NetApp Workload Factory 설정 및 관리 문서

Setup and administration

NetApp
October 06, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/workload-setup-admin/index.html on October 06, 2025. Always check docs.netapp.com for the latest.

목차

NetApp Workload Factory 설정 및 관리 문서 . . . 1
릴리스 정보 . . . 2
NetApp Workload Factory 관리 기능의 새로운 기능 . . . 2
2025년 10월 6일 . . . 2
2025년 10월 5일 . . . 2
2025년 6월 29일 . . . 2
2025년 5월 4일 . . . 2
2025년 3월 30일 . . . 3
2025년 2월 2일 . . . 3
2025년 1월 22일 . . . 3
2025년 1월 5일 . . . 4
2024년 11월 11일 . . . 4
2024년 9월 1일 . . . 4
2024년 8월 4일 . . . 5
2024년 7월 7일 . . . 5
시작하십시오 . . . 6
기본 사항 학습 . . . 6
NetApp Workload Factory에 대해 알아보세요 . . . 6
운영 모드 및 AWS 자격 증명에 대해 자세히 알아보십시오 . . . 10
콘솔 환경 . . . 14
NetApp Workload Factory에 대한 권한 . . . 14
NetApp Workload Factory 빠른 시작 . . . 63
NetApp Workload Factory에 가입하세요 . . . 64
Workload Factory에 AWS 자격 증명 추가 . . . 66
개요 . . . 66
계정에 자격 증명을 수동으로 추가합니다 . . . 66
CloudFormation을 사용하여 계정에 자격 증명을 추가합니다 . . . 69
NetApp Workload Factory로 워크로드 최적화 . . . 72
워크로드 팩토리 관리 . . . 73
NetApp Workload Factory에 로그인하세요 . . . 73
서비스 계정을 관리합니다 . . . 73
서비스 계정을 생성합니다 . . . 74
서비스 계정을 삭제합니다 . . . 75
NetApp Workload Factory 알림 구성 . . . 75
알림 유형 및 메시지 . . . 75
Workload Factory 알림 구성 . . . 77
Amazon SNS 주제 구독하기 . . . 78
알림을 필터링합니다 . . . 78
코드박스를 사용하여 작업을 자동화합니다 . . . 80

코드박스 자동화에 대해 알아보십시오 . . . 80
NetApp Workload Factory에서 자동화를 위해 Codebox 사용 . . . 81
NetApp Workload Factory에서 CloudShell 사용 . . . 84
이 작업에 대해 . . . 84
CloudShell 명령 . . . 85
시작하기 전에 . . . 86
CloudShell 구축 . . . 86
CloudShell 세션 탭의 이름을 변경합니다 . . . 88
중복된 CloudShell 세션 탭 . . . 88
CloudShell 세션 탭을 닫습니다 . . . 89
CloudShell 세션 탭을 분할합니다 . . . 89
CloudShell 세션에 대한 설정을 업데이트합니다 . . . 89
NetApp Workload Factory에서 자격 증명 제거 . . . 90
지식 및 지원 . . . 91
지원을 위해 등록하십시오 . . . 91
지원 등록 개요 . . . 91
NetApp 지원에 계정을 등록합니다 . . . 91
도움을 받으십시오 . . . 93
FSx for ONTAP에 대한 지원을 받으십시오 . . . 93
자체 지원 옵션을 사용합니다 . . . 93
NetApp Support로 케이스 생성 . . . 93
지원 사례 관리(Preview) . . . 96
NetApp Workload Factory에 대한 법적 고지 사항 . . . 99
저작권 . . . 99
상표 . . . 99
특허 . . . 99
개인 정보 보호 정책 . . . 99
오픈 소스 . . . 99

NetApp Workload Factory 설정 및 관리 문서

릴리스 정보

NetApp Workload Factory 관리 기능의 새로운 기능

Workload Factory 관리 기능의 새로운 기능에 대해 알아보세요: 클라우드 공급자 자격 증명, Codebox 개선 사항 등.

2025년 10월 6일

BlueXP workload factory NetApp 워크로드 팩토리로 변경되었습니다**.**

BlueXP 데이터 인프라 관리에 있어서의 역할을 더 잘 반영하도록 이름이 바뀌고 재설계되었습니다. 결과적으로 BlueXP workload factory NetApp 워크로드 팩토리로 이름이 변경되었습니다.

MCP와 **Ask Me** 통합

Workload Factory의 AI 어시스턴트인 Ask Me는 MCP(Model Context Protocol)와 통합되어 있습니다. Ask Me는 MCP를 사용하여 외부 환경과 안전하게 인터페이스하고 API 도구를 쿼리하여 특정 스토리지 환경에 맞춤형 응답을 제공합니다.

2025년 10월 5일

저장소에 대한 새로운 알림

NetApp Workload Factory 알림 서비스에는 스토리지에 대한 잘 설계된 문제에 대한 알림이 포함되어 있습니다.

"NetApp Workload Factory에 대한 알림"

2025년 6월 29일

데이터베이스에 대한 사용 권한 업데이트

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

"권한 참조 변경 로그"

BlueXP 워크로드 팩토리 알림 서비스 지원

BlueXP 워크로드 팩토리 알림 서비스를 사용하면 워크로드 팩토리가 BlueXP 알림 서비스 또는 Amazon SNS 주제로 알림을 전송할 수 있습니다. BlueXP 알림으로 전송된 알림은 BlueXP 알림 패널에 표시됩니다. 워크로드 팩토리가 Amazon SNS 주제에 알림을 게시하면 해당 주제 구독자(예: 사용자 또는 다른 애플리케이션)는 해당 주제에 대해 구성된 엔드포인트(예: 이메일 또는 SMS 메시지)에서 알림을 수신합니다.

"BlueXP 워크로드 팩토리 알림 구성"

2025년 5월 4일

CloudShell 자동 지원

BlueXP 워크로드 팩토리 CloudShell을 사용하는 경우 명령 입력을 시작하고 Tab 키를 눌러 사용 가능한 옵션을 볼 수 있습니다. 가능성이 여러 개인 경우 CLI에 제안 목록이 표시됩니다. 이 기능은 오류를 최소화하고 명령 실행 속도를 높여 생산성을 향상시킵니다.

사용 권한 용어가 업데이트되었습니다

워크로드 팩토리 사용자 인터페이스와 문서에서는 이제 읽기 권한을 나타내는 데 "읽기 전용"을 사용하고 자동화 권한을 나타내는 데 "읽기/쓰기"를 사용합니다.

2025년 3월 30일

CloudShell은 **ONTAP CLI** 명령에 대한 **AI**에서 생성된 오류 응답을 보고합니다

CloudShell을 사용할 경우 ONTAP CLI 명령을 실행하고 오류가 발생할 때마다 실패 설명, 장애 원인, 상세한 해결 방법 등을 통해 AI에서 생성된 오류에 대한 응답을 받을 수 있습니다.

"CloudShell을 사용합니다"

IAM: SimulatePermissionPolicy 권한 업데이트

이제 AWS 계정 자격 증명을 추가하거나 GenAI 워크로드와 같은 새로운 워크로드 기능을 추가할 때 워크로드 팩토리 콘솔에서 권한을 관리할 수 있습니다 `iam:SimulatePrincipalPolicy`.

"권한 참조 변경 로그"

2025년 2월 2일

BlueXP 워크로드 공장 콘솔에서 사용할 수 있는 **CloudShell**

CloudShell은 BlueXP 워크로드 공장 콘솔의 모든 곳에서 사용할 수 있습니다. CloudShell을 사용하면 BlueXP 계정에 제공한 AWS 및 ONTAP 자격 증명을 사용하고 셸 유사 환경에서 AWS CLI 명령 또는 ONTAP CLI 명령을 실행할 수 있습니다.

"CloudShell을 사용합니다"

데이터베이스에 대한 사용 권한 업데이트

이제 데이터베이스에 대해 _READ_MODE에서 다음 권한을 사용할 수 `iam:SimulatePrincipalPolicy` 있습니다.

"권한 참조 변경 로그"

2025년 1월 22일

BlueXP 워크로드 팩토리 권한

이제 BlueXP 워크로드 팩토리에서 스토리지 환경 검색부터 스토리지 또는 GenAI 워크로드에 대한 기술 자료 등의 AWS 리소스 구축에 이르기까지 다양한 작업을 실행하는 데 사용하는 권한을 확인할 수 있습니다. 스토리지, 데이터베이스, VMware 및 GenAI 워크로드에 대한 IAM 정책 및 권한을 볼 수 있습니다.

"BlueXP 워크로드 팩토리 권한"

2025년 1월 5일

BlueXP 워크로드 팩토리에서 서비스 계정 지원

이제 서비스 계정이 BlueXP 워크로드 팩토리에서 지원됩니다. 서비스 계정을 생성하여 인프라 운영을 자동화할 수 있습니다.

"서비스 계정 생성 및 관리"

2024년 11월 11일

BlueXP 콘솔에 워크로드 팩토리 통합

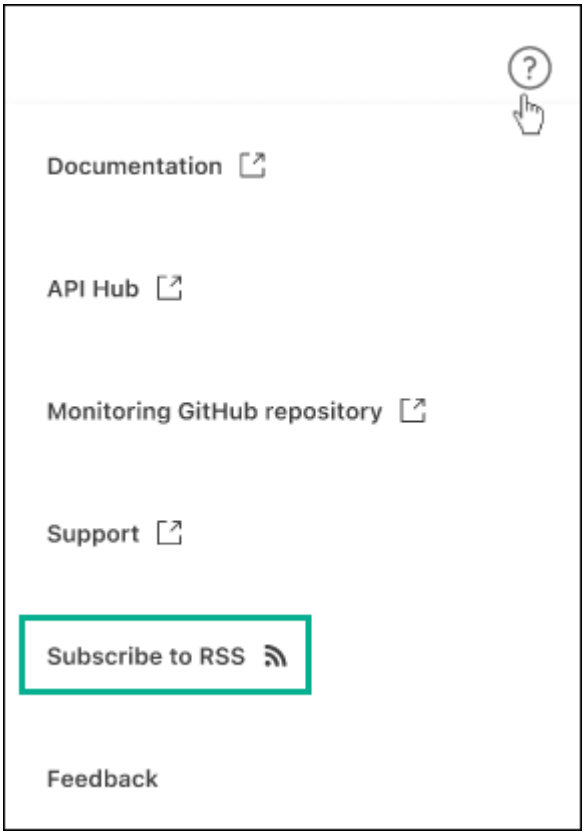
이제 에서 워크로드 팩토리를 사용할 수 "BlueXP 콘솔"있습니다. BlueXP 콘솔 환경은 워크로드 팩토리 콘솔과 동일한 기능을 제공합니다.

"BlueXP 콘솔에서 워크로드 팩토리에 액세스하는 방법을 알아보십시오"

2024년 9월 1일

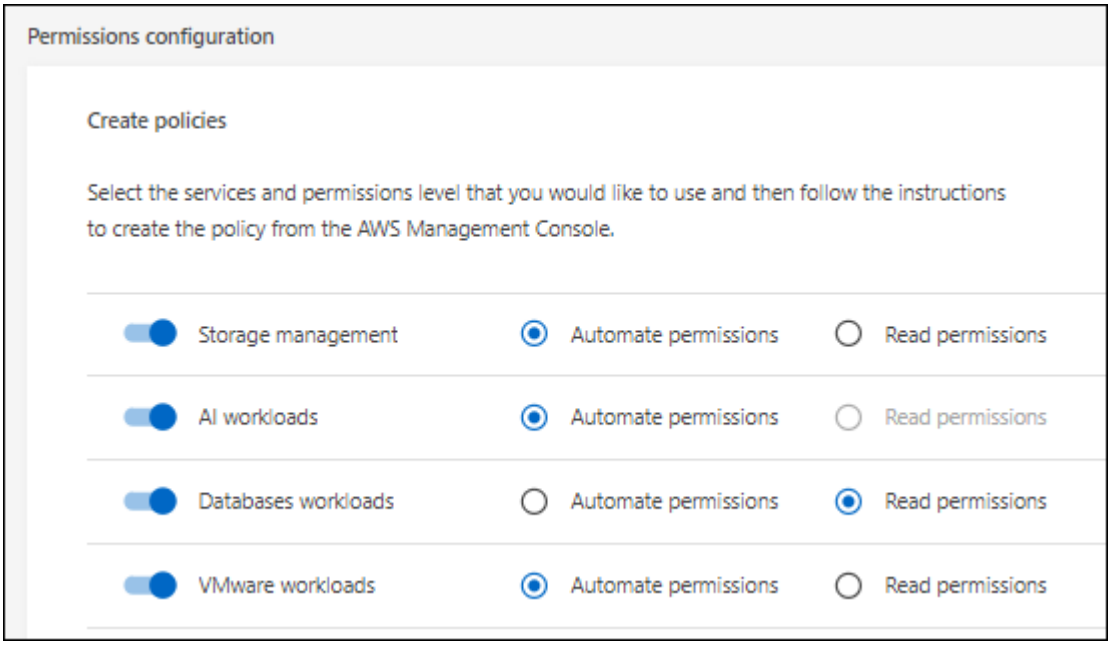
RSS 구독

RSS 구독은 에서 사용할 수 "워크로드 팩토리 콘솔"있습니다. RSS 피드를 사용하면 BlueXP 워크로드 팩토리에서의 변경 사항을 쉽게 확인하고 인식할 수 있습니다.



워크로드당 단일 권한 정책 지원

워크로드 팩토리에서 AWS 자격 증명을 추가할 때 이제 각 워크로드 및 스토리지 관리에 대해 읽기 또는 자동화 모드를 포함한 단일 권한 정책을 선택할 수 있습니다.



"워크로드 팩토리에 AWS 자격 증명을 추가합니다"

2024년 8월 4일

Terraform 지원

Terraform은 Amazon FSx for NetApp ONTAP 파일 시스템 배포 및 스토리지 VM 생성에 지원됩니다. 이제 설정 및 관리 가이드에는 코드박스에서 Terraform을 사용하는 방법에 대한 지침이 나와 있습니다.

"코드박스에서 Terraform을 사용합니다"

2024년 7월 7일

BlueXP 워크로드 공장 초기 릴리즈

BlueXP 워크로드 팩토리는 Amazon FSx for NetApp ONTAP 파일 시스템을 사용하여 워크로드를 최적화하도록 설계된 강력한 라이프사이클 관리 플랫폼입니다. 워크로드 팩토리 및 FSx for ONTAP를 사용하여 능률적으로 처리할 수 있는 워크로드에는 데이터베이스, AWS 기반 VMware Cloud로의 VMware 마이그레이션, AI 챗봇 등이 있습니다.

시작하십시오

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.

워크로드는 비즈니스 목표를 달성하기 위해 설계된 리소스, 코드, 서비스 또는 애플리케이션의 조합을 포함합니다. 이는 고객 대상 애플리케이션부터 백엔드 프로세스까지 모든 것이 될 수 있습니다. 워크로드는 단일 AWS 계정 내의 리소스 서브셋과 관련되거나 여러 계정에 분산될 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 **AWS**의 **VMware Cloud**로 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 NetApp 의 최우선 순위입니다. Workload Factory의 모든 워크로드는 Amazon FSx for NetApp ONTAP 에서 실행됩니다. 모든 것 외에도"AWS 보안 기능" , NetApp Workload Factory가 수신되었습니다."SOC2 유형 1 준수" .

NetApp Workload Factory Amazon FSx for NetApp ONTAP 는"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.

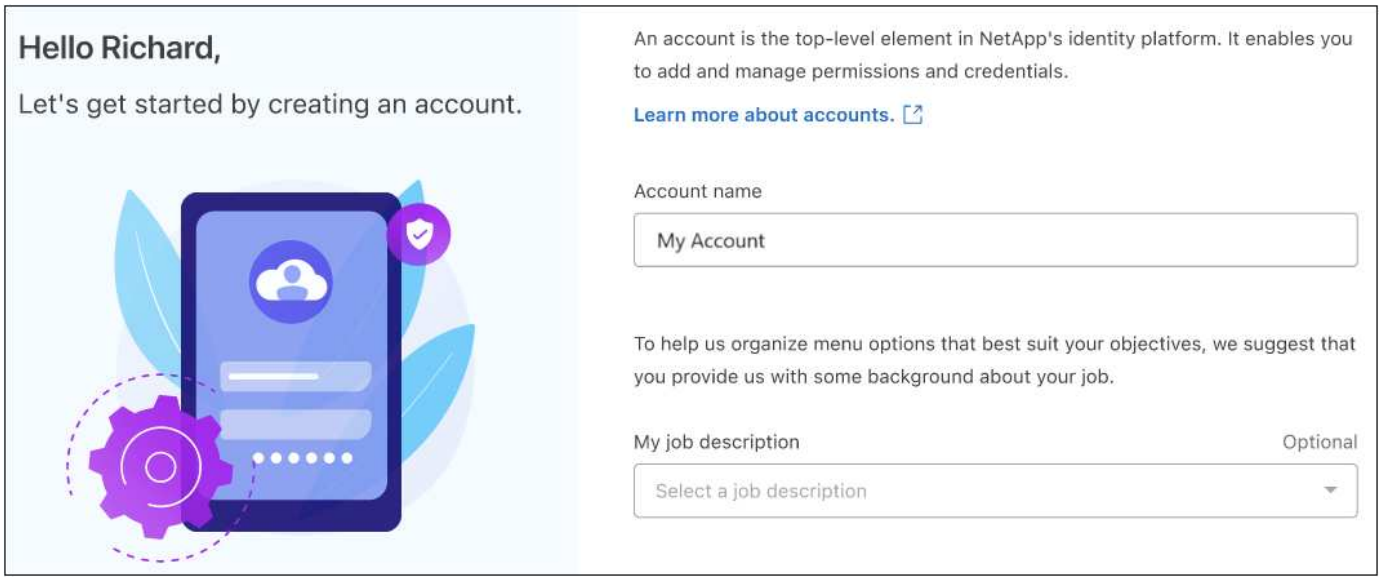
서비스형 소프트웨어

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.

다른 제품에 대해 자세히 "콘솔 환경"알아보십시오.

계정

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



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"..

작동 모드

Workload Factory는 클라우드 자산에 대한 액세스를 신중하게 제어하고 IT 정책에 따라 Workload Factory에 점진적인 신뢰를 할당할 수 있는 세 가지 운영 모드를 제공합니다.

- *기본 모드*는 제로 트러스트 관계를 나타내며 Workload Factory를 조기에 탐색하고 다양한 마법사를 사용하여 필요한 Infrastructure as Code를 생성하도록 설계되었습니다. 이 코드는 사용자가 관련 AWS 자격 증명과 함께 수동으로 복사하여 사용할 수 있습니다.
- * 읽기 전용 모드 * 사용자가 다양한 리소스와 도구를 탐지할 수 있도록 지원하여 관련 마법사를 완료할 수 있도록 지원함으로써 기본 모드의 사용 환경을 개선합니다.
- * 읽기/쓰기 모드 * 는 완전 신뢰 관계를 나타내며, 실행을 위해 필요하고 검증된 권한이 있는 할당된 자격 증명과 함께 사용자를 대신하여 실행 및 자동화하도록 설계되었습니다.

"Workload Factory 운영 모드에 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 통해서는 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 FSx for ONTAP 파일 시스템의 스토리지 환경이나 데이터베이스 워크로드 비용을 Elastic Block Store(EBS), Elastic File Systems(EFS), FSx for Windows File Server와 비교할 수 있는 절감 계산기를 제공합니다. 스토리지 요구 사항에 따라 FSx for ONTAP 파일 시스템이 가장 비용 효율적인 옵션일 수 있습니다.

- "스토리지 환경의 비용 절감 방법을 알아보십시오"
- "데이터베이스 워크로드 비용 절감 방법을 알아보십시오"

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"

운영 모드 및 **AWS** 자격 증명에 대해 자세히 알아보십시오

NetApp Workload Factory는 IT 정책에 따라 Workload Factory와 클라우드 자산 간의 액세스를 신중하게 제어할 수 있는 세 가지 운영 모드를 제공합니다. 사용하는 운영 모드는 Workload Factory에 제공하는 AWS 권한 수준에 따라 결정됩니다.

작동 모드

운영 모드는 사용자가 지정한 신뢰 수준에 따라 Workload Factory에서 제공하는 기능과 성능을 논리적으로 구성합니다. 운영 모드의 주요 목표는 Workload Factory가 AWS 계정 내에서 수행할 수 있는 작업과 수행할 수 없는 작업을 명확하게 전달하는 것입니다.

