성된 EC2 역할을 EC2의 인스턴스 프로필에 추가하여 EC2의 스크립트가 배포에 필요한 리소스에 액세스할 수 있도록 합니다.	IAM:AddRoleToInstanceProfile 을 참조하십시오	구축	데이터베이스 호스트 생성
EC2의 인스턴스 프로필을 생성하고 생성된 EC2 역할을 연결합니다.	IAM:CreateInstanceProfile	구축	데이터베이스 호스트 생성
아래에 나열된 권한이 있는 템플릿을 통해 EC2 역할을 생성합니다	IAM: CreateRole	구축	데이터베이스 호스트 생성
EC2 서비스에 연결된 역할을 생성합니다	IAM: CreateServiceLinkedRole (영어)	구축	데이터베이스 호스트 생성
특히 검증 노드에 대해 구축 중에 생성된 인스턴스 프로필을 삭제합니다	IAM: DeleteInstanceProfile	구축	데이터베이스 호스트 생성

목적	조치	사용된 위치	허가 정책
역할 및 정책 세부 정보를 확인하여 사용 권한의 공백을 확인하고 배포를 검증합니다	IAM: GetPolicy 를 참조하십시오	구축	데이터베이스 호스트 생성
	IAM: GetPolicyVersion 을 참조하십시오	구축	데이터베이스 호스트 생성
	IAM:GetRole	구축	데이터베이스 호스트 생성
	IAM: GetRolePolicy 를 참조하십시오	구축	데이터베이스 호스트 생성
	IAM: GetUser	구축	데이터베이스 호스트 생성
생성된 역할을 EC2 인스턴스로 전달합니다	IAM: 패스역할 3	구축	데이터베이스 호스트 생성
생성된 EC2 역할에 필요한 권한이 있는 정책을 추가합니다	IAM: PutRolePolicy(입수 정책)	구축	데이터베이스 호스트 생성
프로비저닝된 EC2 인스턴스 프로필에서 역할을 분리합니다	IAM:RemoveRoleFromInstanceProfile 을 참조하십시오	구축	데이터베이스 호스트 생성
워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축	모두
오류 로그 분석에 사용할 수 있는 기초 모델을 얻으세요	Bedrock: GetFoundationModelAvailability를 참조하십시오	오류 로그 분석	보기, 계획 및 분석
오류 로그 분석을 위해 Amazon Bedrock에서 사용 가능한 인터페이스 프로필을 나열합니다.	Bedrock: ListInferenceProfiles 를 참조하십시오	오류 로그 분석	보기, 계획 및 분석

1. 권한이 WLMDB로 시작하는 리소스로 제한됩니다.
2. "IAM:CreateServiceLinkedRole" 제한:"ec2.amazonaws.com"*
3. "IAM:PassRole"이 "IAM:PassedToService":"ec2.amazonaws.com"* 으로 제한됩니다

GenAI 워크로드에 대한 권한

VMware 워크로드에 대한 IAM 정책은 VMware용 Workload Factory가 사용자의 운영 모드에 따라 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다.

GenAI IAM 정책은 읽기/쓰기 권한으로만 사용할 수 있습니다.

- 읽기/쓰기: 할당된 자격 증명을 사용하여 실행에 필요하고 검증된 권한을 가진 AWS에서 작업을 실행하고 자동화합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",

```

```

        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
    ],
    "Resource": "*"
},
{
    "Sid": "IAMGroup",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "IAMGroup2",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "FSXNGroup",
    "Effect": "Allow",
    "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
    ],
    "Resource": "*"
},
{
    "Sid": "FSXNGroup2",
    "Effect": "Allow",
    "Action": [

```

```

        "fsx:UntagResource",
        "fsx:TagResource"
    ],
    "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    ]
},
{
    "Sid": "SSMParameterStore",
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
    ],
    "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
},
{
    "Sid": "SSM",
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
    ],
    "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
},
{
    "Sid": "SSMMessages",
    "Effect": "Allow",
    "Action": [
        "ssm:GetCommandInvocation"
    ],
    "Resource": "*"
},
{
    "Sid": "SSMCommandDocument",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
    ]
},
{
    "Sid": "SSMCommandInstance",

```