기본 모드

Workload Factory에 AWS 권한이 할당되지 않은 제로 트러스트 관계를 나타냅니다. Workload Factory를 조기에 탐색하고 다양한 마법사를 사용하여 필요한 Infrastructure as Code(IaC)를 생성하도록 설계되었습니다. AWS 자격 증명을 수동으로 입력하여 코드를 복사한 후 AWS에서 사용할 수 있습니다.

읽기 전용 모드입니다

IaC 템플릿에 특정 변수(예: VPC, 보안 그룹 등)를 채울 수 있도록 읽기 전용 권한을 추가하여 기본 모드의 경험을 향상시킵니다. 이를 통해 Workload Factory에 수정 권한을 제공하지 않고도 AWS 계정에서 직접 IaC를 실행할 수 있습니다.

읽기/쓰기 모드입니다

Workload Factory에 모든 권한이 할당되도록 완전한 신뢰 관계를 나타냅니다. 이를 통해 Workload Factory는 실행에 필요한 권한이 있는 할당된 자격 증명을 사용하여 사용자를 대신하여 AWS에서 작업을 실행하고 자동화할 수 있습니다.

자세히 알아보세요 "NetApp Workload Factory에 대한 권한" .

작동 모드 기능

각 모드에서 사용할 수 있는 기능은 각 모드에 따라 증가합니다.

모드를 선택합니다	**Workload Factory**의 자동화	**IAC**를 사용하여 **AWS** 내에서 자동화되었습니다	**AWS** 리소스 검색 및 자동 완성	진행 상황 모니터링
기본	아니요	최소 전체 IAC 템플릿	아니요	아니요
읽기 전용	아니요	IAC 템플릿을 적당히 작성합니다	예	예
읽기/쓰기	완전 자동화	완전 자동화가 가능한 완전한 IAC 템플릿	예	예

운영 모드 요구사항

Workload Factory에서는 어떤 모드를 사용할지 식별하기 위해 설정해야 할 선택기가 없습니다. 모드는 Workload Factory 계정에 할당한 AWS 자격 증명과 권한에 따라 결정됩니다.

모드를 선택합니다	**AWS** 계정 자격 증명	링크
기본	필요하지 않습니다	필요하지 않습니다
읽기 전용	읽기 전용	필요하지 않습니다
읽기/쓰기	읽기/쓰기 자격 증명	필수 요소입니다

"링크에 대해 자세히 알아보세요"

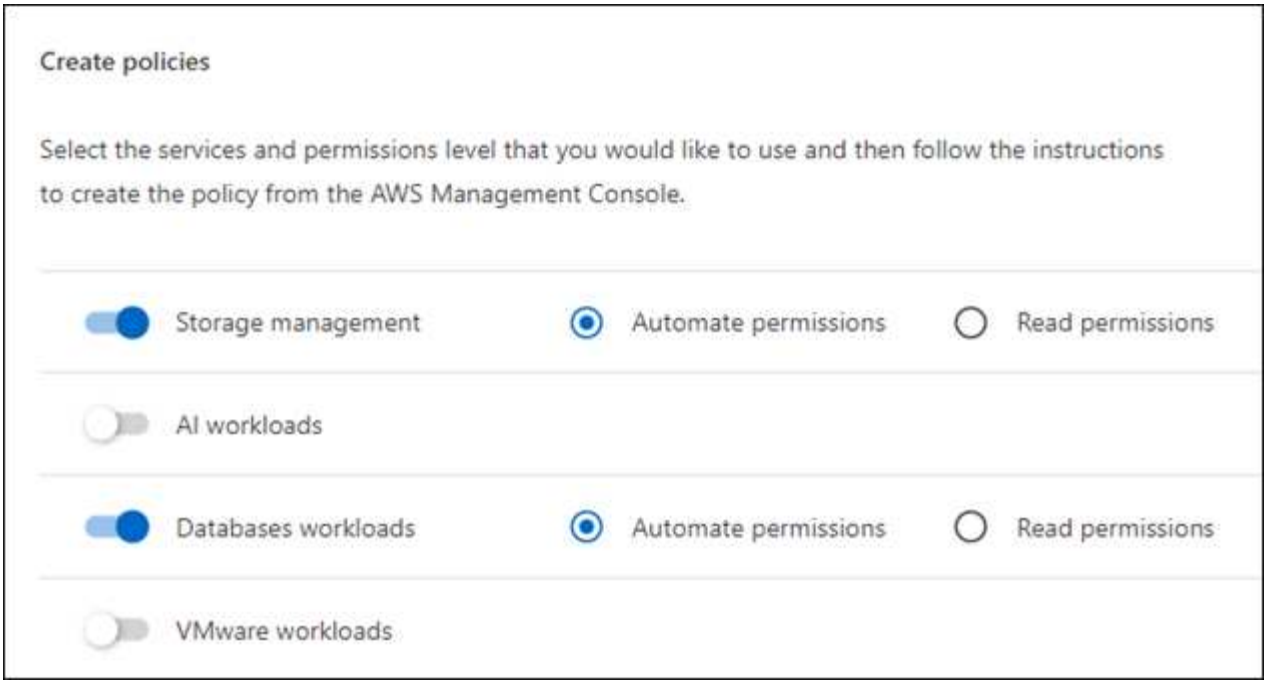
작동 모드의 예

자격 증명을 설정하여 하나의 워크로드 구성 요소에 대해 하나의 모드를 제공하고 다른 구성 요소에 대해 다른 모드를 제공할 수 있습니다. 예를 들어, FSx for ONTAP 파일 시스템을 배포하고 관리하는 작업의 경우 읽기/쓰기 모드를 구성할 수 있지만, Workload Factory를 사용하여 데이터베이스 워크로드를 생성하고 배포하는 경우에는 읽기 전용 모드만 구성할 수 있습니다.

Workload Factory 계정의 단일 자격 증명 세트 내에서 이러한 기능을 제공할 수도 있고, 각 자격 증명이 고유한 워크로드 배포 기능을 제공하는 경우 여러 자격 증명 세트를 만들 수도 있습니다.

예 **1**

다음 권한이 부여된 자격 증명을 사용하는 계정 사용자는 FSx for ONTAP 파일 시스템 생성, 데이터베이스 배포, 계정에서 사용되는 다른 유형의 AWS 스토리지 보기에 대한 전체 제어 권한(읽기/쓰기 모드)을 갖습니다.

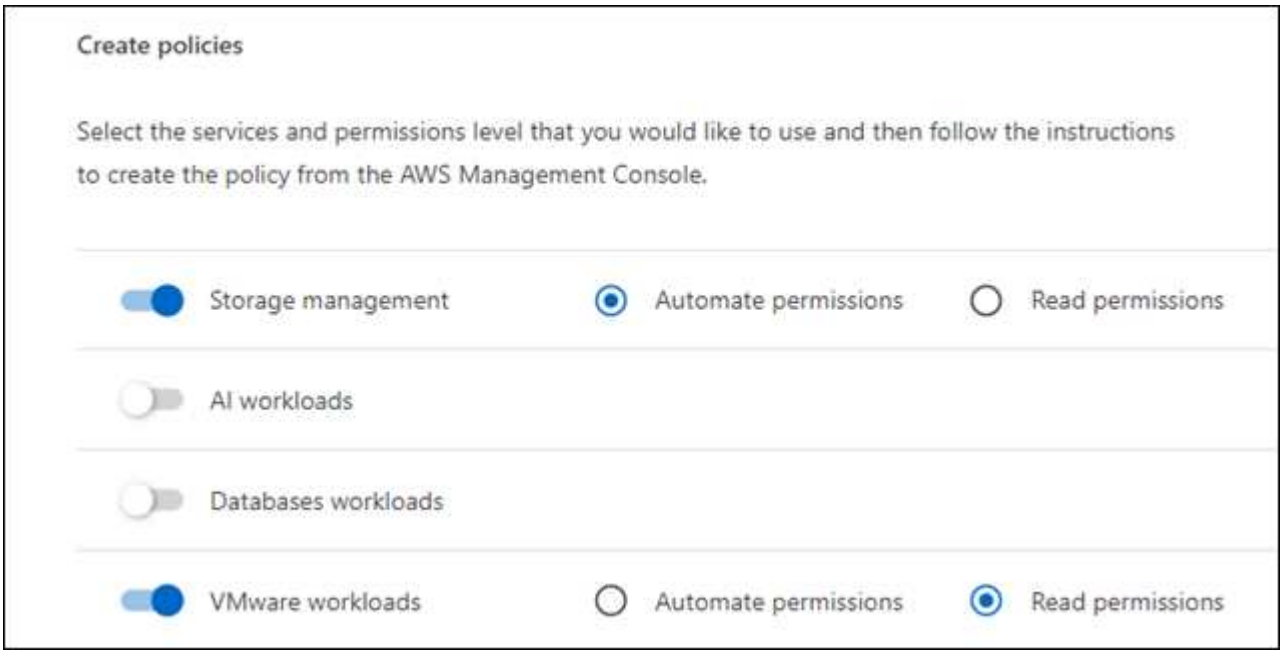


하지만 Workload Factory에서 VMware 워크로드(기본 모드)를 생성하고 배포하기 위한 자동화 제어 기능은 없습니다. VMware 워크로드를 생성하려면 Codebox에서 코드를 복사하고, AWS 계정에 수동으로 로그인하고, 생성된 코드에서 누락된 항목을 수동으로 채워서 이 기능을 사용해야 합니다.

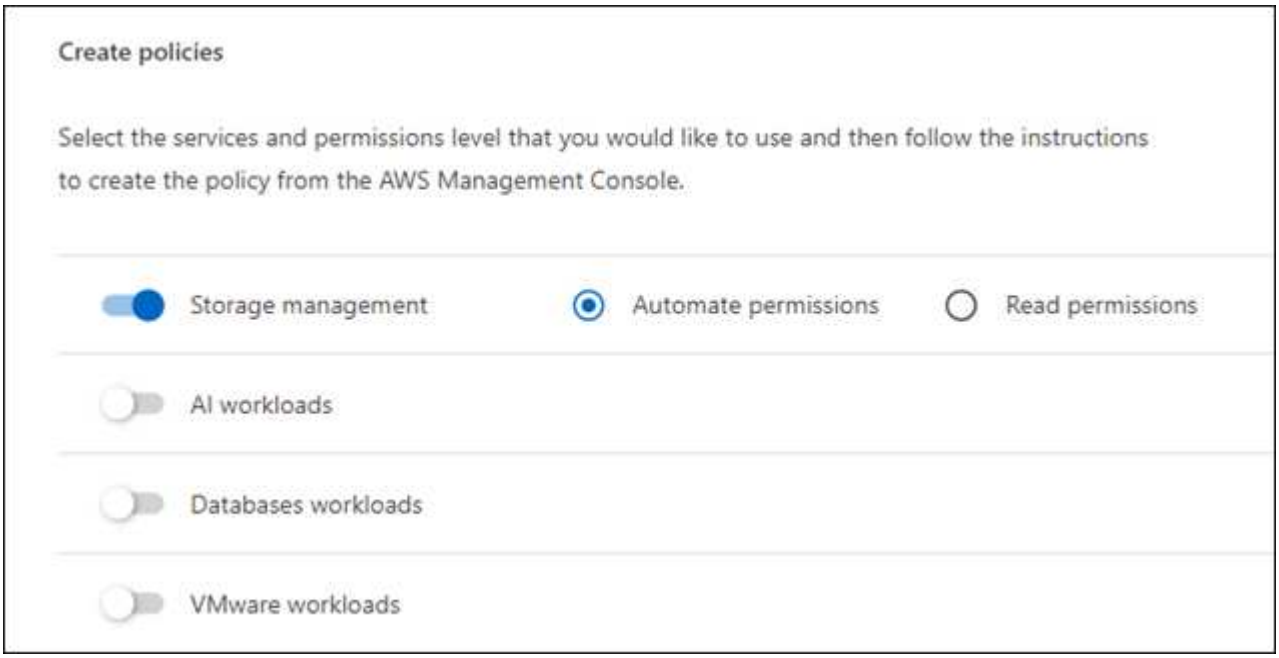
예 **2**

여기서 사용자는 선택한 자격 증명 세트에 따라 서로 다른 작동 기능을 사용할 수 있도록 두 개의 자격 증명을 만들었습니다. 일반적으로 각 자격 증명 세트는 다른 AWS 계정에 페어링됩니다.

첫 번째 자격 증명 세트에는 사용자에게 FSx for ONTAP 파일 시스템을 생성하는 데 필요한 모든 권한(및 계정에서 사용되는 다른 유형의 AWS 스토리지를 볼 수 있는 권한)을 부여하는 권한이 포함되어 있지만, VMware 워크로드를 사용하는 경우 읽기 전용 권한만 부여됩니다.



두 번째 자격 증명 세트는 FSx for ONTAP 파일 시스템을 생성하고 계정에 사용된 다른 유형의 AWS 스토리지를 볼 수 있는 권한을 사용자에게 부여할 뿐입니다.



AWS 자격 증명

다음과 같은 AWS 가정 역할 자격 증명 등록 흐름을 설계했습니다.

- 사용할 워크로드 기능을 지정하고 이러한 선택 항목에 따라 IAM 정책 요구사항을 제공하여 보다 조율된 AWS 계정 권한을 지원합니다.
- 특정 워크로드 기능에 대한 옵트인 또는 옵트아웃을 통해 부여된 AWS 계정 권한을 조정할 수 있습니다.
- AWS 콘솔에 적용할 수 있는 맞춤형 JSON 정책 파일을 제공하여 수동 IAM 정책 생성을 간소화합니다.
- AWS CloudFormation 스택을 사용하여 필요한 IAM 정책 및 역할 생성을 위한 자동화 옵션을 사용자에게 제공하여 자격 증명 등록 프로세스를 더욱 단순화합니다.
- FSx for ONTAP 서비스 자격 증명을 AWS 기반 기밀 관리 백엔드에서 저장할 수 있으므로 AWS 클라우드 에코시스템 경계 내에 자격 증명을 저장하려는 FSx for ONTAP 사용자에게 더 적합합니다.

하나 이상의 **AWS** 자격 증명

첫 번째 Workload Factory 기능(또는 기능들)을 사용할 때 해당 워크로드 기능에 필요한 권한을 사용하여 자격 증명을 만들어야 합니다. Workload Factory에 자격 증명을 추가하지만 IAM 역할과 정책을 생성하려면 AWS Management Console에 액세스해야 합니다. 이러한 자격 증명은 Workload Factory의 모든 기능을 사용할 때 계정 내에서 사용할 수 있습니다.

초기 AWS 자격 증명 세트에는 하나의 기능 또는 여러 기능에 대한 IAM 정책이 포함될 수 있습니다. 비즈니스 요구 사항에 따라 다릅니다.

Workload Factory에 AWS 자격 증명 세트를 두 개 이상 추가하면 FSx for ONTAP 파일 시스템, FSx for ONTAP 에 데이터베이스 배포, VMware 워크로드 마이그레이션 등의 추가 기능을 사용하는 데 필요한 추가 권한이 제공됩니다.

"Workload Factory에 AWS 자격 증명을 추가하는 방법을 알아보세요." .

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 Factory**에 액세스

NetApp 콘솔에서 Workload Factory에 액세스할 수 있습니다. AWS 스토리지 및 워크로드 기능에 Workload Factory를 사용하는 것 외에도 NetApp Copy and Sync, NetApp Digital Wallet 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 Factory**에 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

읽기 전용 또는 읽기/쓰기 모드 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. 사용하는 작업 부하로 스크롤하여 권한 목록, 권한의 목적, 사용 위치, 권한을 지원하는 모드를 확인하세요.

Storage에 사용할 수 있는 IAM 정책은 Workload Factory가 퍼블릭 클라우드 환경 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하며, 이는 사용자가 운영하는 운영 모드에 따라 달라집니다.

필요한 IAM 정책을 보려면 운영 모드를 선택하십시오.

읽기 전용 모드입니다

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "ec2:Describe*",
        "kms:Describe*",
        "elasticfilesystem:Describe*",
        "kms:List*",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

읽기/쓰기 모드입니다

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "iam:CreateServiceLinkedRole",
        "kms:Describe*",
        "elasticfilesystem:Describe*",
        "kms:List*",
        "kms:CreateGrant",
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "iam:SimulatePrincipalPolicy",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    }
  ]
}
```

다음 표에는 스토리지에 대한 사용 권한이 나와 있습니다.

스토리지에 대한 사용 권한 표

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP 파일 시스템을 생성합니다	FSx:CreateFileSystem*	구축	읽기/쓰기
FSx for ONTAP 파일 시스템에 대한 보안 그룹을 생성합니다	EC2:CreateSecurityGroup입니다	구축	읽기/쓰기
FSx for ONTAP 파일 시스템의 보안 그룹에 태그를 추가합니다	EC2: CreateTags(태그 생성)	구축	읽기/쓰기
FSx for ONTAP 파일 시스템에 대한 보안 그룹 송신 및 수신 권한을 부여합니다	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	읽기/쓰기
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
허가된 역할은 FSx for ONTAP과 다른 AWS 서비스 간에 통신을 제공합니다	IAM: CreateServiceLinkedRole	구축	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP 파일 시스템 배포 양식을 작성하는 방법에 대해 자세히 알아보십시오	EC2: 설명	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeSubnet	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: 설명	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeSecurityGroups	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: 설명표	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeNetworkInterfaces를 참조하십시오	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: VolumeStatus를 설명합니다	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
KMS 키 세부 정보를 얻고 FSx for ONTAP 암호화를 사용합니다	KMS: CreateGrant	구축	읽기/쓰기
	KMS: 설명 *	구축	• 읽기 전용 • 읽기/쓰기
	KMS: 목록 *	구축	• 읽기 전용 • 읽기/쓰기
EC2 인스턴스의 볼륨 세부 정보를 가져옵니다	EC2: 설명 볼륨을 참조하십시오	• 인벤토리 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
EC2 인스턴스에 대한 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
비용 절감 계산기에 Elastic File System에 대해 설명하십시오	Elasticfilesystem: 설명*	비용 절감 효과를	읽기 전용
FSx for ONTAP 리소스의 태그를 나열합니다	FSX:ListTagsForResource.를 참조하십시오	인벤토리	• 읽기 전용 • 읽기/쓰기
FSx for ONTAP 파일 시스템에 대한 보안 그룹 송신 및 수신을 관리합니다	EC2: RevokeSecurityGroupIngress 를 참조하십시오	관리 운영	읽기/쓰기
	EC2: DeleteSecurityGroup	관리 운영	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP 파일 시스템 리소스를 생성, 확인, 관리합니다	FSx:CreateVolume *	관리 운영	읽기/쓰기
	FSX:TagResource *	관리 운영	읽기/쓰기
	FSx:CreateStorageVirtualMachine *	관리 운영	읽기/쓰기
	FSX:DeleteFileSystem * 을 참조하십시오	관리 운영	읽기/쓰기
	FSx:DeleteStorageVirtualMachine *	관리 운영	읽기/쓰기
	FSx:파일 시스템 설명 *	인벤토리	• 읽기 전용 • 읽기/쓰기
	FSX:DescripbeStorageVirtualMachines *	인벤토리	• 읽기 전용 • 읽기/쓰기
	FSX:UpdateFileSystem*	관리 운영	읽기/쓰기
	FSX:UpdateStorageVirtualMachine*	관리 운영	읽기/쓰기
	FSx:볼륨 설명 *	인벤토리	• 읽기 전용 • 읽기/쓰기
	FSX:UpdateVolume *	관리 운영	읽기/쓰기
	FSx:DeleteVolume * 을 참조하십시오	관리 운영	읽기/쓰기
	FSX:UntagResource *	관리 운영	읽기/쓰기
	FSX:백업 설명 *	관리 운영	• 읽기 전용 • 읽기/쓰기
	FSx:CreateBackup *	관리 운영	읽기/쓰기
	FSX:CreateVolumeFromBackup*	관리 운영	읽기/쓰기
CloudWatch 메트릭 보고	CloudWatch: PutMetricData를 참조하십시오	관리 운영	읽기/쓰기
파일 시스템 및 볼륨 메트릭을 가져옵니다	CloudWatch: GetMetricData	관리 운영	• 읽기 전용 • 읽기/쓰기
	CloudWatch: GetMetricStatistics	관리 운영	• 읽기 전용 • 읽기/쓰기

데이터베이스 워크로드에 사용할 수 있는 IAM 정책은 Workload Factory가 퍼블릭 클라우드 환경 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하며, 이는 사용자가 운영하는 운영 모드에 따라 달라집니다.

필요한 IAM 정책을 보려면 운영 모드를 선택하십시오.

읽기 전용 모드입니다

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

읽기/쓰기 모드입니다