```

"Effect": "Allow",
"Action": [
    "ssm:SendCommand",
    "ssm:GetConnectionStatus"
],
"Resource": [
    "arn:aws:ec2:*:*:instance/*"
],
"Condition": {
    "StringLike": {
        "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
    }
}
},
{
    "Sid": "KMS",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "*"
},
{
    "Sid": "SNS",
    "Effect": "Allow",
    "Action": [
        "sns:Publish"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatch",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatchAiEngine",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",

```

```

        "logs:DescribeLogStreams"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
},
{
    "Sid": "CloudWatchAiEngineLogStream",
    "Effect": "Allow",
    "Action": [
        "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
},
{
    "Sid": "BedrockGroup",
    "Effect": "Allow",
    "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatchBedrock",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
},
{
    "Sid": "BedrockLoggingAttachRole",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam:*:*:role/NetApp_AI_Bedrock*"
},
{

```

```

    "Sid": "BedrockLoggingIamOperations",
    "Effect": "Allow",
    "Action": [
        "iam:CreatePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "QBusiness",
    "Effect": "Allow",
    "Action": [
        "qbusiness:ListApplications"
    ],
    "Resource": "*"
},
{
    "Sid": "S3",
    "Effect": "Allow",
    "Action": [
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource": "*"
}
]
}

```

다음 표에는 GenAI 워크로드에 대한 사용 권한에 대한 세부 정보가 나와 있습니다.

목적	조치	사용된 위치	허가 정책
구축 및 리빌드 작업 중에 AI 엔진 CloudFormation 스택을 생성합니다	CloudFormation:CreateStack	구축	읽기/쓰기
AI 엔진 CloudFormation 스택을 생성합니다	CloudFormation: DescribeStacks	구축	읽기/쓰기
AI 엔진 배포 마법사의 지역을 나열합니다	EC2: 설명	구축	읽기/쓰기
AI 엔진 태그를 표시합니다	EC2: DescribeTags(설명 태그)	구축	읽기/쓰기
S3 버킷 나열	S3:ListAllMyBucket	구축	읽기/쓰기
AI 엔진 스택 생성 전에 VPC 엔드포인트 나열	EC2: CreateVpcEndpoint입니다	구축	읽기/쓰기
배포 및 리빌드 중에 AI 엔진 스택 생성 중에 AI 엔진 보안 그룹을 생성합니다	EC2:CreateSecurityGroup입니다	구축	읽기/쓰기
구축 및 리빌드 작업 중 AI 엔진 스택 생성에서 생성된 리소스에 태그를 지정합니다	EC2: CreateTags(태그 생성)	구축	읽기/쓰기
AI 엔진 스택에서 WLMAI 백엔드에 암호화된 이벤트를 게시합니다	KMS : GenerateDataKey	구축	읽기/쓰기
	KMS: 암호 해독	구축	읽기/쓰기
ai-engine 스택에서 WLMAI 백엔드에 이벤트 및 사용자 지정 리소스를 게시합니다	SNS: 게시	구축	읽기/쓰기
AI 엔진 배포 마법사 중 vPC 나열	EC2: 설명	구축	읽기/쓰기
ai-engine 배포 마법사에서 서브넷을 나열합니다	EC2: DescribeSubnet	구축	읽기/쓰기
AI 엔진 구축 및 리빌드 중에 라우팅 테이블을 가져옵니다	EC2: 설명표	구축	읽기/쓰기
AI 엔진 배포 마법사에서 제공하는 키 쌍을 나열합니다	EC2: 설명	구축	읽기/쓰기
AI 엔진 스택 생성 시 보안 그룹 나열(프라이빗 엔드포인트에서 보안 그룹 찾기)	EC2: DescribeSecurityGroups	구축	읽기/쓰기
AI 엔진을 구축하는 동안 VPC 엔드포인트를 생성할 필요가 있는지 결정합니다	EC2: DescribeVpcEndpoints	구축	읽기/쓰기
Amazon Q Business 응용 프로그램을 나열합니다	qbusiness: ListApplications를 참조하십시오	구축	읽기/쓰기
AI 엔진 상태를 확인할 인스턴스를 나열합니다	EC2: DescribeInstances(지시 인스턴스)	문제 해결	읽기/쓰기

목적	조치	사용된 위치	허가 정책
구축 및 리빌드 작업 중에 AI 엔진 스택을 생성하는 동안 이미지를 나열합니다	EC2: DescribeImages(설명 영상)	구축	읽기/쓰기
구축 및 리빌드 작업 중에 AI 인스턴스 스택 생성 중에 AI 인스턴스 및 프라이빗 엔드포인트 보안 그룹을 생성하고 업데이트합니다	EC2: RevokeSecurityGroupEgress	구축	읽기/쓰기
	EC2: RevokeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
배포 및 리빌드 작업 중에 CloudFormation 스택을 생성하는 동안 AI 엔진을 실행합니다	EC2: 런인스턴스	구축	읽기/쓰기
배포 및 리빌드 작업 중에 스택 생성 중에 보안 그룹을 연결하고 AI 엔진에 대한 규칙을 수정합니다	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	읽기/쓰기
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
기초 모델 중 하나에 대한 채팅 요청을 시작합니다	Bedrock: InvokeModelWithResponseStream 을 호출합니다	구축	읽기/쓰기
기초 모델에 대한 채팅/포함 요청을 시작합니다	Bedrock: InvokeModel 을 참조하십시오	구축	읽기/쓰기
지역에서 사용 가능한 기반 모델을 표시합니다	Bedrock: ListFoundationModels를 참조하십시오	구축	읽기/쓰기
기반 모델에 대한 정보 확인	Bedrock: GetFoundationModel 을 참조하십시오	구축	읽기/쓰기
기초 모델에 대한 액세스 권한을 확인합니다	Bedrock: GetFoundationModelAvailability를 참조하십시오	구축	읽기/쓰기
배포 및 재구축 작업 중에 Amazon CloudWatch 로그 그룹을 생성해야 하는지 확인합니다	로그:DescribeLogGroups	구축	읽기/쓰기
AI 엔진 마법사에서 FSx 및 Amazon Bedrock을 지원하는 영역을 확보할 수 있습니다	SSM:GetParametersByPath 입니다	구축	읽기/쓰기
구축 및 리빌드 작업 중에 AI 엔진 구축에 필요한 최신 Amazon Linux 이미지를 확인할 수 있습니다	SSM:GetParameters 를 참조하십시오	구축	읽기/쓰기
AI 엔진으로 전송된 명령에서 SSM 응답을 가져옵니다	SSM: GetCommandInvocation 을 참조하십시오	구축	읽기/쓰기
AI 엔진에 대한 SSM 연결을 점검하십시오	SSM: SendCommand 를 참조하십시오	구축	읽기/쓰기
	SSM: GetConnectionStatus 를 참조하십시오	구축	읽기/쓰기

목적	조치	사용된 위치	허가 정책
구축 및 리빌드 작업 중에 스택 생성 중에 AI 엔진 인스턴스 프로필을 생성할 수 있습니다	IAM: CreateRole	구축	읽기/쓰기