```
{
  "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:ModifyInstanceAttribute",
        "ec2:ModifyInstancePlacement",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolume",
        "ec2:ModifyVolumeAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "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": "CommonGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeLaunchTemplates",
        "ec2:RunInstances",
        "ec2:ModifyVpcAttribute",
        "fsx:CreateFileSystem",
        "fsx:UpdateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:UpdateVolume",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeBackups",
        "fsx:ListTagsForResource",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:DescribeCustomKeyStores",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "servicequotas:ListServiceQuotas",
        "sns:ListTopics",
        "sns:Publish",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeInstancePatchStates",
        "ssm:DescribePatchBaselines",
        "ssm:GetParametersByPath",
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:ListCommands",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
```

```
        "ssm:PutInventory",
        "ssm:SendCommand",
        "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",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:ListInferenceProfiles",
        "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*"
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter",
```

```
          "ssm:DeleteParameters"
        ],
        "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "*"
      }
    ]
  }
```

다음 표에는 데이터베이스 워크로드에 대한 사용 권한이 나와 있습니다.

데이터베이스 워크로드에 대한 사용 권한 테이블

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP, EBS 및 FSx for Windows File Server에 대한 메트릭 통계를 얻고 컴퓨팅 최적화 권장 사항을 확인하세요.	CloudWatch: GetMetricStatistics	• 인벤토리 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
등록된 SQL 노드에서 Amazon CloudWatch에 저장된 성능 지표를 수집합니다. 데이터는 등록된 SQL 인스턴스의 인스턴스 관리 화면에서 성능 추세 차트로 생성됩니다.	CloudWatch: GetMetricData	인벤토리	읽기 전용
이벤트의 트리거를 나열하고 설정합니다	SNS: ListTopics 를 참조하십시오	구축	• 읽기 전용 • 읽기/쓰기
EC2 인스턴스에 대한 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	• 인벤토리 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	EC2: 설명	구축	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeNetworkInterfaces를 참조하십시오	구축	• 읽기 전용 • 읽기/쓰기
	EC2:DescripbeInstanceTypes를 참조하십시오	• 구축 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP 배포 양식을 작성하는 방법에 대해 자세히 알아보십시오	EC2: 설명	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeSubnet	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeSecurityGroups	구축	• 읽기 전용 • 읽기/쓰기
	EC2: DescribeImages(설명 영상)	구축	• 읽기 전용 • 읽기/쓰기
	EC2: 설명	구축	• 읽기 전용 • 읽기/쓰기
	EC2: 설명표	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
기존 VPC 엔드포인트를 가져와 구축 전에 새 엔드포인트를 생성해야 하는지 여부를 결정합니다	EC2: DescribeVpcEndpoints	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
EC2 인스턴스의 공용 네트워크 연결과 상관없이 필요한 서비스에 VPC 엔드포인트가 없으면 생성합니다	EC2: CreateVpcEndpoint입니다	구축	읽기/쓰기
유효성 검사 노드 (t2.micro/t3.micro)에 대해 지역에서 사용할 수 있는 인스턴스 유형 가져오기	EC2: InstanceTypeOfferings를 설명합니다	구축	• 읽기 전용 • 읽기/쓰기
가격 책정 및 절감 효과를 위해 연결된 각 EBS 볼륨의 스냅샷 세부 정보를 확인합니다	EC2: 설명	비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
가격 책정 및 절감 예상 비용을 위해 연결된 각 EBS 볼륨의 세부 정보를 봅니다	EC2: 설명 볼륨을 참조하십시오	• 인벤토리 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
FSx for ONTAP 파일 시스템 암호화에 대한 KMS 키 세부 정보를 확인하십시오	KMS: ListAliases	구축	• 읽기 전용 • 읽기/쓰기
	KMS: ListKeys	구축	• 읽기 전용 • 읽기/쓰기
	KMS: 설명키	구축	• 읽기 전용 • 읽기/쓰기
환경에서 실행 중인 CloudFormation 스택 목록을 확인하여 할당량 제한을 확인합니다	CloudFormation: ListStacks	구축	• 읽기 전용 • 읽기/쓰기
배포를 트리거하기 전에 리소스에 대한 계정 제한을 확인하십시오	CloudFormation: DescripbeAccountLimits 를 참조하십시오	구축	• 읽기 전용 • 읽기/쓰기
해당 지역에서 AWS에서 관리하는 Active Directory 목록을 가져옵니다	DS:설명 디렉토리	구축	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
볼륨, 백업, SVM, AZ의 파일 시스템, FSx for ONTAP 파일 시스템용 태그의 목록과 세부 정보를 확인할 수 있습니다	FSx:볼륨 설명	• 인벤토리 • 비용 절감 살펴보기	• 읽기 전용 • 읽기/쓰기
	FSX:백업 설명	• 인벤토리 • 비용 절감 살펴보기	• 읽기 전용 • 읽기/쓰기
	FSX:DescripbeStorageVirtualMachines를 참조하십시오	• 구축 • 운영 관리 • 인벤토리	• 읽기 전용 • 읽기/쓰기
	FSx:파일 시스템 설명	• 구축 • 운영 관리 • 인벤토리 • 비용 절감 효과를	• 읽기 전용 • 읽기/쓰기
	FSX:ListTagsForResource.를 참조하십시오	운영 관리	• 읽기 전용 • 읽기/쓰기
CloudFormation 및 VPC에 대한 서비스 할당량 제한을 받습니다	servicequotas:ListServiceQuotas 입니다	구축	• 읽기 전용 • 읽기/쓰기
SSM 기반 쿼리를 사용하여 ONTAP용 FSx 지원 지역의 업데이트된 목록을 확인하십시오	SSM:GetParametersByPath 입니다	구축	• 읽기 전용 • 읽기/쓰기
구축 후 작업 관리 명령을 전송한 후 SSM 응답을 폴링합니다	SSM: GetCommandInvocation 을 참조하십시오	• 운영 관리 • 인벤토리 • 비용 절감 효과를 • 최적화	• 읽기 전용 • 읽기/쓰기
SSM을 통해 EC2 인스턴스로 명령을 전송합니다	SSM: SendCommand 를 참조하십시오	• 운영 관리 • 인벤토리 • 비용 절감 효과를 • 최적화	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
배포 후 인스턴스의 SSM 연결 상태를 가져옵니다	SSM: GetConnectionStatus 를 참조하십시오	• 운영 관리 • 인벤토리 • 최적화	• 읽기 전용 • 읽기/쓰기
관리되는 EC2 인스턴스 그룹(SQL 노드)에 대한 SSM 연결 상태 가져오기	SSM: DescripbeInstanceInformation을 참조하십시오	인벤토리	읽기
운영 체제 패치 평가에 사용할 수 있는 패치 기준 목록을 가져옵니다	SSM: PatchBaseline 설명	최적화	• 읽기 전용 • 읽기/쓰기
운영 체제 패치 평가를 위해 Windows EC2 인스턴스의 패치 상태를 가져옵니다	SSM: InstancePatchStates 설명	최적화	• 읽기 전용 • 읽기/쓰기
운영 체제 패치 관리를 위해 EC2 인스턴스에서 AWS Patch Manager가 실행한 명령을 나열합니다	SSM: ListCommands 를 참조하십시오	최적화	• 읽기 전용 • 읽기/쓰기
계정이 AWS Compute Optimizer에 등록되었는지 확인합니다	계산 최적화 프로그램: GetEnrollmentStatus	• 비용 절감 효과를 • 최적화	읽기/쓰기
AWS Compute Optimizer에서 기존 권장 사항 기본 설정을 업데이트하여 SQL Server 워크로드에 대한 제안을 조정합니다	컴퓨팅 최적화 프로그램: 권장 사항 권장 사항 기본 설정	• 비용 절감 효과를 • 최적화	읽기/쓰기
AWS Compute Optimizer에서 특정 리소스에 적용되는 권장 사항 기본 설정을 확인합니다	Compute-Optimizer: GetEffective권장 사항 기본 설정	• 비용 절감 효과를 • 최적화	읽기/쓰기
AWS Compute Optimizer가 Amazon EC2(Amazon Elastic Compute Cloud) 인스턴스에 대해 생성하는 권장 사항을 가져옵니다	컴퓨팅 최적화: GetEC2InstanceRecommendations 를 참조하십시오	• 비용 절감 효과를 • 최적화	읽기/쓰기
자동 크기 조정 그룹에 대한 인스턴스 연결을 확인합니다	자동 크기 조정: AutoScalingGroup 설명	• 비용 절감 효과를 • 최적화	읽기/쓰기
	자동 크기 조정:자동 크기 조정 설명	• 비용 절감 효과를 • 최적화	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
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	• 구축 • 운영 관리	• 읽기 전용 • 읽기/쓰기
	SSM: GetParameters(GetParameters	운영 관리	• 읽기 전용 • 읽기/쓰기
	SSM: PutParameter 1	• 구축 • 운영 관리	• 읽기 전용 • 읽기/쓰기
	SSM: 매개 변수 삭제	운영 관리	• 읽기 전용 • 읽기/쓰기
네트워크 리소스를 SQL 노드 및 유효성 검사 노드에 연결하고 SQL 노드에 보조 IP를 추가합니다	EC2: AllocateAddress(주소 1)	구축	읽기/쓰기
	EC2: AllocateHosts(호스트 1)	구축	읽기/쓰기
	2:1:1:1(주소 지정)	구축	읽기/쓰기
	EC2: 연관 주소 1	구축	읽기/쓰기
	2:1(2)	구축	읽기/쓰기
	EC2: AssociateSubnetCidrBlock(연결	구축	읽기/쓰기
	2:1:1:1:1:1:1:1:1:1:1:1:1:1:1:1	구축	읽기/쓰기
	(영어): AttachInternetGateway (영어	구축	읽기/쓰기
	(영어) - 어탯치먼트 네트워크 인터페이스 (영어	구축	읽기/쓰기
구축을 위해 필요한 EBS 볼륨을 SQL 노드에 연결	EC2: AttachVolume	구축	읽기/쓰기
보안 그룹을 연결하고 프로비저닝된 노드에 대한 규칙을 수정합니다	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	읽기/쓰기
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
구축을 위해 SQL 노드에 필요한 EBS 볼륨을 생성합니다	EC2: CreateVolume	구축	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
t2.micro 유형으로 생성된 임시 유효성 검사 노드를 제거하고 실패한 EC2 SQL 노드의 롤백 또는 재시도를 위해 제거합니다	EC2: DeleteNetworkInterface	구축	읽기/쓰기
	EC2: DeleteSecurityGroup	구축	읽기/쓰기
	EC2: 삭제 태그	구축	읽기/쓰기
	EC2: DeleteVolume(삭제 볼륨)	구축	읽기/쓰기
	EC2: 분리 네트워크 인터페이스	구축	읽기/쓰기
	EC2: DetachVolume(분리 볼륨)	구축	읽기/쓰기
	EC2: 연결 해제 주소	구축	읽기/쓰기
	EC2: DiscassociateIamInstanceProfile 을 참조하십시오	구축	읽기/쓰기
	EC2: 연결 해제 라우팅 테이블	구축	읽기/쓰기
	EC2: 연결 해제 SubnetCidrBlock	구축	읽기/쓰기
	EC2: 연결 해제 VpcCidrBlock	구축	읽기/쓰기
생성된 SQL 인스턴스의 특성을 수정합니다. WLMDB로 시작하는 이름에만 적용됩니다.	EC2: ModifyInstanceAttribute	구축	읽기/쓰기
	EC2:ModifyInstancePlacement	구축	읽기/쓰기
	EC2: ModifyNetworkInterfaceAttribute 입니다	구축	읽기/쓰기
	EC2: ModifySubnetAttribute 를 사용합니다	구축	읽기/쓰기
	EC2: ModifyVolume(수정 볼륨)	구축	읽기/쓰기
	EC2: ModifyVolumeAttribute	구축	읽기/쓰기
	EC2:ModifyVpcAttribute 를 사용합니다	구축	읽기/쓰기
유효성 검사 인스턴스의 연결을 끊고 제거합니다	EC2: ReleaseAddress(릴리스 주소)	구축	읽기/쓰기
	EC2: ReplaceRoute	구축	읽기/쓰기
	EC2: ReplaceRouteTableAssociation 을 참조하십시오	구축	읽기/쓰기
	EC2: RevokeSecurityGroupEgress	구축	읽기/쓰기
	EC2: RevokeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
배포된 인스턴스를 시작합니다	EC2: StartInstances(시작 인스턴스)	구축	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
배포된 인스턴스를 중지합니다	EC2: StopInstances(중지 인스턴스)	구축	읽기/쓰기
WLMDB에서 생성한 Amazon FSx for NetApp ONTAP 리소스에 대한 사용자 지정 값에 태그를 지정하여 리소스 관리 중에 청구 세부 정보를 가져옵니다	자유무역협정(FSX)	• 구축 • 운영 관리	읽기/쓰기
배포할 CloudFormation 템플릿을 만들고 유효성을 검사합니다	CloudFormation:CreateStack	구축	읽기/쓰기
	CloudFormation: DescribeStackEvents	구축	읽기/쓰기
	CloudFormation: DescribeStacks	구축	읽기/쓰기
	CloudFormation: ListStacks	구축	읽기/쓰기
	CloudFormation:ValidateTemplate을 참조하십시오	구축	읽기/쓰기
지역에서 사용 가능한 디렉토리를 가져옵니다	DS:설명 디렉토리	구축	읽기/쓰기
프로비저닝된 EC2 인스턴스에 연결된 보안 그룹에 대한 규칙을 추가합니다	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	구축	읽기/쓰기
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
재시도 및 롤백을 위해 중첩된 스택 템플릿을 생성합니다	EC2:CreateLaunchTemplate	구축	읽기/쓰기
	EC2: CreateLaunchTemplateVersion	구축	읽기/쓰기
생성된 인스턴스에서 태그 및 네트워크 보안을 관리합니다	EC2: CreateNetworkInterface입니다	구축	읽기/쓰기
	EC2:CreateSecurityGroup입니다	구축	읽기/쓰기
	EC2: CreateTags(태그 생성)	구축	읽기/쓰기
유효성 검사 노드를 위해 임시로 만든 보안 그룹을 삭제합니다	EC2: DeleteSecurityGroup	구축	읽기/쓰기
프로비저닝을 위한 인스턴스 세부 정보를 가져옵니다	ec2:주소 설명	구축	읽기/쓰기
	ec2:DescribeLaunchTemplates	구축	읽기/쓰기
생성된 인스턴스를 시작합니다	EC2: 런인스턴스	구축	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
프로비저닝에 필요한 FSx for ONTAP 리소스를 생성합니다. 기존 FSx for ONTAP 시스템의 경우 SQL 볼륨을 호스팅하는 새로운 SVM이 생성됩니다.	FSX:CreateFileSystem 을 참조하십시오	구축	읽기/쓰기
	FSx:CreateStorageVirtualMachine	구축	읽기/쓰기
	FSX:CreateVolume 을 참조하십시오	• 구축 • 운영 관리	읽기/쓰기
FSx for ONTAP 정보를 확인하십시오	fsx:파일 시스템 별칭 설명	구축	읽기/쓰기
	파일 시스템 여유 공간을 해결하기 위해 FSx for ONTAP 파일 시스템의 크기를 조정합니다	FSx:UpdateFile system입니다	최적화
읽기/쓰기	로그 및 TempDB 드라이브 크기를 수정하기 위해 볼륨 크기를 조정합니다	FSX:UpdateVolume을 참조하십시오	최적화
읽기/쓰기	KMS 키 세부 정보를 얻고 FSx for ONTAP 암호화를 사용합니다	KMS: CreateGrant	구축
읽기/쓰기		kms:사용자 정의 키 저장소 설명	구축
읽기/쓰기		KMS : GenerateDataKey	구축

목적	조치	사용된 위치	모드를 선택합니다
읽기/쓰기	EC2 인스턴스에서 실행되는 검증 및 프로비저닝 스크립트를 위한 CloudWatch 로그를 생성합니다	로그:CreateLogGroup	구축
읽기/쓰기		로그: CreateLogStream	구축
읽기/쓰기		로그:DescripbeLogStreams	• 구축 • 평가
읽기/쓰기		로그:GetLogGroupFields	구축
읽기/쓰기		로그:GetLogRecord	구축
읽기/쓰기		로그:ListLogDeliveries입니다	구축
읽기/쓰기		로그: PutLogEvents	• 구축 • 운영 관리
읽기/쓰기		로그:TagResource	구축
읽기/쓰기	SSM 출력 잘림이 발생하면 Workload Factory가 SQL 인스턴스에 대한 Amazon CloudWatch 로그로 전환됩니다.	로그:GetLogEvents	• 스토리지 평가(최적화) • 인벤토리
• 읽기 전용 • 읽기/쓰기	Workload Factory가 현재 로그 그룹을 가져오고 Workload Factory에서 생성한 로그 그룹에 대한 보존이 설정되었는지 확인하도록 허용합니다.	로그:DescripbeLogGroups	• 스토리지 평가(최적화) • 인벤토리
읽기 전용	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	• 스토리지 평가(최적화) • 인벤토리
• 읽기 전용 • 읽기/쓰기	SQL, 도메인 및 FSx for ONTAP에 대해 제공된 자격 증명에 대한 암호를 사용자 계정에 생성합니다	servicequotas:ListServiceQuotas 입니다	구축
읽기/쓰기	고객 SNS 항목을 나열하고 WLMDB 백엔드 SNS 및 고객 SNS에 게시합니다(선택한 경우)	SNS: ListTopics를 참조하십시오	구축
읽기/쓰기		SNS: 게시	구축

목적	조치	사용된 위치	모드를 선택합니다
읽기/쓰기	프로비저닝된 SQL 인스턴스에서 검색 스크립트를 실행하고 FSx for ONTAP 지원 AWS 지역의 최신 목록을 가져오려면 SSM 권한이 필요합니다.	SSM: PutComplianceItems 를 참조하십시오	구축
읽기/쓰기		SSM: PutConfigurePackageResult 를 참조하십시오	구축
읽기/쓰기		SSM: 재고 입고	구축
읽기/쓰기		SSM: SendCommand 를 참조하십시오	• 구축 • 인벤토리 • 운영 관리
읽기/쓰기		SSM: 업데이트 연결 상태	구축
읽기/쓰기		SSM: UpdateInstanceAssociationStatus 를 참조하십시오	구축
읽기/쓰기		SSM: UpdateInstanceInformation 을 참조하십시오	구축
읽기/쓰기		ssmmessages: CreateControlChannel	구축
읽기/쓰기		ssmmessages: CreateDataChannel	구축
읽기/쓰기		ssmmessages: OpenControlChannel	구축
읽기/쓰기		ssmmessages: 오픈데이터채널	구축

목적	조치	사용된 위치	모드를 선택합니다
읽기/쓰기	FSx for ONTAP, Active Directory 및 SQL 사용자에 대한 자격 증명 저장(SQL 사용자 인증에만 해당)	SSM: GetParameter(GetParameter	• 구축 • 운영 관리 • 인벤토리
읽기/쓰기		SSM: GetParameters(GetParameters	• 구축 • 인벤토리
읽기/쓰기		SSM: PutParameter 1	• 구축 • 운영 관리
읽기/쓰기		SSM: 매개 변수 삭제	• 구축 • 운영 관리
읽기/쓰기	성공 또는 실패에 대한 신호 CloudFormation 스택.	이 부분의 본문은 서명자 입니다	구축
읽기/쓰기	템플릿으로 생성된 EC2 역할을 EC2의 인스턴스 프로필에 추가하여 EC2의 스크립트가 배포에 필요한 리소스에 액세스할 수 있도록 합니다.	IAM:AddRoleToInstanceProfile 을 참조하십시오	구축
읽기/쓰기	EC2의 인스턴스 프로필을 생성하고 생성된 EC2 역할을 연결합니다.	IAM:CreateInstanceProfile	구축
읽기/쓰기	아래에 나열된 권한이 있는 템플릿을 통해 EC2 역할을 생성합니다	IAM: CreateRole	구축
읽기/쓰기	EC2 서비스에 연결된 역할을 생성합니다	IAM: CreateServiceLinkedRole (영어	구축
읽기/쓰기	특히 검증 노드에 대해 구축 중에 생성된 인스턴스 프로필을 삭제합니다	IAM: DeleteInstance Profile	구축
읽기/쓰기	역할 및 정책 세부 정보를 확인하여 사용 권한의 공백을 확인하고 배포를 검증합니다	IAM: GetPolicy 를 참조하십시오	구축
읽기/쓰기		IAM: GetPolicyVersion 을 참조하십시오	구축
읽기/쓰기		IAM:GetRole	구축
읽기/쓰기		IAM: GetRolePolicy 를 참조하십시오	구축
읽기/쓰기		IAM: GetUser	구축

목적	조치	사용된 위치	모드를 선택합니다
읽기/쓰기	생성된 역할을 EC2 인스턴스로 전달합니다	IAM: 패스역할 3	구축
읽기/쓰기	생성된 EC2 역할에 필요한 권한이 있는 정책을 추가합니다	IAM: PutRolePolicy(입수 정책)	구축
읽기/쓰기	프로비저닝된 EC2 인스턴스 프로필에서 역할을 분리합니다	IAM:RemoveRoleFromInstanceProfile 을 참조하십시오	구축
읽기/쓰기	워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축

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 모드에서만 사용할 수 있습니다.

GenAI 워크로드를 위한 IAM 정책

```
{
  "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.