	IAM:CreateInstanceProfile	구축	읽기/쓰기
	IAM:AddRoleToInstanceProfile 을 참조하십시오	구축	읽기/쓰기
	IAM: PutRolePolicy(입수 정책)	구축	읽기/쓰기
	IAM: GetRolePolicy 를 참조하십시오	구축	읽기/쓰기
	IAM:GetRole	구축	읽기/쓰기
	IAM: 태그 역할	구축	읽기/쓰기
	IAM: 암호 역할	구축	읽기/쓰기
워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축	읽기/쓰기
"기술 자료 생성" 마법사에서 FSx for ONTAP 파일 시스템을 나열합니다	FSx:볼륨 설명	기술 자료 작성	읽기/쓰기
"기술 자료 생성" 마법사 중에 FSx for ONTAP 파일 시스템 볼륨을 나열합니다	FSx:파일 시스템 설명	기술 자료 작성	읽기/쓰기
리빌드 작업 중에 AI 엔진에 대한 지식 기반을 관리합니다	FSX:ListTagsForResource.를 참조하십시오	문제 해결	읽기/쓰기
"기술 자료 생성" 마법사에서 FSx for ONTAP 파일 시스템 스토리지 가상 머신 나열	FSX:DescribeStorageVirtualMachines를 참조하십시오	구축	읽기/쓰기
지식 베이스를 새 인스턴스로 이동합니다	FSx:UntagResource	문제 해결	읽기/쓰기
리빌드 중 AI 엔진에 대한 지식 기반을 관리합니다	FSX:태그 리소스	문제 해결	읽기/쓰기
SSM 비밀(ECR 토큰, CIFS 자격 증명, 테넌시 서비스 계정 키)을 안전한 방식으로 저장합니다	SSM:GetParameter입니다	구축	읽기/쓰기
	SSM: PutParameter	구축	읽기/쓰기
배포 및 재구축 작업 중에 AI 엔진 로그를 Amazon CloudWatch 로그 그룹으로 보냅니다	로그:CreateLogGroup	구축	읽기/쓰기
	로그: PutRetentionPolicy	구축	읽기/쓰기
AI 엔진 로그를 Amazon CloudWatch 로그 그룹으로 보냅니다	로그:TagResource	문제 해결	읽기/쓰기
Amazon CloudWatch에서 SSM 응답 받기(응답이 너무 긴 경우)	로그:DescribeLogStreams	문제 해결	읽기/쓰기
Amazon CloudWatch에서 SSM 응답을 받으십시오	로그:GetLogEvents	문제 해결	읽기/쓰기

목적	조치	사용된 위치	허가 정책
배포 및 재구축 작업 중에 스택 생성 중에 Amazon Bedrock 로그에 대한 Amazon CloudWatch 로그 그룹을 생성합니다	로그:CreateLogGroup	구축	읽기/쓰기
	로그: PutRetentionPolicy	구축	읽기/쓰기
	로그:TagResource	구축	읽기/쓰기
모델에 대한 추론 프로파일을 나열합니다	Bedrock: ListInferenceProfiles 를 참조하십시오	문제 해결	읽기/쓰기

VMware 워크로드에 대한 권한

VMware 워크로드에는 다음과 같은 권한 정책이 선택 가능합니다.

- 보기, 계획 및 분석: EVS 가상화 환경 인벤토리를 보고, 시스템에 대한 잘 설계된 분석을 얻고, 절감 방안을 알아보세요.
- 데이터 저장소 배포 및 연결: 권장되는 VM 레이아웃을 AWS vSphere 클러스터의 Amazon EVS, Amazon EC2 또는 VMware Cloud에 배포하고 사용자 지정 Amazon FSx for NetApp ONTAP 파일 시스템을 외부 데이터 저장소로 사용합니다.

필요한 IAM 정책을 보려면 권한 정책을 선택하세요.



보기, 계획 및 분석

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "secretsmanager:ListSecrets",
        "evs:ListEnvironments",
        "evs:GetEnvironment",
        "evs:ListEnvironmentVlans"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

데이터 저장소 배포 및 연결

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

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}