GenAI 워크로드에 대한 사용 권한 표

목적	조치	사용된 위치	모드를 선택합니다
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	모드를 선택합니다
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:DescripbeLogGroups	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

목적	조치	사용된 위치	모드를 선택합니다
AI 엔진에 대한 SSM 연결을 점검하십시오	SSM: SendCommand 를 참조하십시오	구축	읽기/쓰기
	SSM: GetConnectionStatus 를 참조하십시오	구축	읽기/쓰기
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:DescripbeStorageVirtualMachines를 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

목적	조치	사용된 위치	모드를 선택합니다
Amazon CloudWatch에서 SSM 응답 받기(응답이 너무 긴 경우)	로그:DescripbeLogStreams	문제 해결	읽기/쓰기
Amazon CloudWatch에서 SSM 응답을 받으십시오	로그:GetLogEvents	문제 해결	읽기/쓰기
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 워크로드에 대한 IAM 정책은 VMware용 Workload Factory가 사용자의 운영 모드에 따라 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다.

필요한 IAM 정책을 보려면 운영 모드를 선택하십시오.

읽기 전용 모드입니다

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ssm:GetParametersByPath",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

읽기/쓰기 모드입니다

```
{
  "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:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath",
        "ssm:GetParameters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
```

```
        "Resource": "*"
      }
    ]
  }
```

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

VMware 워크로드에 대한 사용 권한 표

목적	조치	사용된 위치	모드를 선택합니다
보안 그룹을 연결하고 프로비저닝된 노드에 대한 규칙을 수정합니다	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	구축	읽기/쓰기
EBS 볼륨을 생성합니다	EC2: CreateVolume	구축	읽기/쓰기
VMware 워크로드에서 생성한 FSx for NetApp ONTAP 리소스에 대한 사용자 지정 값에 태그를 지정합니다	FSX:태그 리소스	구축	읽기/쓰기
CloudFormation 템플릿을 만들고 유효성을 검사합니다	CloudFormation:CreateStack	구축	읽기/쓰기
생성된 인스턴스에서 태그 및 네트워크 보안을 관리합니다	EC2:CreateSecurityGroup입니다	구축	읽기/쓰기
생성된 인스턴스를 시작합니다	EC2: 런인스턴스	구축	읽기/쓰기
EC2 인스턴스 세부 정보를 가져옵니다	EC2: DescribeInstances(지시 인스턴스)	구축	읽기/쓰기
배포 및 재구축 작업 중에 스택을 생성하는 동안 이미지를 나열합니다	EC2: DescribeImages(설명 영상)	구축	읽기/쓰기
선택한 환경에서 VPC를 가져와 배포 양식을 작성합니다	EC2: 설명	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
선택한 환경에서 서브넷을 가져와 배포 양식을 완성합니다	EC2: DescribeSubnet	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
선택한 환경의 보안 그룹을 가져와 배포 양식을 작성합니다	EC2: DescribeSecurityGroups	구축	• 읽기 전용 • 읽기/쓰기
선택한 환경에서 가용 영역을 가져옵니다	EC2:가용성 영역 설명	• 구축 • 인벤토리	• 읽기 전용 • 읽기/쓰기
Amazon FSx for NetApp ONTAP 지원으로 지역을 확인하십시오	EC2: 설명	구축	• 읽기 전용 • 읽기/쓰기
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키 별칭을 가져옵니다	KMS: ListAliases	구축	• 읽기 전용 • 읽기/쓰기
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키를 가져옵니다	KMS: ListKeys	구축	• 읽기 전용 • 읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
Amazon FSx for NetApp ONTAP 암호화에 사용할 KMS 키 만료 세부 정보를 가져옵니다	KMS: 설명키	구축	• 읽기 전용 • 읽기/쓰기
SSM 기반 쿼리는 Amazon FSx for NetApp ONTAP 지원 지역의 업데이트된 목록을 가져오는 데 사용됩니다	SSM:GetParametersByPath 입니다	구축	• 읽기 전용 • 읽기/쓰기
프로비저닝에 필요한 Amazon FSx for NetApp ONTAP 리소스를 생성합니다	FSX:CreateFileSystem 을 참조하십시오	구축	읽기/쓰기
	FSx:CreateStorageVirtualMachine	구축	읽기/쓰기
	FSX:CreateVolume 을 참조하십시오	• 구축 • 관리 운영	읽기/쓰기
NetApp ONTAP용 Amazon FSx에 대해 자세히 알아보십시오	FSX: 설명 *	• 구축 • 인벤토리 • 관리 운영 • 비용 절감 효과를	읽기/쓰기
	FSX:목록 *	• 구축 • 인벤토리	읽기/쓰기
KMS 키 세부 정보를 확인하고 Amazon FSx for NetApp ONTAP 암호화에 사용합니다	KMS: CreateGrant	구축	읽기/쓰기
	KMS: 설명 *	구축	읽기/쓰기
	KMS: 목록 *	구축	읽기/쓰기
	KMS: 암호 해독	구축	읽기/쓰기
	KMS : GenerateDataKey	구축	읽기/쓰기
고객 SNS 항목을 나열하고 WLMVMC 백엔드 SNS 및 고객 SNS에 게시합니다(선택한 경우)	SNS: 게시	구축	읽기/쓰기
Amazon FSx for NetApp ONTAP 지원 AWS 지역의 최신 목록을 가져오는 데 사용됩니다	SSM: GET *	• 구축 • 관리 운영	읽기/쓰기
워크로드 작업을 시뮬레이션하여 사용 가능한 권한을 검증하고 필요한 AWS 계정 권한과 비교하십시오	IAM: SimulatePrincipalPolicy(IAM: 시뮬레이션 정책)	구축	읽기/쓰기

목적	조치	사용된 위치	모드를 선택합니다
SSM 매개 변수 저장소는 Amazon FSx for NetApp ONTAP의 자격 증명을 저장하는 데 사용됩니다	SSM:GetParameter입니다	• 구축 • 관리 운영 • 인벤토리	읽기/쓰기
	SSM: PutParameters 를 참조하십시오	• 구축 • 인벤토리	읽기/쓰기
	SSM: PutParameter	• 구축 • 관리 운영	읽기/쓰기
	SSM: 매개 변수 삭제	• 구축 • 관리 운영	읽기/쓰기

변경 로그

권한이 추가되고 제거됨에 따라 아래 섹션에 해당 권한이 표시됩니다.

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` .

NetApp Workload Factory 빠른 시작

NetApp Workload Factory를 시작하려면 가입하고 계정을 만든 후, Workload Factory가 AWS 리소스를 직접 관리할 수 있도록 자격 증명을 추가하고, Amazon FSx for NetApp ONTAP 사용하여 워크로드를 최적화하세요.

NetApp Workload Factory는 사용자가 웹 기반 콘솔에서 클라우드 서비스로 접근할 수 있습니다. 시작하기 전에 다음

사항을 이해해야 합니다."작업 부하 공장" 그리고"작동 모드" .

1 등록하고 계정을 만듭니다

로 가다 "워크로드 팩토리 콘솔" , 가입하고 계정을 만드세요.

"계정 등록 및 생성 방법에 대해 알아보십시오"..

2 **Workload Factory**에 **AWS** 자격 증명 추가

이 단계는 선택 사항입니다. AWS 계정에 액세스하기 위한 자격 증명을 추가하지 않고도 기본 모드에서 Workload Factory를 사용할 수 있습니다. Workload Factory에 AWS 자격 증명을 읽기 전용 모드 또는 읽기/쓰기 모드로 추가하면 Workload Factory 계정에 FSx for ONTAP 파일 시스템을 생성하고 관리하고 데이터베이스 및 GenAI와 같은 특정 워크로드를 배포하고 관리하는 데 필요한 권한이 부여됩니다.

"계정에 자격 증명을 추가하는 방법에 대해 알아봅니다"..

3 **FSx for ONTAP**를 사용하여 워크로드를 최적화하십시오

가입하고, 계정을 만들고, 선택적으로 AWS 자격 증명을 추가한 후 FSx for ONTAP 사용하여 워크로드를 최적화하기 위해 Workload Factory를 사용할 수 있습니다.

"FSx for ONTAP 으로 워크로드를 최적화하세요" .

NetApp Workload Factory에 가입하세요

NetApp Workload Factory는 웹 기반 콘솔에서 접근할 수 있습니다. Workload Factory를 시작하려면 먼저 기존 NetApp 지원 사이트 자격 증명을 사용하거나 NetApp 클라우드 로그인을 만들어 가입해야 합니다.

이 작업에 대해

다음 옵션 중 하나를 사용하여 Workload Factory에 가입할 수 있습니다.

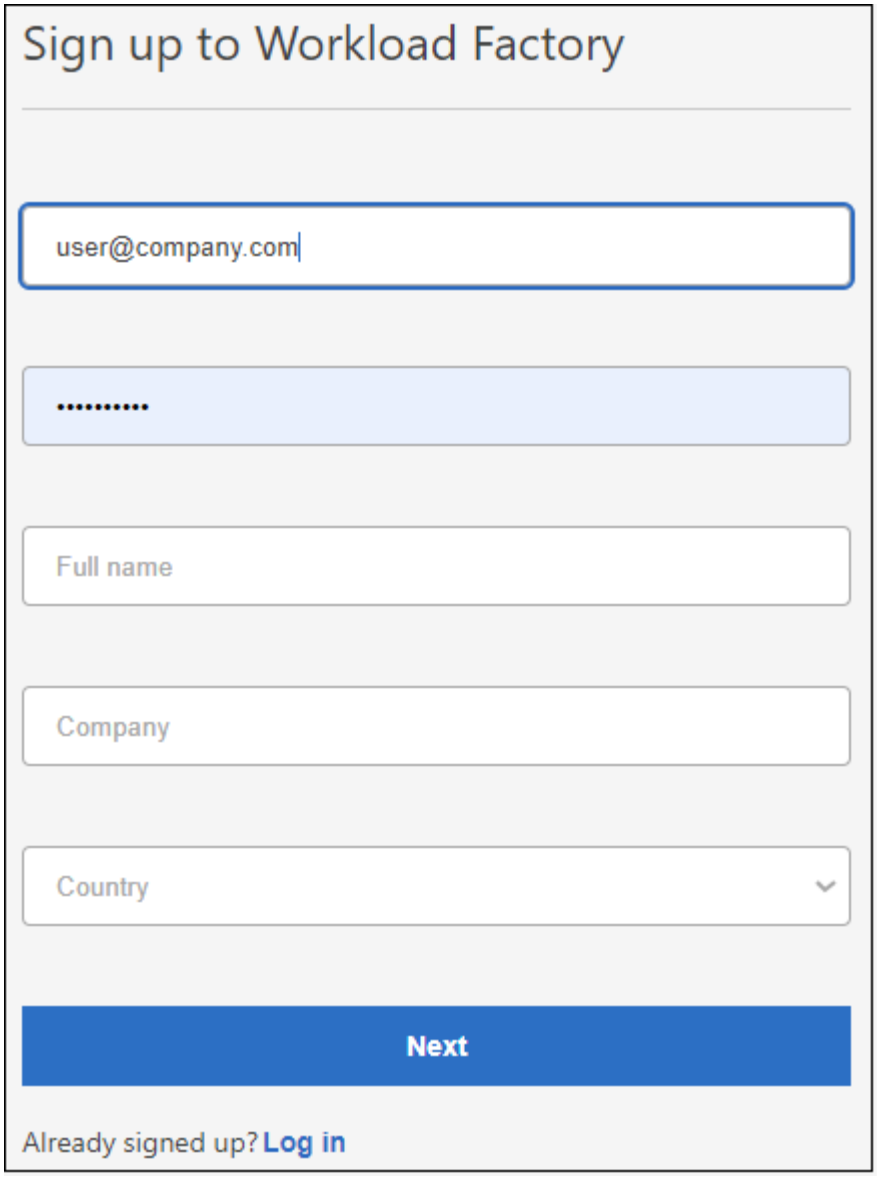
- 기존 NetApp Support 사이트(NSS) 자격 증명
- 이메일 주소와 암호를 지정하여 NetApp 클라우드 로그인입니다

단계

1. 웹 브라우저를 열고 이동하세요 "워크로드 팩토리 콘솔"
2. NetApp Support 사이트 계정이 있는 경우 NSS 계정과 연결된 이메일 주소를 * 로그인 * 페이지에 직접 입력합니다.

   NSS 계정이 있으면 가입 페이지를 건너뛸 수 있습니다. Workload Factory는 귀하를 이 초기 로그인의 일부로 등록합니다.

3. NSS 계정이 없는 경우 NetApp 클라우드 로그인을 생성하여 등록하려면 * 등록 * 을 선택하십시오.



4. 등록 * 페이지에서 NetApp 클라우드 로그인을 생성하는 데 필요한 정보를 입력하고 * 다음 * 을 선택합니다.

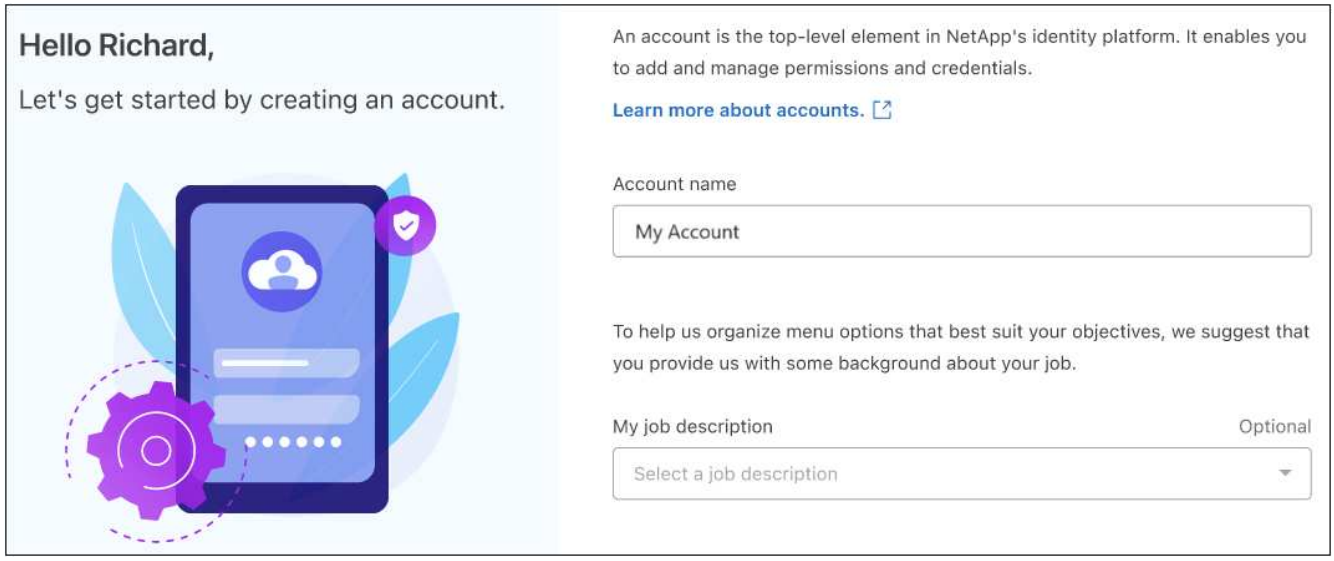
   등록 양식에는 영어 문자만 사용할 수 있습니다.

5. 회사의 세부 정보를 입력하고 * 등록 * 을 선택합니다.
6. 받은 편지함에서 이메일 주소 확인에 대한 지침이 포함된 NetApp의 이메일을 확인합니다.

   이 단계는 로그인하기 전에 필요합니다.

7. 메시지가 표시되면 최종 사용자 사용권 계약을 검토하고 약관에 동의하고 * 계속 * 을 선택합니다.
8. 계정 * 페이지에서 계정 이름을 입력하고 필요한 경우 직무 설명을 선택합니다.

   계정은 NetApp의 ID 플랫폼에서 최상위 요소이며 사용 권한과 자격 증명을 추가 및 관리할 수 있습니다.



9. *만들기*를 선택하면 Workload Factory 홈페이지가 표시됩니다.

결과

이제 Workload Factory 로그인과 계정이 생겼습니다. 귀하는 계정 관리자로 간주되며 모든 Workload Factory 기능에 액세스할 수 있습니다.

Workload Factory에 AWS 자격 증명 추가

NetApp Workload Factory가 AWS 계정에서 클라우드 리소스를 배포하고 관리하는 데 필요한 권한을 갖도록 AWS 자격 증명을 추가하고 관리합니다.

개요

AWS 계정 자격 증명을 추가하지 않으면 Workload Factory는 기본 모드로 작동합니다. 자격 증명을 추가하여 읽기 전용 모드 및 읽기/쓰기 모드와 같은 다른 작업 모드를 활성화할 수 있습니다. "작동 모드에 대해 자세히 알아보십시오" .

자격 증명 페이지에서 기존 Workload Factory 계정에 AWS 자격 증명을 추가할 수 있습니다. 이를 통해 Workload Factory는 AWS 클라우드 환경 내의 리소스와 프로세스를 관리하는 데 필요한 권한을 얻습니다.

다음 두 가지 방법을 사용하여 자격 증명을 추가할 수 있습니다.

- 수동으로: Workload Factory에서 자격 증명을 추가하는 동안 AWS 계정에서 IAM 정책과 IAM 역할을 생성합니다.
- * 자동 *: 사용 권한에 대한 최소한의 정보를 캡처한 다음 CloudFormation 스택을 사용하여 자격 증명에 대한 IAM 정책 및 역할을 생성합니다.

계정에 자격 증명을 수동으로 추가합니다

Workload Factory에 AWS 자격 증명을 수동으로 추가하여 Workload Factory 계정에 고유한 워크로드를 실행하는 데 사용할 AWS 리소스를 관리하는 데 필요한 권한을 부여할 수 있습니다. 추가하는 각 자격 증명 세트에는 사용하려는 워크로드 기능에 따라 하나 이상의 IAM 정책과 계정에 할당된 IAM 역할이 포함됩니다.

Workload Factory 콘솔이나 NetApp 콘솔에서 계정에 AWS 자격 증명을 추가할 수 있습니다.

자격 증명은 세 부분으로 구성됩니다.