```

다음 표에는 VMware 작업 부하에 대한 사용 권한에 대한 세부 정보가 나와 있습니다.

목적	조치	사용된 위치	허가 정책
보안 그룹을 연결하고 프로비저닝된 노드에 대한 규칙을 수정합니다	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	데이터 저장소 배포 및 연결
EBS 볼륨을 생성합니다	FSX:CreateVolume 을 참조하십시오	구축	데이터 저장소 배포 및 연결
VMware 워크로드에서 생성한 FSx for NetApp ONTAP 리소스에 대한 사용자 지정 값에 태그를 지정합니다	FSX:태그 리소스	구축	데이터 저장소 배포 및 연결
CloudFormation 템플릿을 만들고 유효성을 검사합니다	CloudFormation:CreateStack	구축	데이터 저장소 배포 및 연결
생성된 인스턴스에서 태그 및 네트워크 보안을 관리합니다	EC2:CreateSecurityGroup입니다	구축	데이터 저장소 배포 및 연결
생성된 인스턴스를 시작합니다	EC2: 런인스턴스	구축	데이터 저장소 배포 및 연결
EC2 인스턴스 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	인벤토리	데이터 저장소 배포 및 연결
배포 및 재구축 작업 중에 스택을 생성하는 동안 이미지를 나열합니다	EC2: DescribeImages(설명 영상)	인벤토리	데이터 저장소 배포 및 연결
VPC와 연결된 DHCP 옵션 세트의 구성 세부 정보 보기	ec2:Dhcp옵션 설명	인벤토리	보기, 계획 및 분석
선택한 환경에서 VPC를 가져와 배포 양식을 작성합니다	EC2: 설명	<ul style="list-style-type: none"> • 구축 • 인벤토리 	보기, 계획 및 분석
선택한 환경에서 서브넷을 가져와 배포 양식을 완성합니다	EC2: DescribeSubnet	<ul style="list-style-type: none"> • 구축 • 인벤토리 	보기, 계획 및 분석
선택한 환경의 보안 그룹을 가져와 배포 양식을 작성합니다	EC2: DescribeSecurityGroups	구축	보기, 계획 및 분석
선택한 환경에서 가용 영역을 가져옵니다	EC2:가용성 영역 설명	<ul style="list-style-type: none"> • 구축 • 인벤토리 	보기, 계획 및 분석
Amazon FSx for NetApp ONTAP 지원으로 지역을 확인하십시오	EC2: 설명	구축	보기, 계획 및 분석
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키 별칭을 가져옵니다	KMS: ListAliases	구축	보기, 계획 및 분석
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키를 가져옵니다	KMS: ListKeys	구축	보기, 계획 및 분석

목적	조치	사용된 위치	허가 정책
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키 만료 세부 정보를 가져옵니다	KMS: 설명키	구축	보기, 계획 및 분석
AWS Secrets Manager에서 비밀 나열	secretsmanager:ListSecrets	인벤토리	보기, 계획 및 분석
Amazon EVS에서 환경 목록 가져오기	evs:환경 목록	인벤토리	보기, 계획 및 분석
특정 Amazon EVS 환경에 대한 자세한 정보를 얻으세요	evs:환경 가져오기	인벤토리	보기, 계획 및 분석
Amazon EVS 환경과 연결된 VLAN 나열	evs:ListEnvironmentVlans	인벤토리	보기, 계획 및 분석
프로비저닝에 필요한 Amazon FSx for NetApp ONTAP 리소스를 생성합니다	FSX:CreateFileSystem 을 참조하십시오	구축	데이터 저장소 배포 및 연결
	FSx:CreateStorageVirtualMachine	구축	데이터 저장소 배포 및 연결
	FSX:CreateVolume 을 참조하십시오	<ul style="list-style-type: none"> 구축 관리 운영 	데이터 저장소 배포 및 연결
NetApp ONTAP용 Amazon FSx에 대해 자세히 알아보십시오	FSX: 설명 *	<ul style="list-style-type: none"> 구축 인벤토리 관리 운영 비용 절감 효과를 	데이터 저장소 배포 및 연결
KMS 키 세부 정보를 확인하고 Amazon FSx for NetApp ONTAP 암호화에 사용합니다	KMS: CreateGrant	구축	데이터 저장소 배포 및 연결
	KMS: 설명 *	구축	보기, 계획 및 분석
	KMS: 목록 *	구축	보기, 계획 및 분석
	KMS: 암호 해독	구축	데이터 저장소 배포 및 연결
	KMS : GenerateDataKey	구축	데이터 저장소 배포 및 연결
고객 SNS 항목을 나열하고 WLMVMC 백엔드 SNS 및 고객 SNS에 게시합니다(선택한 경우)	SNS: 게시	구축	데이터 저장소 배포 및 연결

목적	조치	사용된 위치	허가 정책
워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축	<ul style="list-style-type: none"> 데이터 저장소 배포 및 연결 보기, 계획 및 분석

변경 로그

권한이 추가되고 제거됨에 따라 아래 섹션에 해당 권한이 표시됩니다.