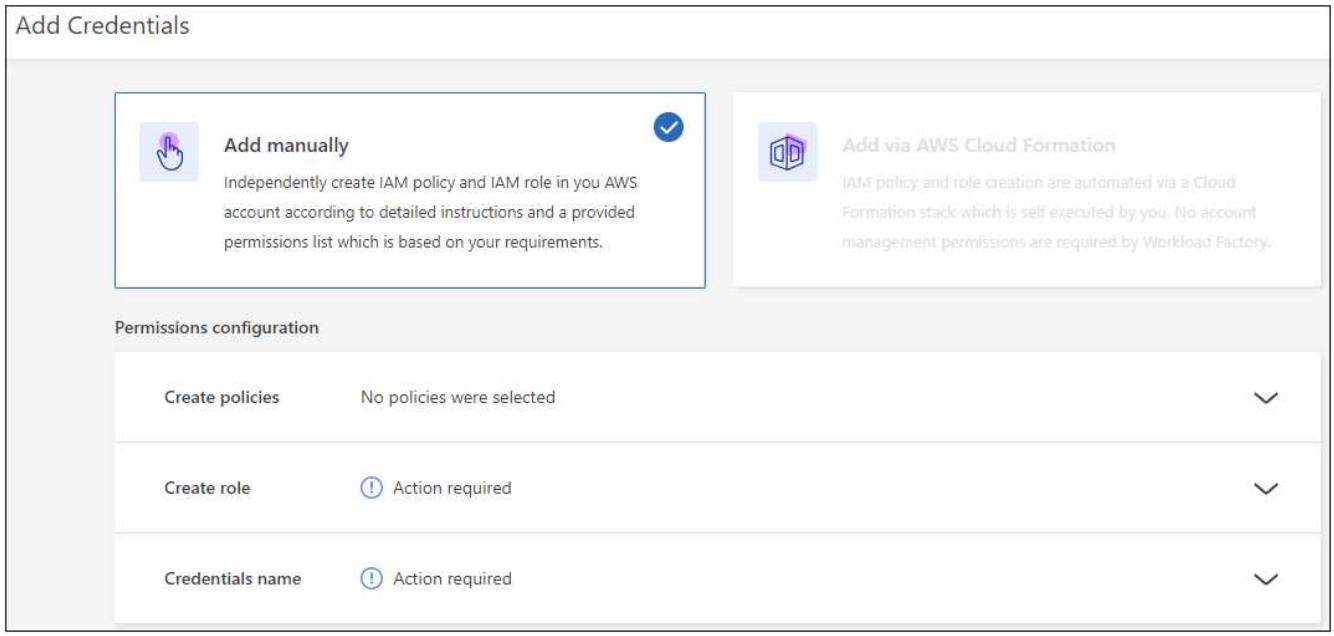
- 사용할 서비스 및 권한 수준을 선택한 다음 AWS Management Console에서 IAM 정책을 생성합니다.
- AWS Management Console에서 IAM 역할을 생성합니다.
- Workload Factory에서 이름을 입력하고 자격 증명을 추가합니다.

시작하기 전에

AWS 계정에 로그인하려면 자격 증명이 필요합니다.

단계

1. 에 로그인하세요 "워크로드 팩토리 콘솔" .
2. 메뉴에서 *관리*를 선택한 다음 *자격 증명*을 선택합니다.
3. 자격 증명 페이지에서 * 자격 증명 추가 * 를 선택합니다.
4. 자격 증명 추가 페이지에서 * 수동으로 추가 * 를 선택한 후 다음 단계에 따라 *Permissions configuration* 아래의 각 섹션을 완료합니다.



1단계**:** 워크로드 기능을 선택하고 **IAM** 정책을 생성합니다

이 섹션에서는 이러한 자격 증명의 일부로 관리할 수 있는 워크로드 기능 유형과 각 워크로드에 대해 사용할 수 있는 권한을 선택합니다. Codebox에서 선택한 각 워크로드에 대한 정책 권한을 복사한 다음 AWS 계정 내의 AWS 관리 콘솔에 추가하여 정책을 생성해야 합니다.

단계

1. Create policies * 섹션에서 자격 증명에 포함할 각 워크로드 기능을 활성화합니다.

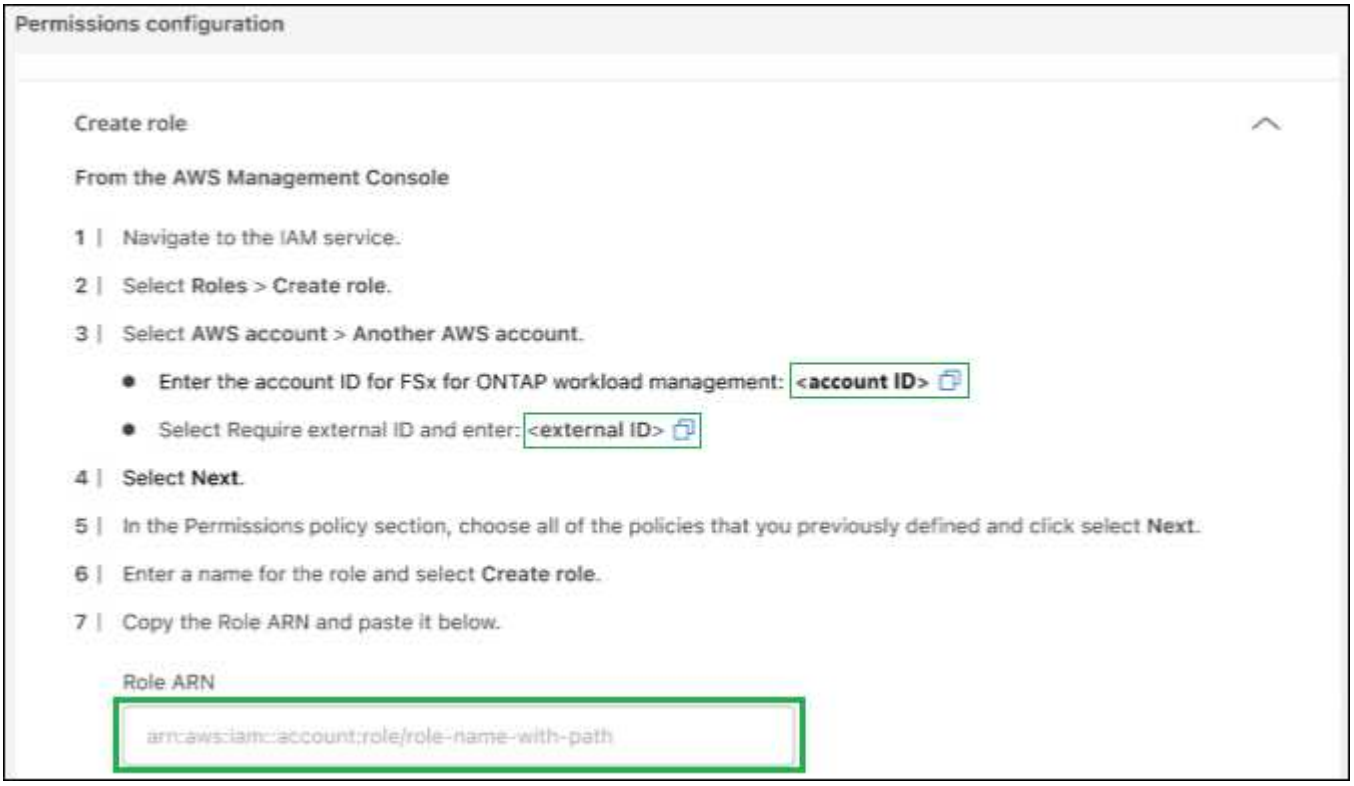
   나중에 기능을 추가할 수 있으므로 현재 배포 및 관리하려는 워크로드를 선택하기만 하면 됩니다.

2. 권한 수준(읽기 전용 또는 읽기/쓰기)을 선택할 수 있는 워크로드 기능의 경우, 해당 자격 증명으로 사용할 수 있는 권한 유형을 선택합니다.

3. 선택 사항: * 자동 권한 확인 사용 * 을 선택하여 워크로드 작업을 완료하는 데 필요한 AWS 계정 권한이 있는지 확인하십시오. 검사를 활성화하면 사용 권한 정책에 가 `iam:SimulatePrincipalPolicy permission` 추가됩니다. 이 권한은 사용 권한을 확인하는 용도로만 사용됩니다. 자격 증명을 추가한 후 사용 권한을 제거할 수 있지만 부분적으로 성공한 작업을 위해 리소스가 생성되지 않도록 유지하고 필요한 수동 리소스 정리를 방지하는 것이 좋습니다.
4. 코드박스 창에서 첫 번째 IAM 정책에 대한 권한을 복사합니다.
5. 다른 브라우저 창을 열고 AWS 관리 콘솔에서 AWS 계정에 로그인합니다.
6. IAM 서비스를 열고 * Policies * > * Create Policy * 를 선택합니다.
7. 파일 형식으로 JSON을 선택하고 3단계에서 복사한 권한을 붙여 넣은 후 * 다음 * 을 선택합니다.
8. 정책 이름을 입력하고 * 정책 생성 * 을 선택합니다.
9. 1단계에서 여러 작업 부하 기능을 선택한 경우 이 단계를 반복하여 각 작업 부하 권한 집합에 대한 정책을 만듭니다.

2단계**:** 정책을 사용하는 **IAM** 역할을 생성합니다

이 섹션에서는 Workload Factory가 방금 만든 권한과 정책을 포함하는 IAM 역할을 설정합니다.



단계

1. AWS Management Console에서 * 역할 > 역할 생성 * 을 선택합니다.
2. 신뢰할 수 있는 엔터티 유형 * 에서 * AWS 계정 * 을 선택합니다.
   a. *다른 AWS 계정*을 선택하고 Workload Factory UI에서 FSx for ONTAP 워크로드 관리에 대한 계정 ID를 복사하여 붙여넣습니다.
   b. *필수 외부 ID*를 선택하고 Workload Factory UI에서 외부 ID를 복사하여 붙여넣습니다.
3. 다음 * 을 선택합니다.

4. 권한 정책 섹션에서 이전에 정의한 모든 정책을 선택하고 * 다음 * 을 선택합니다.
5. 역할의 이름을 입력하고 * 역할 생성 * 을 선택합니다.
6. 역할 ARN을 복사합니다.
7. Workload Factory의 자격 증명 추가 페이지로 돌아가서, 권한 구성 아래의 역할 만들기 섹션을 확장하고, 역할 *ARN* 필드에 ARN을 붙여넣습니다.

3단계**:** 이름을 입력하고 자격 증명을 추가합니다

마지막 단계는 Workload Factory에서 자격 증명의 이름을 입력하는 것입니다.

단계

1. Workload Factory의 자격 증명 추가 페이지에서 권한 구성 아래의 *자격 증명 이름*을 확장합니다.
2. 이러한 자격 증명에 사용할 이름을 입력합니다.
3. Add * 를 선택하여 자격 증명을 생성합니다.

결과

자격 증명이 생성되고 자격 증명 페이지로 돌아갑니다.

CloudFormation을 사용하여 계정에 자격 증명을 추가합니다

AWS CloudFormation 스택을 사용하여 Workload Factory에 AWS 자격 증명을 추가할 수 있습니다. 사용하려는 Workload Factory 기능을 선택한 다음 AWS 계정에서 AWS CloudFormation 스택을 시작합니다. CloudFormation은 선택한 워크로드 기능에 따라 IAM 정책과 IAM 역할을 생성합니다.

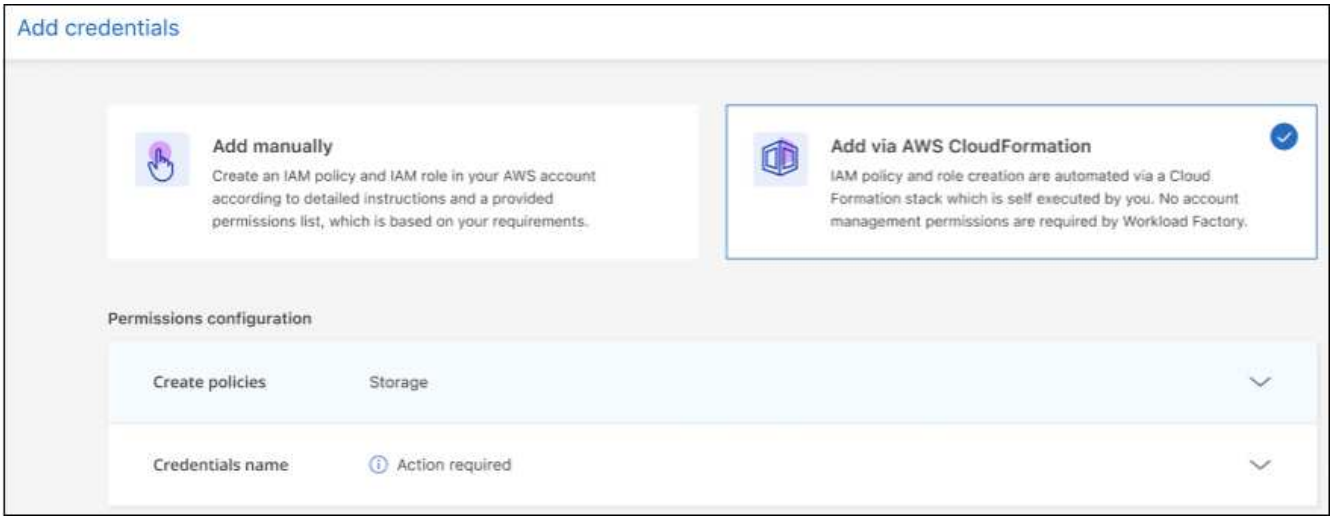
시작하기 전에

- AWS 계정에 로그인하려면 자격 증명이 필요합니다.
- CloudFormation 스택을 사용하여 자격 증명을 추가할 때 AWS 계정에 다음 권한이 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

단계

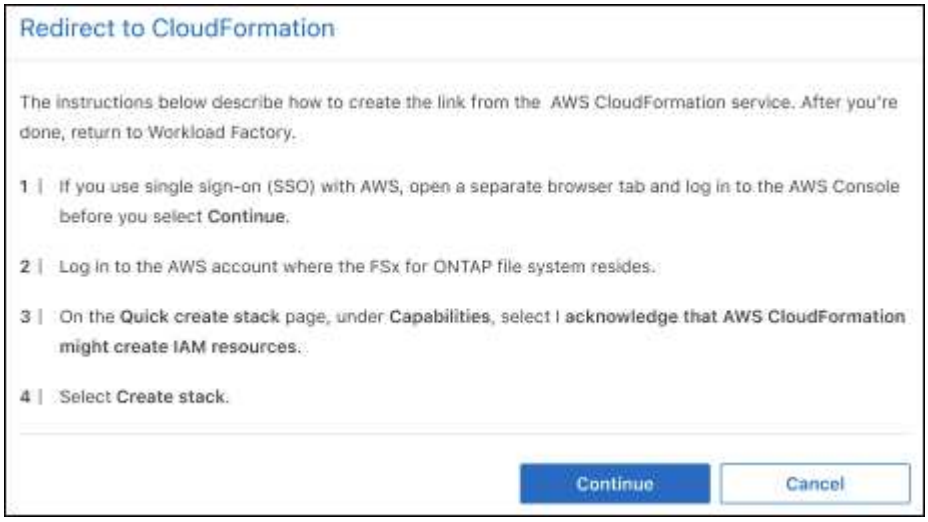
1. 에 로그인하세요 "워크로드 팩토리 콘솔" .
2. 메뉴에서 *관리*를 선택한 다음 *자격 증명*을 선택합니다.
3. 자격 증명 페이지에서 * 자격 증명 추가 * 를 선택합니다.
4. Add via AWS CloudFormation * 을 선택합니다.



5. Create policies * 에서 이러한 자격 증명에 포함할 각 워크로드 기능을 활성화하고 각 워크로드에 대한 권한 수준을 선택합니다.

   나중에 기능을 추가할 수 있으므로 현재 배포 및 관리하려는 워크로드를 선택하기만 하면 됩니다.

6. 선택 사항: * 자동 권한 확인 사용 * 을 선택하여 워크로드 작업을 완료하는 데 필요한 AWS 계정 권한이 있는지 확인하십시오. 검사를 사용하면 `iam:SimulatePrincipalPolicy` 사용 권한 정책에 사용 권한이 추가됩니다. 이 권한은 사용 권한을 확인하는 용도로만 사용됩니다. 자격 증명을 추가한 후 사용 권한을 제거할 수 있지만 부분적으로 성공한 작업을 위해 리소스가 생성되지 않도록 유지하고 필요한 수동 리소스 정리를 방지하는 것이 좋습니다.
7. 자격 증명 이름 * 에 자격 증명에 사용할 이름을 입력합니다.
8. AWS CloudFormation에서 자격 증명 추가:
   a. 추가 * 를 선택하거나 * CloudFormation으로 리디렉션 * 을 선택하면 CloudFormation으로 리디렉션 페이지가 표시됩니다.



   b. AWS에서 SSO(Single Sign-On)를 사용하는 경우 * Continue * 를 선택하기 전에 별도의 브라우저 탭을 열고 AWS 콘솔에 로그인합니다.

      FSx for ONTAP 파일 시스템이 상주하는 AWS 계정에 로그인해야 합니다.

c. CloudFormation으로 이동 페이지에서 * 계속 * 을 선택합니다.

d. 빠른 스택 만들기 페이지의 기능 에서 * AWS CloudFormation이 IAM 리소스를 생성할 수 있음을 확인합니다 * 를 선택합니다.

e. Create stack * 을 선택합니다.

f. Workload Factory로 돌아가서 자격 증명 페이지를 모니터링하여 새 자격 증명이 진행 중인지 또는 추가되었는지 확인합니다.

NetApp Workload Factory로 워크로드 최적화

로그인하고 NetApp Workload Factory를 설정한 후에는 Amazon FSx for ONTAP 파일 시스템 생성, FSx for ONTAP 파일 시스템에 데이터베이스 배포, FSx for ONTAP 파일 시스템을 외부 데이터 저장소로 사용하여 가상 머신 구성을 AWS의 VMware Cloud로 마이그레이션하는 등 여러 가지 ONTAP Factory 기능을 사용할 수 있습니다.

- "NetApp ONTAP용 Amazon FSx"

  FSx for ONTAP을 스토리지 인프라로 사용하여 현재 데이터 목록을 평가하고 분석하여 잠재적인 비용 절감을 실현하십시오. 또한, 모범 사례를 기준으로 FSx for ONTAP 배포를 프로비저닝 및 템플릿 화하고, 고급 관리 기능에 액세스할 수 있습니다.

- "데이터베이스 워크로드"

  AWS에서 기존 데이터베이스 자산을 감지하고, FSx for ONTAP로 전환하여 잠재적 비용 절감을 평가하고, 최적화를 위한 내장 모범 사례를 통해 데이터베이스를 엔드 투 엔드 로 구축하고, CI/CD 파이프라인을 위한 씬 클로닝을 자동화합니다.

- "제나이주식회사"

  RAG(Retrieval-Augmented Generation) 인프라를 배포 및 관리하여 AI 애플리케이션의 정확성과 고유성을 개선합니다. 기본 제공 데이터 보안 및 규정 준수를 통해 FSx for ONTAP에 대한 지식 기반을 구축하십시오.

- "VMware 워크로드"

  스마트 권장사항과 자동 개선 기능을 통해 마이그레이션 및 운영을 간소화합니다. 효율적인 백업 및 강력한 재해 복구 솔루션 구축 VM을 모니터링하고 문제를 해결합니다.

워크로드 팩토리 관리

NetApp Workload Factory에 로그인하세요

NetApp Workload Factory에 가입한 후 언제든지 웹 기반 콘솔에서 로그인하여 워크로드와 FSx for ONTAP 파일 시스템을 관리할 수 있습니다.

이 작업에 대해

다음 옵션 중 하나를 사용하여 Workload Factory 웹 기반 콘솔에 로그인할 수 있습니다.

- 기존 NetApp Support 사이트(NSS) 자격 증명
- 이메일 주소 및 암호를 사용하여 NetApp 클라우드 로그인

단계

1. 웹 브라우저를 열고 이동하세요 "워크로드 팩토리 콘솔" .
2. 로그인 * 페이지에서 로그인과 관련된 이메일 주소를 입력합니다.
3. 로그인과 관련된 인증 방법에 따라 자격 증명을 입력하라는 메시지가 표시됩니다.
   - NetApp 클라우드 자격 증명: 암호를 입력합니다
   - 통합 사용자: 통합 ID 자격 증명을 입력합니다
   - NetApp Support 사이트 계정: NetApp Support 사이트 자격 증명을 입력합니다
4. 로그인 * 을 선택합니다.

   이전에 성공적으로 로그인한 적이 있다면 Workload Factory 홈페이지가 나타나고 기본 계정을 사용하게 됩니다.

   처음 로그인하는 경우 * 계정 * 페이지로 연결됩니다.

   - 단일 계정의 구성원인 경우 * 계속 * 을 선택합니다.
   - 여러 계정의 구성원인 경우 계정을 선택하고 * 계속 * 을 선택합니다.

결과

이제 로그인하여 Workload Factory를 사용하여 FSx for ONTAP 파일 시스템과 워크로드를 관리할 수 있습니다.

서비스 계정을 관리합니다

서비스 계정을 생성하여 인프라 운영을 자동화하는 시스템 사용자 역할을 수행합니다. 언제든지 서비스 계정에 대한 액세스를 취소하거나 변경할 수 있습니다.

이 작업에 대해

서비스 계정은 NetApp 에서 제공하는 다중 테넌시 기능입니다. 계정 관리자는 서비스 계정을 생성하고, 액세스를 제어하고, 서비스 계정을 삭제합니다. NetApp 콘솔이나 NetApp Workload Factory 콘솔에서 서비스 계정을 관리할 수 있습니다.

클라이언트 비밀번호를 다시 생성할 수 있는 NetApp 콘솔에서 서비스 계정을 관리하는 것과 달리, Workload Factory는 서비스 계정의 생성과 삭제만 지원합니다. NetApp Workload Factory 콘솔에서 특정 서비스 계정에 대한 클라이언트

비밀번호를 다시 생성하려면 다음이 필요합니다.서비스 계정을 삭제합니다 , 그런 다음새 계정을 만듭니다 .

서비스 계정은 암호 대신 클라이언트 ID와 암호를 인증에 사용합니다. 계정 관리자가 클라이언트 ID 및 암호를 변경하기로 결정할 때까지 클라이언트 ID 및 암호가 고정됩니다. 서비스 계정을 사용하려면 액세스 토큰을 생성하려면 클라이언트 ID와 암호가 필요합니다. 그렇지 않으면 액세스 권한을 얻을 수 없습니다. 액세스 토큰은 수명이 짧고 몇 시간 동안만 사용할 수 있다는 점에 유의하십시오.

시작하기 전에

NetApp 콘솔이나 Workload Factory 콘솔에서 서비스 계정을 만들지 여부를 결정합니다. 약간의 차이가 있습니다. 다음 지침에서는 Workload Factory 콘솔에서 서비스 계정을 관리하는 방법을 설명합니다.

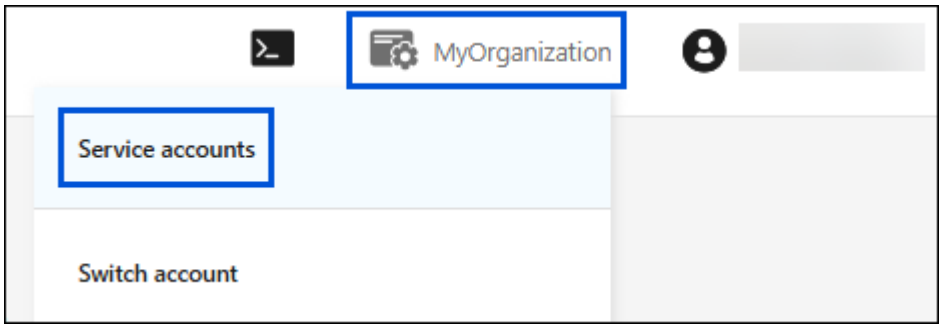
NetApp 콘솔에서 서비스 계정을 관리하려면"ID 및 액세스 관리가 작동하는 방식을 알아보세요" 그리고"IAM 멤버를 추가하고 권한을 관리하는 방법을 알아보세요." .

서비스 계정을 생성합니다

서비스 계정을 만들면 Workload Factory를 사용하여 서비스 계정의 클라이언트 ID와 클라이언트 비밀번호를 복사하거나 다운로드할 수 있습니다. 이 키 쌍은 Workload Factory 인증에 사용됩니다.

단계

1. Workload Factory 콘솔에서 * 계정 * 아이콘을 선택하고 * 서비스 계정 * 을 선택합니다.



2. 서비스 계정 * 페이지에서 * 서비스 계정 생성 * 을 선택합니다.
3. 서비스 계정 만들기 대화 상자에서 * 서비스 계정 이름 * 필드에 서비스 계정의 이름을 입력합니다.

   역할 * 은 * 계정 관리자 * 로 미리 선택됩니다.

4. Continue * 를 선택합니다.
5. 클라이언트 ID 및 클라이언트 암호를 복사하거나 다운로드합니다.

   클라이언트 비밀번호는 한 번만 표시되며 Workload Factory의 어디에도 저장되지 않습니다. 비밀을 복사하거나 다운로드하여 안전하게 보관하세요.

6. 선택적으로 클라이언트 자격 증명 교환을 실행하여 Auth0 관리 API에 대한 액세스 토큰을 얻을 수 있습니다. curl 예제는 클라이언트 ID와 비밀번호를 가져와 API를 사용하여 시간 제한이 있는 액세스 토큰을 생성하는 방법을 보여줍니다. 토큰은 NetApp Workload Factory API에 몇 시간 동안 액세스할 수 있는 권한을 제공합니다.
7. 닫기 * 를 선택합니다.

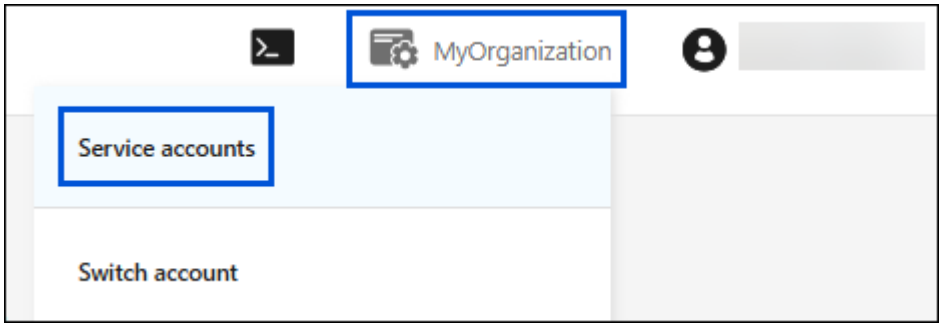
새 서비스 계정이 만들어지고 서비스 계정 페이지에 나열됩니다.

서비스 계정을 삭제합니다

더 이상 사용할 필요가 없는 경우 서비스 계정을 삭제합니다.

단계

1. Workload Factory 콘솔에서 * 계정 * 아이콘을 선택하고 * 서비스 계정 * 을 선택합니다.



2. 서비스 계정 페이지에서 작업 메뉴를 선택한 다음 *삭제*를 선택합니다.
3. 서비스 계정 삭제 대화 상자에서 텍스트 상자에 * DELETE * 를 입력합니다.
4. 삭제를 확인하려면 * 삭제 * 를 선택합니다.

NetApp Workload Factory 알림 구성

NetApp Workload Factory 알림 서비스를 구성하여 NetApp 콘솔이나 Amazon SNS 주제에 알림을 보낼 수 있습니다. 콘솔 에이전트나 링크가 배포된 경우 경고로 전송된 알림은 NetApp 콘솔에 나타납니다. Workload Factory가 Amazon SNS 주제에 알림을 게시하면 해당 주제의 구독자(예: 사람 또는 다른 애플리케이션)는 해당 주제에 대해 구성된 엔드포인트(예: 이메일 또는 SMS 메시지)에서 알림을 받습니다.

알림 유형 및 메시지

Workload Factory는 다음 이벤트에 대한 알림을 보냅니다.

이벤트	설명	알림 유형입니다	심각도입니다	워크로드	리소스 유형
계정의 일부 데이터베이스 인스턴스가 제대로 설계되지 않았습니다.	귀하 계정의 모든 Microsoft SQL Server 인스턴스는 잘 설계된 문제에 대해 분석되었습니다. 이 이벤트에 대한 설명은 잘 설계된 인스턴스와 최적화되지 않은 인스턴스의 수를 제공합니다. Workload Factory 콘솔의 데이터베이스 인벤토리에서 잘 설계된 상태 결과와 권장 사항을 검토합니다.	잘 설계된	권장 사항	데이터베이스를 지원합니다	Microsoft SQL Server 인스턴스
Microsoft SQL Server/PostgreSQL 서버 배포가 성공했습니다.	Microsoft SQL Server 또는 PostgreSQL 호스트 배포가 성공했습니다. 자세한 내용은 작업 모니터링을 참조하세요.	구축	성공	데이터베이스를 지원합니다	ONTAP용 FSx, DB 호스트
Microsoft SQL Server/PostgreSQL 서버 배포에 실패했습니다.	Microsoft SQL Server 또는 PostgreSQL 호스트 배포에 실패했습니다. 자세한 내용은 작업 모니터링을 참조하세요.	구축	오류	데이터베이스를 지원합니다	ONTAP용 FSx, DB 호스트
복제 관계 생성에 실패했습니다.	SnapMirror 복제 관계 생성에 실패했습니다. 자세한 내용은 Tracker를 참조하세요.	복제	비판적인	일반 보관	ONTAP 용 FSx
ONTAP 생성 실패를 위한 FSx	FSx for ONTAP 파일 시스템 생성 프로세스가 실패했습니다. 자세한 내용은 Tracker를 참조하세요.	FSx for ONTAP 파일 시스템 작업	비판적인	일반 보관	ONTAP 용 FSx

이벤트	설명	알림 유형입니다	심각도입니다	워크로드	리소스 유형
FSx for ONTAP 문제가 감지되었습니다.	모든 FSx for ONTAP 파일 시스템은 잘 설계된 문제에 대해 분석되었습니다. 검사 결과 하나 이상의 문제가 감지되었습니다. 자세한 내용은 Workload Factory 콘솔의 Storage 대시보드에서 잘 설계된 분석을 검토하세요.	잘 설계된 분석	권장 사항	일반 보관	ONTAP 파일 시스템용 FSx

Workload Factory 알림 구성

NetApp 콘솔이나 Workload Factory 콘솔을 사용하여 Workload Factory 알림을 구성합니다. NetApp 콘솔을 사용하는 경우 Workload Factory를 구성하여 NetApp 콘솔이나 Amazon SNS 주제로 알림을 보낼 수 있습니다. NetApp 콘솔의 *알림 설정*에서 알림을 구성할 수 있습니다.

시작하기 전에

- Amazon SNS 콘솔이나 AWS CLI를 사용하여 Amazon SNS를 구성하고 Amazon SNS 주제를 생성해야 합니다.
- Workload Factory는 표준 주제 유형을 지원합니다. 이 유형의 주제에서는 알림이 수신 순서대로 구독자에게 전송되지 않으므로 중요하거나 긴급한 알림이 있는 경우 이 점을 고려하세요.

NetApp 콘솔에서 알림 구성

단계

1. 에 로그인하세요"NetApp 콘솔" .
2. NetApp 콘솔 메뉴에서 워크로드, 관리, *알림 설정*을 차례로 선택합니다.
3. 알림 설정 페이지에서 다음을 수행하세요.
   a. 선택 사항: NetApp 콘솔에서 알림을 보내도록 Workload Factory를 구성하려면 * NetApp 콘솔 알림 사용*을 선택합니다.
   b. *SNS 알림 사용*을 선택하세요.
   c. Amazon SNS 콘솔에서 Amazon SNS를 구성하려면 지침을 따르세요.

      주제를 만든 후 주제 ARN을 복사하여 알림 설정 페이지의 **SNS** 주제 **ARN** 필드에 입력합니다.
4. 테스트 알림을 보내 구성을 확인한 후 *적용*을 선택합니다.

결과

Workload Factory는 사용자가 지정한 Amazon SNS 주제에 알림을 보내도록 구성되었습니다.

Workload Factory 콘솔에서 알림 구성

단계

1. 에 로그인하세요"워크로드 팩토리 콘솔" .
2. Workload Factory 콘솔 메뉴에서 워크로드, 관리, *알림 설정*을 차례로 선택합니다.
3. *SNS 알림 사용*을 선택하세요.
4. Amazon SNS 콘솔에서 Amazon SNS를 구성하려면 지침을 따르세요.
5. 테스트 알림을 보내 구성을 확인한 후 *적용*을 선택합니다.

결과

Workload Factory는 사용자가 지정한 Amazon SNS 주제에 알림을 보내도록 구성되었습니다.

Amazon SNS 주제 구독하기

Workload Factory를 구성하여 주제에 알림을 보낸 후 다음을 따르세요. "지침" Workload Factory에서 알림을 받을 수 있도록 Amazon SNS 설명서에서 주제를 구독하세요.

알림을 필터링합니다

알림에 필터를 적용하면 불필요한 알림 트래픽을 줄이고 특정 사용자를 대상으로 특정 알림 유형을 타겟팅할 수 있습니다. SNS 알림에 대한 Amazon SNS 정책을 사용하고 NetApp 콘솔의 알림 설정을 사용하여 이 작업을 수행할 수 있습니다.

Amazon SNS 알림 필터링

Amazon SNS 주제를 구독하면 기본적으로 해당 주제에 게시된 모든 알림을 받게 됩니다. 해당 주제의 특정 알림만 받으려면 필터 정책을 사용하여 받을 알림을 제어할 수 있습니다. 필터 정책을 사용하면 Amazon SNS가 필터 정책과

일치하는 알림만 구독자에게 전달합니다.

다음 기준으로 Amazon SNS 알림을 필터링할 수 있습니다.

설명	필터 정책 필드 이름	가능한 값
리소스 유형	`resourceType`	• `DB` • `Microsoft SQL Server host` • `PostgreSQL Server host`
워크로드	`workload`	`WLMDB`
우선 사항	`priority`	• `Success` • `Info` • `Recommendation` • `Warning` • `Error` • `Critical`
알림 유형입니다	`notificationType`	• `Deployment` • `Well-architected`

단계

1. Amazon SNS 콘솔에서 SNS 주제에 대한 구독 세부 정보를 편집합니다.
2. 구독 필터 정책 영역에서 *메시지 속성*으로 필터링하도록 선택합니다.
3. 구독 필터 정책 옵션을 활성화합니다.
4. **JSON** 편집기 상자에 JSON 필터 정책을 입력합니다.

   예를 들어, 다음 JSON 필터 정책은 WLMDB 작업 부하와 관련된 Microsoft SQL Server 리소스의 알림을 수락하고, 성공 또는 오류의 우선순위를 가지며, Well-architected 상태에 대한 세부 정보를 제공합니다.

```
{
  "accountId": [
    "account-a"
  ],
  "resourceType": [
    "Microsoft SQL Server host"
  ],
  "workload": [
    "WLMDB"
  ],
  "priority": [
    "Success",
    "Error"
  ],
  "notificationType": [
    "Well-architected"
  ]
}
```

5. *변경 사항 저장*을 선택하세요.

필터 정책의 다른 예는 다음을 참조하세요. "Amazon SNS 필터 정책 예시" .

필터 정책 생성에 대한 자세한 내용은 다음을 참조하세요. "아마존 SNS 문서" .

NetApp 콘솔에서 알림 필터링

NetApp 콘솔 알림 설정을 사용하면 콘솔에서 받는 알림을 중요, 정보, 경고 등의 심각도 수준에 따라 필터링할 수 있습니다.

콘솔에서 알림 필터링에 대한 자세한 내용은 다음을 참조하세요. "NetApp 콘솔 설명서" .

코드박스를 사용하여 작업을 자동화합니다

코드박스 자동화에 대해 알아보십시오

Codebox는 개발자와 DevOps가 NetApp Workload Factory에서 지원하는 모든 작업을 실행하는 데 필요한 코드를 생성하는 데 도움이 되는 Infrastructure as Code(IaC) 공동 파일럿입니다. Codebox는 Workload Factory 운영 모드(기본, 읽기 전용, 읽기/쓰기)에 맞춰 조정되며 실행 준비에 대한 명확한 경로를 설정하는 동시에 빠른 향후 재사용을 위한 자동화 카탈로그를 제공합니다.

코드박스 기능

Codebox는 두 가지 주요 IAC 기능을 제공합니다.

- _Codebox 뷰어 _ 는 그래픽 마법사 또는 대화 채팅 인터페이스에서 항목과 선택을 일치시켜 특정 작업 흐름 작업에 의해 생성되는 IAC를 표시합니다. Codebox 뷰어는 간편한 탐색 및 분석을 위해 색상 코딩을 지원하지만, 자동화 카탈로그에 코드를 복사하거나 저장하는 것은 허용되지 않습니다.
- *Codebox Automation Catalog* 저장된 모든 IAC 작업을 표시하여 나중에 사용할 수 있도록 쉽게 참조할 수 있습니다. 자동화 카탈로그 작업은 템플릿으로 저장되고 적용되는 리소스의 컨텍스트로 표시됩니다.

또한 Workload Factory 자격 증명을 설정할 때 Codebox는 IAM 정책을 만드는 데 필요한 AWS 권한을 동적으로 표시합니다. 사용하려는 각 Workload Factory 기능(데이터베이스, AI, FSx for ONTAP 등)에 대한 권한이 제공되며, 정책 사용자에게 읽기 전용 권한이 주어지는지 또는 전체 읽기/쓰기 권한이 주어지는지에 따라 사용자 지정됩니다. Codebox에서 권한을 복사한 다음 AWS Management Console에 붙여넣으면 Workload Factory가 워크로드를 관리할 수 있는 올바른 권한을 갖게 됩니다.

지원되는 코드 형식

지원되는 코드 형식은 다음과 같습니다.

- 워크로드 팩토리 REST API
- AWS CLI를 참조하십시오
- AWS CloudFormation 을 참조하십시오

관련 정보

"Codebox 사용 방법에 대해 알아봅니다"..

"Workload Factory REST API 문서" .

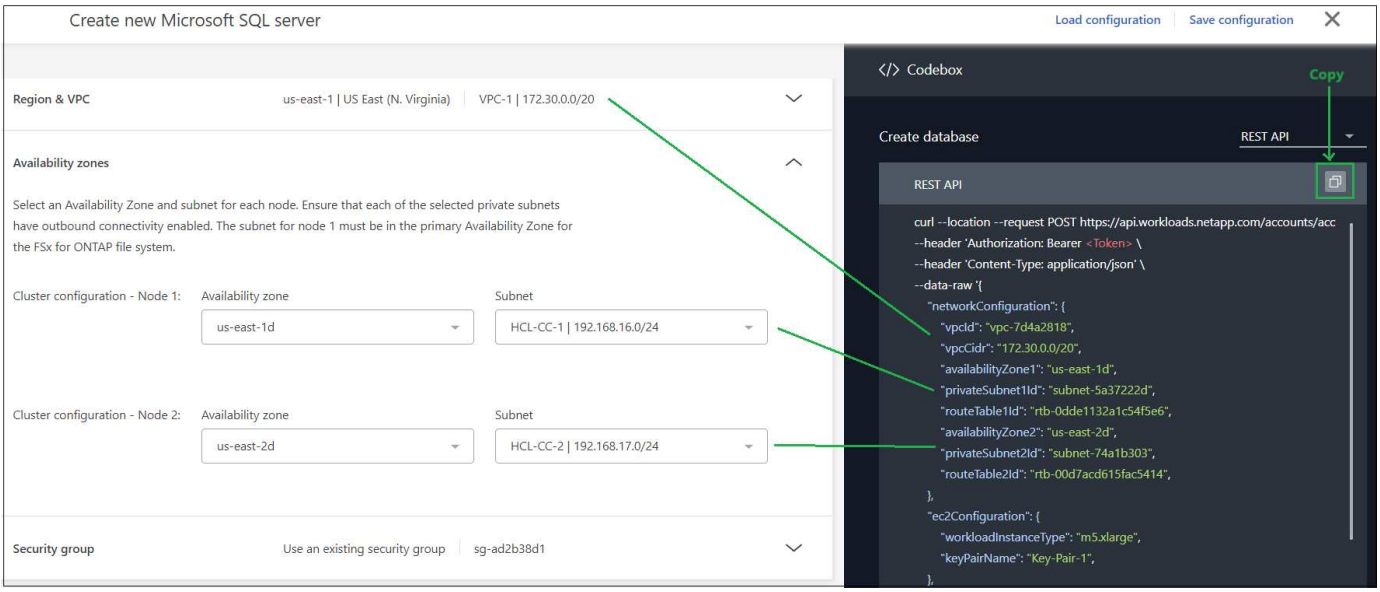
NetApp Workload Factory에서 자동화를 위해 Codebox 사용

Codebox를 사용하면 NetApp Workload Factory에서 지원하는 모든 작업을 실행하는 데 필요한 코드를 생성할 수 있습니다. Workload Factory REST API, AWS CLI, AWS CloudFormation을 사용하여 사용 및 실행할 수 있는 코드를 생성할 수 있습니다.

Codebox는 각 사용자의 Workload Factory 계정에서 제공된 AWS 권한에 따라 코드에 적절한 데이터를 채워 Workload Factory 운영 모드(기본, 읽기 전용, 읽기/쓰기)에 맞춰 조정됩니다. 이 코드는 누락된 정보(예: 자격 증명)를 채우거나 코드를 실행하기 전에 특정 데이터를 사용자 지정할 수 있는 템플릿처럼 사용할 수 있습니다.