2025년 2월 1일

다음 권한이 저장소 워크로드에 추가되었습니다.

- s3:TagResource
- s3:ListTagsForResource
- s3:UntagResource
- s3tables:CreateTableBucket
- s3tables:ListTables
- s3tables:GetTable
- s3tables:GetTableMetadataLocation
- s3tables:CreateTable
- s3tables:GetNamespace
- s3tables:PutTableData
- s3tables:CreateNamespace
- s3tables:GetTableData
- s3tables:ListNamespaces
- s3tables:ListTableBuckets
- s3tables:GetTableBucket
- s3tables:UpdateTableMetadataLocation
- s3tables:ListTagsForResource
- s3tables:TagResource
- s3:GetObjectTagging
- s3:ListBucket

2025년 12월 4일

다음 권한이 저장소 워크로드에 추가되었습니다.

- `fsx:CreateAndAttachS3AccessPoint`
- `fsx:DetachAndDeleteS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3>DeleteAccessPoint`

2025년 11월 27일

다음 권한이 저장소 워크로드에 추가되었습니다.

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2025년 11월 2일

저장소, 데이터베이스 워크로드, VMware 워크로드에서 "읽기 전용" 및 "읽기/쓰기" 권한 정책이 대체되어 권한을 할당하는 데 있어 더 세부적이고 유연한 방식이 제공되었습니다.

2025년 10월 5일

다음 권한은 GenAI에서 제거되었으며 이제 GenAI 엔진에서 처리됩니다.

- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

2025년 6월 29일

다음 권한은 이제 데이터베이스에 대한 읽기 전용 모드에서 사용 가능합니다. `cloudwatch:GetMetricData`.

2025년 6월 3일

다음 권한은 이제 GenAI의 읽기/쓰기 모드에서 사용할 수 있습니다. `s3:ListAllMyBuckets`.

2025년 5월 4일

다음 권한은 이제 GenAI의 읽기/쓰기 모드에서 사용할 수 있습니다. `qbusiness:ListApplications`.

이제 데이터베이스에 대해 읽기 전용 모드에서 다음 권한을 사용할 수 있습니다.

- logs:GetLogEvents
- logs:DescribeLogGroups

다음 권한은 이제 데이터베이스에 대한 읽기/쓰기 모드에서 사용 가능합니다.
logs:PutRetentionPolicy.

2025년 4월 2일

다음 권한은 이제 데이터베이스에 대한 읽기 전용 모드에서 사용 가능합니다.
ssm:DescribeInstanceInformation.

2025년 3월 30일

GenAI 워크로드 권한이 업데이트됩니다

이제 GenAI의 _읽기/쓰기 모드_에서 다음 권한을 사용할 수 있습니다.

- bedrock:PutModelInvocationLoggingConfiguration
- iam:AttachRolePolicy
- iam:PassRole
- iam:createPolicy
- bedrock:ListInferenceProfiles

GenAI의 _읽기/쓰기 모드_에서 다음 권한이 제거되었습니다. Bedrock:GetFoundationModel.

IAM: SimulatePrincipalPolicy 권한 업데이트

그만큼 iam:SimulatePrincipalPolicy Workload Factory 콘솔에서 추가 AWS 계정 자격 증명을 추가하거나 새로운 워크로드 기능을 추가할 때 자동 권한 확인을 활성화하는 경우 권한은 모든 워크로드 권한 정책의 일부입니다. 이 권한은 워크로드 작업을 시뮬레이션하고 Workload Factory에서 리소스를 배포하기 전에 필요한 AWS 계정 권한이 있는지 확인합니다. 이 검사를 활성화하면 실패한 작업으로 인해 발생한 리소스를 정리하고 누락된 권한을 추가하는 데 필요한 시간과 노력이 줄어듭니다.

2025년 3월 2일

다음 권한은 이제 GenAI의 읽기/쓰기 모드에서 사용할 수 있습니다. bedrock:GetFoundationModel.

2025년 2월 3일

다음 권한은 이제 데이터베이스에 대한 읽기 전용 모드에서 사용 가능합니다. iam:SimulatePrincipalPolicy.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.