코드박스 사용 방법

Workload Factory UI 마법사에 값을 입력하면 각 필드를 완료할 때마다 Codebox에서 데이터가 업데이트되는 것을 볼 수 있습니다. 마법사를 완료한 후 페이지 하단의 만들기 버튼을 선택하기 전에 다음을 선택하세요. 구성을 빌드하는 데 필요한 코드를 캡처하려면 Codebox에 복사하세요. 예를 들어, 새로운 Microsoft SQL Server를 만드는 이 스크린샷은 VPC 및 가용성 영역에 대한 마법사 항목과 REST API 구현에 대한 Codebox의 해당 항목을 보여줍니다.



일부 코드 형식의 경우 다운로드 버튼을 선택하여 코드를 파일에 저장한 다음 다른 시스템으로 가져올 수도 있습니다. 필요한 경우, 코드를 다운로드한 후 편집하여 다른 AWS 계정에 맞게 조정할 수 있습니다.

Codebox에서 **CloudFormation** 코드를 사용합니다

Codebox에서 생성된 CloudFormation 코드를 복사한 다음 AWS 계정에서 Amazon Web Services CloudFormation 스택을 시작할 수 있습니다. CloudFormation은 Workload Factory UI에서 정의한 작업을 수행합니다.

CloudFormation 코드를 사용하는 단계는 FSx for ONTAP 파일 시스템을 배포하는지, 계정 자격 증명을 생성하는지, 기타 Workload Factory 작업을 수행하는지에 따라 다를 수 있습니다.

CloudFormation에서 생성된 YAML 파일 내의 코드는 보안상의 이유로 7일 후에 만료됩니다.

시작하기 전에

- AWS 계정에 로그인하려면 자격 증명이 필요합니다.
- CloudFormation 스택을 사용하려면 다음 사용자 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:UpdateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeChangeSet",
                "cloudformation:ExecuteChangeSet",
                "cloudformation:ListStacks",
                "cloudformation:ListStackResources",
                "cloudformation:GetTemplate",
                "cloudformation:ValidateTemplate",
                "lambda:InvokeFunction",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:UpdateAssumeRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

단계

1. Workload Factory 콘솔을 사용하여 수행하려는 작업을 정의한 후 Codebox에 코드를 복사합니다.
2. Redirect to CloudFormation * 을 선택하면 CloudFormation으로 리디렉션 페이지가 표시됩니다.
3. 다른 브라우저 창을 열고 AWS 관리 콘솔에 로그인합니다.
4. CloudFormation으로 이동 페이지에서 * 계속 * 을 선택합니다.
5. 코드를 실행할 AWS 계정에 로그인합니다.
6. 빠른 스택 만들기 페이지의 기능 에서 * AWS CloudFormation이… * 을 선택합니다.
7. Create stack * 을 선택합니다.
8. AWS 또는 Workload Factory에서 진행 상황을 모니터링합니다.

코드박스의 **REST API** 코드를 사용합니다

Codebox에서 생성된 Workload Factory REST API를 사용하여 FSx for ONTAP 파일 시스템 및 기타 AWS 리소스를 배포하고 관리할 수 있습니다.

curl을 지원하고 인터넷에 연결된 모든 호스트에서 API를 실행할 수 있습니다.

인증 토큰은 Codebox에서 숨겨지지만 API 호출을 복사하여 붙여 넣으면 채워집니다.

단계

1. Workload Factory 콘솔을 사용하여 수행하려는 작업을 정의한 후 Codebox에서 API 코드를 복사합니다.
2. 코드를 붙여 넣고 호스트 시스템에서 실행합니다.

코드박스에서 **AWS CLI** 코드를 사용합니다

Codebox에서 생성된 Amazon Web Services CLI를 사용하여 FSx for ONTAP 파일 시스템 및 기타 AWS 리소스를 구축하고 관리할 수 있습니다.

단계

1. Workload Factory 콘솔을 사용하여 수행하려는 작업을 정의한 후 Codebox에 AWS CLI를 복사합니다.
2. 다른 브라우저 창을 열고 AWS 관리 콘솔에 로그인합니다.
3. 코드를 붙여 넣고 실행합니다.

코드박스에서 **Terraform**을 사용합니다

Terraform을 사용하여 FSx for ONTAP 파일 시스템 및 기타 AWS 리소스를 구축하고 관리할 수 있습니다.

시작하기 전에

- Terraform이 설치된 시스템(Windows/Mac/Linux)이 필요합니다.
- AWS 계정에 로그인하려면 자격 증명이 필요합니다.

단계

1. Workload Factory 콘솔을 사용하여 수행하려는 작업을 정의한 후 Codebox에서 Terraform 코드를 다운로드합니다.
2. 다운로드한 스크립트 아카이브를 Terraform이 설치된 시스템에 복사합니다.
3. zip 파일의 압축을 풀고 README.MD 파일의 단계를 따릅니다.

NetApp Workload Factory에서 CloudShell 사용

NetApp Workload Factory 콘솔의 어느 곳에서나 AWS 또는 ONTAP CLI 명령을 실행하려면 CloudShell을 엽니다.

이 작업에 대해

CloudShell을 사용하면 Workload Factory 콘솔 내에서 셸과 같은 환경에서 AWS CLI 명령이나 ONTAP CLI 명령을 실행할 수 있습니다. 브라우저에서 터미널 세션을 시뮬레이션하여 터미널 기능을 제공하고 Workload Factory의 백엔드를 통해 메시지를 프록시합니다. NetApp 계정에서 제공한 AWS 자격 증명과 ONTAP 자격 증명을 사용할 수

있습니다.

CloudShell의 기능은 다음과 같습니다.

- 여러 CloudShell 세션: 한 번에 여러 CloudShell 세션을 배포하여 여러 명령 시퀀스를 병렬로 실행합니다.
- 다중 보기: CloudShell 탭 세션을 분할하여 두 개 이상의 탭을 동시에 가로 또는 세로로 볼 수 있습니다
- 세션 이름 바꾸기: 필요에 따라 세션 이름을 바꿉니다
- 마지막 세션 콘텐츠 지속성: 실수로 세션을 닫은 경우 마지막 세션을 다시 엽니다
- 설정 환경 설정: 글꼴 크기 및 출력 유형을 변경합니다
- ONTAP CLI 명령에 대한 AI에서 생성된 오류 응답
- 자동 완성 지원: 명령 입력을 시작하고 * TAB * 키를 사용하여 사용 가능한 옵션을 봅니다

CloudShell 명령

CloudShell GUI 인터페이스 내에서 를 `help` 입력하여 사용 가능한 CloudShell 명령을 볼 수 있습니다. `help`명령을 실행하면 다음과 같은 참조가 나타납니다.

설명

NetApp CloudShell은 NetApp Workload Factory에 내장된 GUI 인터페이스로, 셸과 유사한 환경에서 AWS CLI 명령이나 ONTAP CLI 명령을 실행할 수 있습니다. Workload Factory의 백엔드를 통해 터미널 기능을 제공하고 메시지를 프록시하여 브라우저에서 터미널 세션을 시뮬레이션합니다. NetApp 계정에서 제공한 AWS 자격 증명과 ONTAP 자격 증명을 사용할 수 있습니다.

사용 가능한 명령

- `clear`
- `help`
- `[--fsx <fsxId>] <ontap-command> [parameters]`
- `aws <aws-command> <aws-sub-command> [parameters]`

상황

각 터미널 세션은 자격 증명, 지역 및 선택적으로 FSx for ONTAP 파일 시스템과 같은 특정 컨텍스트에서 실행됩니다.

+ 모든 AWS 명령은 제공된 컨텍스트에서 실행됩니다. AWS 명령은 제공된 자격 증명에 지정된 지역에서 권한이 있는 경우에만 성공합니다.

+ ONTAP 명령을 선택적으로 지정할 수 있습니다. `fsxId` . 당신이 제공하는 경우 `fsxId` 개별 ONTAP 명령을 사용하는 경우 이 ID는 컨텍스트의 ID를 재정의합니다. 터미널 세션에 FSx for ONTAP 파일 시스템 ID 컨텍스트가 없는 경우 다음을 제공해야 합니다. `fsxId` 각 ONTAP 명령과 함께.

+ 다양한 컨텍스트 세부 사항을 업데이트하려면 다음을 수행합니다. * 자격 증명을 변경하려면: "using credentials <credentialId>" * 지역을 변경하려면: "using region <regionCode>" * ONTAP 파일 시스템에 대한 FSx를 변경하려면: "using fsx <fileSystemId>"

항목 표시

- 사용 가능한 자격 증명을 표시하려면 "자격 증명 표시"
- 사용 가능한 지역 표시하기: "지역 표시"

- 명령 히스토리를 표시하려면: "show history"

변수

다음은 변수를 설정하고 사용하는 예제입니다. 변수 값에 공백이 포함된 경우 따옴표 안에 값을 설정해야 합니다.

+ * 변수를 설정하려면: $<변수> = <값> * 변수를 사용하려면: $<변수> * 변수 설정 예: $svm1 = svm123 * 변수 사용 예: --fsx FileSystem-1 volumes show --vserver $svm1 * 문자열 값으로 변수를 설정하는 예 $comment1 = "공백이 있는 주석"

연산자

파이프, 백그라운드 실행 `&`, 리디렉션 > 등의 셸 연산자는 `|` 지원되지 않습니다. 이러한 연산자를 포함하면 명령 실행이 실패합니다.

시작하기 전에

CloudShell은 AWS 자격 증명의 컨텍스트에서 작동합니다. CloudShell을 사용하려면 하나 이상의 AWS 자격 증명을 제공해야 합니다.

> CloudShell은 모든 AWS 또는 ONTAP CLI 명령을 실행할 수 있습니다. 하지만 FSx for ONTAP 파일 시스템 내에서 작업하려면 다음 명령을 실행해야 합니다 `using fsx <file-system-name>`.

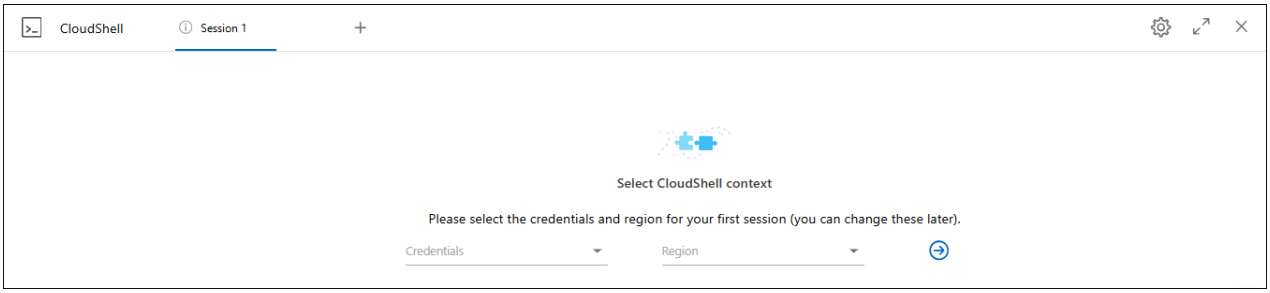
CloudShell 구축

NetApp Workload Factory 콘솔의 어느 곳에서나 CloudShell을 배포할 수 있습니다. NetApp 콘솔에서 CloudShell을 배포할 수도 있습니다.

Workload Factory 콘솔에서 배포

단계

1. 에 로그인하세요 "워크로드 팩토리 콘솔" .
2. 메뉴에서 *관리*를 선택한 다음 *CloudShell*을 선택합니다.
3. CloudShell 창에서 CloudShell 세션의 자격 증명과 지역을 선택한 다음 화살표를 선택하여 계속합니다.



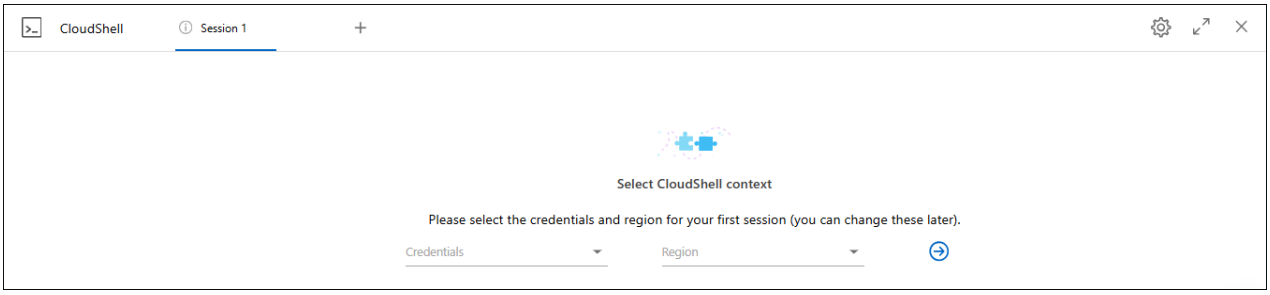
4. 를 입력하여 `help` 사용 가능한 CloudShell 명령지침 및 지침을 확인하거나 다음 CLI 참조 문서에서 사용 가능한 명령을 참조하십시오.
   - "AWS CLI 참조": FSx for ONTAP와 관련된 명령의 경우 * FSX * 를 선택하십시오.
   - "ONTAP CLI 참조입니다"
5. CloudShell 세션 내에서 명령을 실행합니다.

   ONTAP CLI 명령을 실행한 후 오류가 발생하면 전구 아이콘을 선택하여 장애의 설명, 장애의 원인 및 자세한 해결책이 포함된 간단한 AI 생성 오류 응답을 확인하십시오. 자세한 내용을 보려면 * 자세히 보기 * 를 선택하십시오.

NetApp 콘솔에서 배포

단계

1. 에 로그인하세요"NetApp 콘솔" .
2. 메뉴에서 *작업 부하*를 선택한 다음 *관리*를 선택합니다.
3. 관리 메뉴에서 *CloudShell*을 선택합니다.
4. CloudShell 창에서 CloudShell 세션의 자격 증명과 지역을 선택한 다음 화살표를 선택하여 계속합니다.



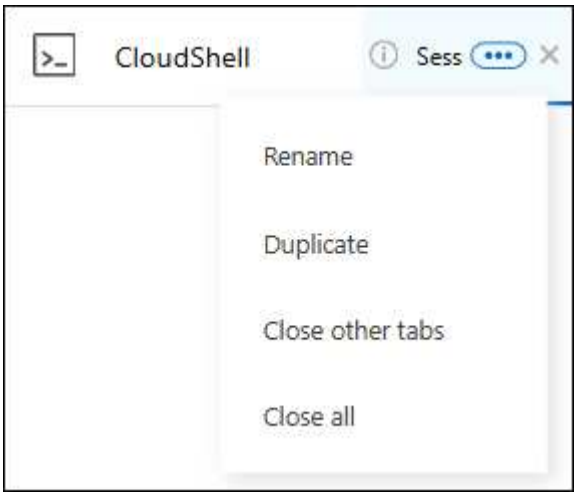
5. 를 입력하여 `help` 사용 가능한 CloudShell 명령 및 지침을 확인하거나 다음 CLI 참조 문서에서 사용 가능한 명령을 참조하십시오.
   - "AWS CLI 참조": FSx for ONTAP와 관련된 명령의 경우 * FSX * 를 선택하십시오.

- "ONTAP CLI 참조입니다"

6. CloudShell 세션 내에서 명령을 실행합니다.

   ONTAP CLI 명령을 실행한 후 오류가 발생하면 전구 아이콘을 선택하여 장애의 설명, 장애의 원인 및 자세한 해결책이 포함된 간단한 AI 생성 오류 응답을 확인하십시오. 자세한 내용을 보려면 * 자세히 보기 * 를 선택하십시오.

이 스크린샷에 표시된 CloudShell 작업은 열려 있는 CloudShell 세션 탭의 작업 메뉴를 선택하여 완료할 수 있습니다. 각 작업에 대한 지침은 다음과 같습니다.



CloudShell 세션 탭의 이름을 변경합니다

CloudShell 세션 탭의 이름을 변경하여 세션을 쉽게 식별할 수 있습니다.

단계

1. CloudShell 세션 탭의 작업 메뉴를 선택합니다.
2. 이름 바꾸기 * 를 선택합니다.
3. 세션 탭의 새 이름을 입력한 다음 탭 이름 바깥쪽을 클릭하여 새 이름을 설정합니다.

결과

CloudShell 세션 탭에 새 이름이 나타납니다.

중복된 CloudShell 세션 탭

CloudShell 세션 탭을 복제하여 이름, 자격 증명 및 지역이 동일한 새 세션을 만들 수 있습니다. 원본 탭의 코드가 복제된 탭에 중복되지 않습니다.

단계

1. CloudShell 세션 탭의 작업 메뉴를 선택합니다.
2. 복제 * 를 선택합니다.

결과

새 탭이 원래 탭과 같은 이름으로 나타납니다.

CloudShell 세션 탭을 닫습니다

CloudShell 탭을 한 번에 하나씩 닫거나, 작업하지 않는 다른 탭을 닫거나, 모든 탭을 한 번에 닫을 수 있습니다.

단계

1. CloudShell 세션 탭의 작업 메뉴를 선택합니다.
2. 다음 중 하나를 선택합니다.
   - CloudShell Tab 창에서 "X"를 선택하여 한 번에 하나의 탭을 닫습니다.
   - 작업 중인 탭을 제외한 열려 있는 다른 모든 탭을 닫으려면 * 다른 탭 닫기 * 를 선택합니다.
   - 모든 탭을 닫으려면 * 모든 탭 닫기 * 를 선택합니다.

결과

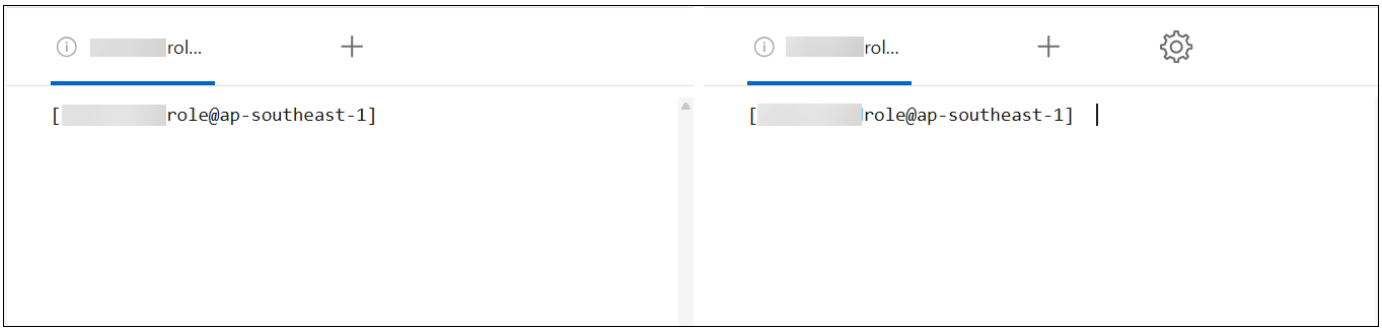
선택한 CloudShell 세션 탭이 닫힙니다.

CloudShell 세션 탭을 분할합니다

CloudShell 세션 탭을 분할하여 두 개 이상의 탭을 동시에 볼 수 있습니다.

단계

CloudShell 세션 탭을 CloudShell 창의 위쪽, 아래쪽, 왼쪽 또는 오른쪽으로 끌어 놓아 보기를 분할합니다.



CloudShell 세션에 대한 설정을 업데이트합니다

CloudShell 세션의 글꼴 및 출력 유형 설정을 업데이트할 수 있습니다.

단계

1. CloudShell 세션을 배포합니다.
2. CloudShell 탭에서 설정 아이콘을 선택합니다.

   설정 대화 상자가 나타납니다.

3. 필요에 따라 글꼴 크기와 출력 유형을 업데이트합니다.

   풍부한 출력은 JSON 객체 및 테이블 서식에 적용됩니다. 다른 모든 출력은 일반 텍스트로 표시됩니다.

4. Apply * 를 선택합니다.

결과

CloudShell 설정이 업데이트됩니다.

NetApp Workload Factory에서 자격 증명 제거

더 이상 자격 증명 세트가 필요하지 않으면 Workload Factory에서 삭제할 수 있습니다. FSx for ONTAP 파일 시스템과 연결되지 않은 자격 증명만 삭제할 수 있습니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴에서 *관리*를 선택한 다음 *자격 증명*을 선택합니다.
3. 자격 증명 페이지에서 다음을 수행합니다.
    - Workload Factory 콘솔에서 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *제거*를 선택합니다. *제거*를 선택하여 확인하세요.
    - NetApp 콘솔에서 자격 증명 세트에 대한 작업 메뉴를 선택한 다음 *삭제*를 선택합니다. 삭제를 선택하여 확인하세요.

지식 및 지원

지원을 위해 등록하십시오

NetApp Workload Factory와 해당 스토리지 솔루션 및 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Workload Factory와는 별도의 웹 기반 콘솔인 NetApp 콘솔에서 지원을 받으려면 등록해야 합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 Workload Factory 설명서에서 "도움말 받기"를 참조하세요.

"ONTAP용 Amazon FSx"

지원 등록 개요

계정 ID 지원 구독을 등록하면(NetApp 콘솔의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호) 단일 지원 구독 ID로 사용됩니다. 각 NetApp 계정 수준 지원 구독을 등록해야 합니다.

등록하면 지원 티켓 개설, 자동 사례 생성 등의 기능을 사용할 수 있습니다. 아래 설명된 대로 NetApp 콘솔에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원에 계정을 등록합니다

지원을 등록하고 지원 자격을 활성화하려면 계정의 한 사용자가 NetApp 지원 사이트 계정을 NetApp 콘솔 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

NSS 계정이 있는 NetApp 고객인 경우 NetApp 콘솔을 통해 지원을 등록하기만 하면 됩니다.

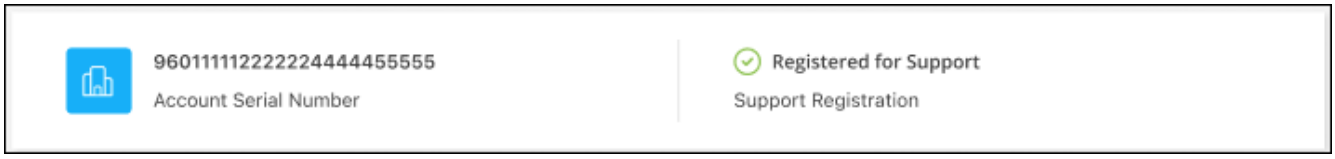
단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택합니다.

   이 옵션을 선택하면 NetApp 콘솔이 새 브라우저 탭에서 열리고 지원 대시보드가 로드됩니다.

2. NetApp 콘솔 메뉴에서 *관리*를 선택한 다음 *자격 증명*을 선택합니다.
3. 사용자 자격 증명 * 을 선택합니다.
4. NSS 자격 증명 추가 * 를 선택하고 NetApp Support 사이트(NSS) 인증 프롬프트를 따릅니다.
5. 등록 프로세스가 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.

   리소스 * 페이지에 계정이 지원을 위해 등록되었다는 내용이 표시됩니다.



NetApp 콘솔 로그인과 NetApp 지원 사이트 계정을 연결하지 않은 다른 NetApp 콘솔 사용자는 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 귀하의 NetApp 계정이 지원에 등록되지 않았다는 것은 아닙니다. 계정의 사용자 한 명이 이러한 단계를 따랐다면 귀하의 계정은 등록된 것입니다.

기존 고객이지만 **NSS** 계정은 없습니다

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 NetApp 콘솔 로그인과 연결해야 합니다.

단계

1. 를 완료하여 NetApp 지원 사이트 계정을 만듭니다 "NetApp Support 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 * NetApp 고객/최종 사용자 *)을 선택해야 합니다.
   b. 위에 사용된 NetApp 계정 일련 번호(960xxxx)를 일련 번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 NetApp 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp이 처음이었습니다

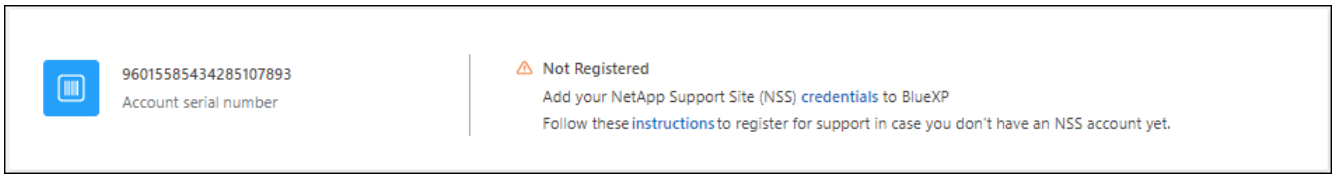
NetApp의 새로운 브랜드이고 NSS 계정이 없는 경우 아래의 각 단계를 수행하십시오.

단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택합니다.

   이 옵션을 선택하면 NetApp 콘솔이 새 브라우저 탭에서 열리고 지원 대시보드가 로드됩니다.

2. 지원 리소스 페이지에서 계정 ID 일련 번호를 찾습니다.



3. 로 "NetApp의 지원 등록 사이트" 이동하여 * 등록된 NetApp 고객이 아님 * 을 선택합니다.
4. 필수 필드(빨간색 별표가 있는 필드)를 입력합니다.
5. [제품 라인] * 필드에서 * Cloud Manager * 를 선택한 다음 해당 청구 공급자를 선택합니다.
6. 위의 2단계에서 계정의 일련 번호를 복사하고 보안 검색을 완료한 다음 NetApp의 글로벌 데이터 개인 정보 보호 정책을 읽는지 확인합니다.

   이 보안 트랜잭션을 완료하기 위해 제공된 사서함으로 즉시 이메일이 전송됩니다. 몇 분 내에 확인 이메일이 도착하지 않으면 스팸 폴더를 확인해야 합니다.

7. 이메일 내에서 작업을 확인합니다.

   확인 시 NetApp에 요청이 제출되고 NetApp Support 사이트 계정을 만들 것을 권장합니다.

8. 를 완료하여 NetApp 지원 사이트 계정을 만듭니다 "NetApp Support 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 * NetApp 고객/최종 사용자 *)을 선택해야 합니다.

b. 일련 번호 필드에 위에서 사용된 계정 일련 번호(960xxxx)를 복사해 주십시오. 이렇게 하면 계정 처리 속도가 빨라집니다.

작업을 마친 후

이 과정에서 NetApp이 연락을 드릴 것입니다. 신규 사용자를 위한 일회성 온보딩 연습입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 NetApp 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

도움을 받으십시오

NetApp 다양한 방법으로 Workload Factory와 클라우드 서비스에 대한 지원을 제공합니다. 지식 기반(KB) 문서와 커뮤니티 포럼 등 광범위한 무료 셀프 지원 옵션을 연중무휴 24시간 이용할 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

FSx for ONTAP에 대한 지원을 받으십시오

FSx for ONTAP, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 Workload Factory 설명서에서 "도움말 받기"를 참조하세요.

"ONTAP용 Amazon FSx"

Workload Factory 및 해당 스토리지 솔루션 및 서비스에 대한 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하십시오.

자체 지원 옵션을 사용합니다

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- 문서화

  현재 보고 있는 Workload Factory 문서입니다.

- "기술 자료"

  Workload Factory 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  Workload Factory 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새로운 토론을 만들어 보세요.

NetApp Support로 케이스 생성

위의 자체 지원 옵션 외에도 NetApp 지원 전문가와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

시작하기 전에

사례 만들기 기능을 사용하려면 먼저 지원에 등록해야 합니다. NetApp 지원 사이트 자격 증명을 Workload Factory 로그인과 연결해야 합니다. "지원 등록 방법을 알아보십시오" .

단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택합니다.

   이 옵션을 선택하면 NetApp 콘솔이 새 브라우저 탭에서 열리고 지원 대시보드가 로드됩니다.

2. 리소스 * 페이지의 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.

   a. 전화로 통화하려면 * 전화 * 를 선택하십시오. 전화를 걸 수 있는 전화 번호가 나열된 netapp.com 페이지로 연결됩니다.

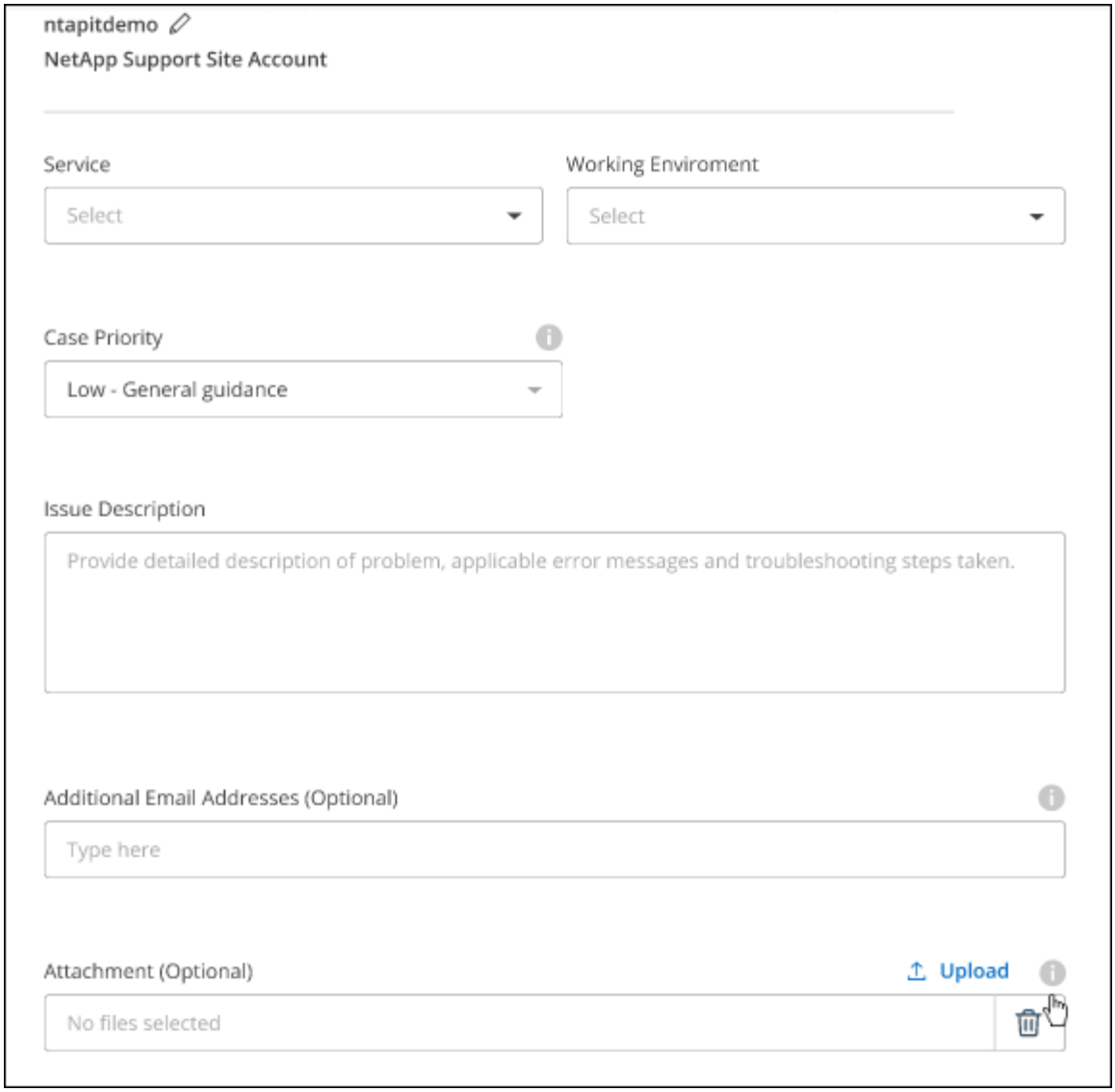
   b. NetApp 지원 전문가와 함께 티켓을 열려면 * 케이스 생성 * 을 선택하십시오.

      - * 서비스 *: * 워크로드 팩토리 * 를 선택합니다.
      - * 케이스 우선 순위 *: 케이스의 우선 순위를 선택합니다. 우선 순위는 낮음, 중간, 높음 또는 긴급입니다.

        이러한 우선 순위에 대한 자세한 내용을 보려면 필드 이름 옆에 있는 정보 아이콘 위로 마우스를 가져갑니다.

      - * 문제 설명 * : 해당 오류 메시지 또는 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공합니다.
      - * 추가 이메일 주소 *: 다른 사람에게 이 문제를 알고자 할 경우 추가 이메일 주소를 입력하십시오.
      - * 첨부 파일(선택 사항) *: 한 번에 하나씩 최대 5개의 첨부 파일을 업로드합니다.

        첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.



작업을 마친 후

지원 케이스 번호와 함께 팝업이 나타납니다. NetApp 지원 전문가가 귀사의 사례를 검토하고 곧 다시 연결해 드릴 것입니다.

지원 케이스 기록을 보려면 * 설정 > 일정 * 을 선택하고 "지원 케이스 생성"이라는 작업을 찾을 수 있습니다. 맨 오른쪽에 있는 버튼을 사용하면 작업을 확장하여 세부 정보를 볼 수 있습니다.

케이스를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 케이스를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 NetApp 콘솔 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 시스템 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 제품 내 채팅을 사용합니다
- 에서 비기술적 케이스를 제출하십시오 https://mysupport.netapp.com/site/help

지원 사례 관리(Preview)

NetApp 콘솔에서 활성 및 해결된 지원 사례를 직접 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된 사례를 관리할 수 있습니다.

케이스 관리를 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

다음 사항에 유의하십시오.

- 페이지 상단의 케이스 관리 대시보드에서는 두 가지 보기를 제공합니다.
  - 왼쪽 보기에는 사용자가 제공한 NSS 계정으로 지난 3개월 동안 개설된 총 케이스가 표시됩니다.
  - 오른쪽 보기에는 사용자 NSS 계정을 기준으로 회사 수준에서 지난 3개월 동안 개설된 총 사례가 표시됩니다.

  테이블의 결과에는 선택한 보기와 관련된 사례가 반영됩니다.
- 관심 있는 열을 추가 또는 제거할 수 있으며 우선 순위 및 상태 등의 열 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

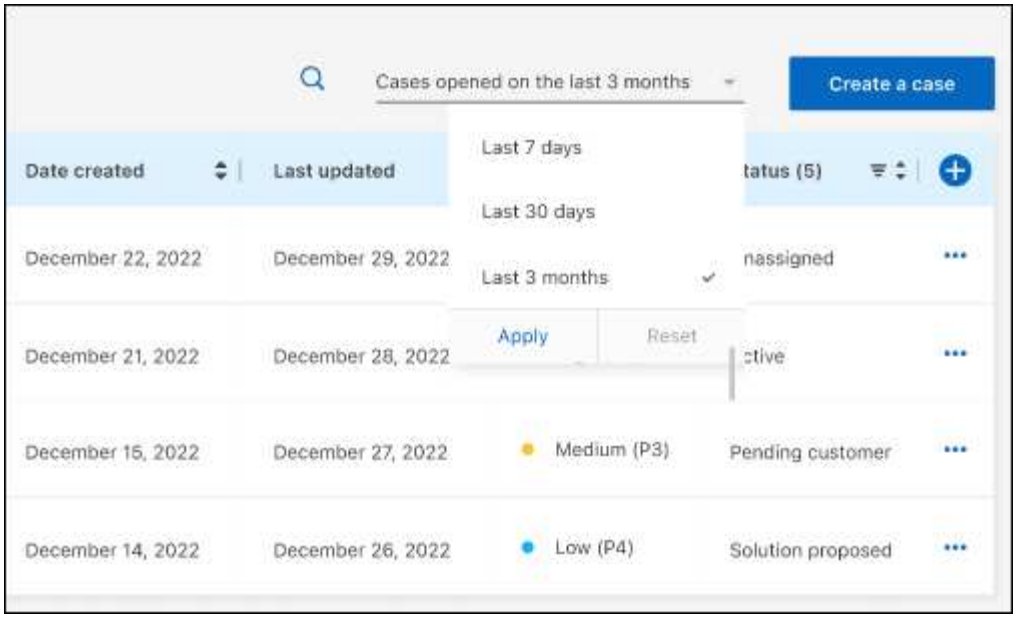
  자세한 내용은 아래 단계를 참조하십시오.
- 케이스 수준별로 케이스 메모를 업데이트하거나 아직 종결 또는 미결 종결 상태가 아닌 케이스를 종결할 수 있습니다.

단계

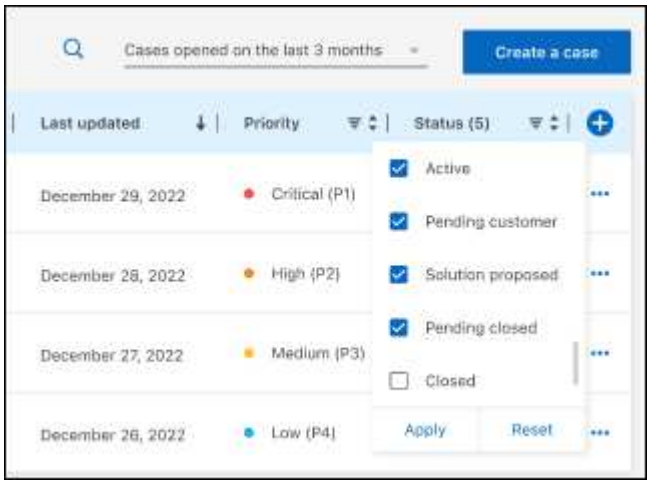
1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택합니다.

   이 옵션을 선택하면 NetApp 콘솔에 새 브라우저 탭이 열리고 지원 대시보드가 로드됩니다.
2. *사례 관리*를 선택하고 메시지가 표시되면 NetApp 콘솔에 NSS 계정을 추가합니다.

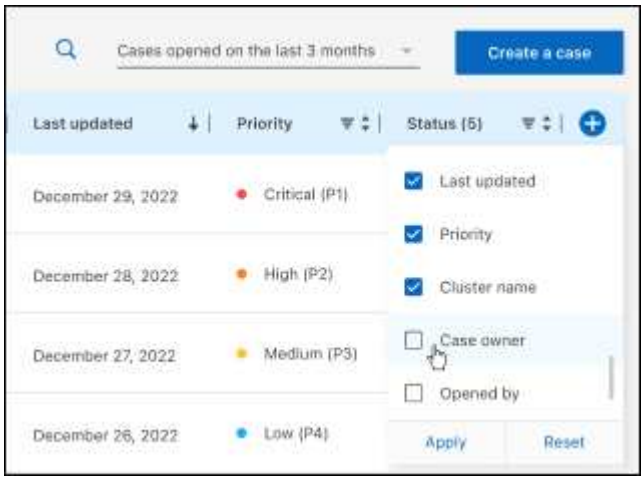
   사례 관리 페이지는 NetApp 콘솔 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 표시합니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요한 경우 테이블에 표시되는 정보를 수정합니다.
   - 조직의 케이스 * 에서 * 보기 * 를 선택하여 회사와 관련된 모든 케이스를 봅니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정합니다.



◦ 열의 내용을 필터링합니다.



◦ 표시할 열을 선택한 다음 선택하여 테이블에 표시되는 열을 변경합니다 [테이블에 나타나는 더하기 아이콘입니다] .



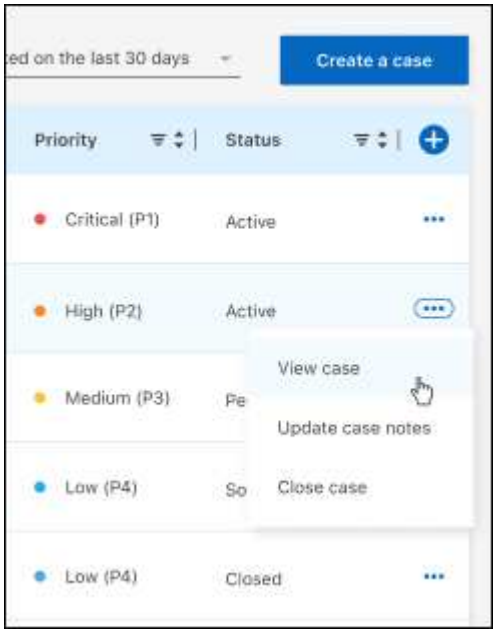
4. 사용 가능한 옵션 중 하나를 선택하고 선택하여 기존 케이스를 [표의 마지막 열에 세 개의 점이 있는 아이콘]

관리합니다.

- * 사례 보기 *: 특정 케이스에 대한 전체 세부 정보를 봅니다.
- * 케이스 메모 업데이트 *: 문제에 대한 추가 세부 정보를 제공하거나 * 파일 업로드 * 를 선택하여 최대 5개의 파일을 첨부할 수 있습니다.

  첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.

- * 케이스 종료 *: 케이스를 종료하는 이유에 대한 세부 정보를 제공하고 * 케이스 닫기 * 를 선택합니다.



NetApp Workload Factory에 대한 법적 고지 사항

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

"NetApp 워크로드 팩토리"

저작권 정보

Copyright © 2025 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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