NetApp 기술 보고서

NetApp Technical Reports

NetApp
June 05, 2026

목차

NetApp 기술 보고서

ONTAP, 애플리케이션 및 데이터베이스 기술 보고서

ONTAP은 많은 엔터프라이즈 애플리케이션 및 데이터베이스 기술을 위한 데이터 관리 및 데이터 보호의 기초입니다. 다음 기술 보고서는 Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA 및 Epic에 대한 NetApp 권장 사례 및 구현 절차에 대한 지침을 제공합니다.

Microsoft SQL Server를 참조하십시오

SQL Server는 Microsoft의 데이터 플랫폼의 토대로서, 인메모리 기술을 통해 업무상 중요한 성능을 제공하고 온프레미스 또는 클라우드의 모든 데이터에 대한 보다 빠른 인사이트를 제공합니다.

"ONTAP 지원 Microsoft SQL Server에 대한 모범 사례" 스토리지 관리자 및 데이터베이스 관리자가 ONTAP 스토리지에 Microsoft SQL Server를 성공적으로 구축하는 방법에 대해 알아보십시오.

이 문서는 이전에 게시된 기술 보고서_TR-4590: ONTAP를 사용하여 Microsoft SQL Server에 대한 모범 사례 가이드를 대체합니다

"TR-4976: NetApp AFF A-Series 및 C-Series 시스템에서 가상화된 Microsoft SQL Server의 성능"
NetApp AFF A-Series 및 C-Series 시스템을 사용하는 Microsoft SQL Server의 성능 특성과 워크로드에 따라 올바른 시스템을 선택하는 방법에 대해 알아보십시오.

"TR-4714: SnapCenter를 사용하는 Microsoft SQL Server의 모범 사례"
SnapCenter 기술을 사용하여 데이터 보호를 지원하는 ONTAP 스토리지에 Microsoft SQL Server를 성공적으로 구축하는 방법에 대해 자세히 알아보십시오.

MySQL

이 문서에서는 구성 요구 사항을 설명하고 ONTAP에서 MySQL을 구축하기 위한 튜닝 및 스토리지 구성에 대한 지침을 제공합니다.

"NetApp ONTAP 기반 MySQL 데이터베이스 모범 사례" MariaDB 및 Percona를 포함한 MySQL과 그 변종은 많은 엔터프라이즈 애플리케이션에 널리 사용되고 있습니다. 이러한 애플리케이션은 글로벌 소셜 네트워킹 사이트, 대규모 전자 상거래 시스템, 수천 개의 데이터베이스 인스턴스를 포함하는 SMB 호스팅 시스템에 이르기까지 다양합니다. ONTAP에서 MySQL을 배포하기 위한 구성 요구 사항 및 튜닝 및 스토리지 구성에 대한 지침을 알아보십시오.

이 문서는 이전에 게시된 기술 보고서 _TR-4722: NetApp ONTAP 모범 사례에 기반한 MySQL 데이터베이스를 대체합니다

오라클

ONTAP는 Oracle 데이터베이스를 위해 설계되었습니다. 지난 수십 년 동안 ONTAP은 관계형 데이터베이스 I/O의 고유한 요구사항에 맞게 최적화되었으며, Oracle 데이터베이스의 필요에 따라 여러 ONTAP 기능이 특별히 개발되었으며, 심지어 Oracle Inc. 자체의 요청도 있었습니다.

"ONTAP 기반의 Oracle 데이터베이스" 스토리지 관리자 및 데이터베이스 관리자가 ONTAP 스토리지에서 Oracle을 성공적으로 구축할 수 있도록 지원하는 권장 사례에 대해 알아보십시오.

"ONTAP을 사용한 Oracle 데이터 보호" 스토리지 관리자와 데이터베이스 관리자가 ONTAP 스토리지의 Oracle에

성공적으로 백업, 복구, 복제 및 재해 복구 기능을 제공할 수 있도록 지원하는 권장 사례에 대해 알아보십시오.

"ONTAP을 사용한 Oracle 재해 복구" MetroCluster 및 SnapMirror 무중단 업무 운영 환경에서 Oracle 데이터베이스 운영을 위한 권장 사례, 테스트 절차 및 기타 고려 사항에 대해 알아보십시오.

"Oracle 데이터베이스를 ONTAP 스토리지 시스템으로 마이그레이션" 마이그레이션 전략을 계획할 때 고려해야 할 전반적인 고려 사항, 데이터 이동이 수행되는 세 가지 수준, 사용 가능한 여러 가지 절차에 대해 자세히 알아봅니다.

위에 링크된 문서는 이전에 게시된 기술 보고서를 대체합니다_TR-3633: ONTAP 기반 Oracle 데이터베이스, TR-4591: Oracle 데이터 보호: 백업, 복구, 복제, TR-4592: MetroCluster 기반 Oracle, TR-4534: Oracle 데이터베이스를 NetApp 스토리지 시스템으로 마이그레이션 _

"TR-4969: AFF A-Series 및 C-Series에서 Oracle 데이터베이스 성능 사용"
ONTAP는 인라인 압축, 무중단 하드웨어 업그레이드, 외부 스토리지 어레이에서 LUN 가져오기 등의 기본 기능을 갖춘 강력한 데이터 관리 플랫폼입니다. 최대 24개의 노드를 함께 클러스터링할 수 있으며 NFS(Network File System), SMB(Server Message Block), iSCSI, FC(Fibre Channel) 및 NVMe(Nonvolatile Memory Express) 프로토콜을 통해 데이터를 동시에 제공할 수 있습니다. 또한 Snapshot 기술은 수만 건의 온라인 백업과 완전하게 작동하는 데이터베이스 클론을 생성하기 위한 기반입니다. ONTAP의 풍부한 기능 세트 외에 데이터베이스 규모, 성능 요구사항, 데이터 보호 요구사항 등 다양한 사용자 요구사항이 있습니다. A-Series와 C-Series를 비롯한 AFF 스토리지 시스템을 사용한 베어 메탈 데이터베이스 성능에 대해 알아보고 두 AFF 옵션 간의 최대 성능과 실질적인 차이점을 모두 살펴봅니다.

"TR-4971: AFF A-Series 및 C-Series에서 가상화된 Oracle 데이터베이스 성능"
ONTAP는 인라인 압축, 무중단 하드웨어 업그레이드, 외부 스토리지 어레이에서 LUN 가져오기 등의 기본 기능을 갖춘 강력한 데이터 관리 플랫폼입니다. 최대 24개의 노드를 함께 클러스터링할 수 있으며 NFS(Network File System), SMB(Server Message Block), iSCSI, FC(Fibre Channel) 및 NVMe(Nonvolatile Memory Express) 프로토콜을 통해 데이터를 동시에 제공할 수 있습니다. 또한 Snapshot 기술은 수만 건의 온라인 백업과 완전하게 작동하는 데이터베이스 클론을 생성하기 위한 기반입니다. ONTAP의 풍부한 기능 세트 외에 데이터베이스 규모, 성능 요구사항, 데이터 보호 요구사항 등 다양한 사용자 요구사항이 있습니다. A-Series와 C-Series를 비롯한 AFF 스토리지 시스템을 사용한 가상 데이터베이스 성능에 대해 알아보고 두 AFF 옵션 간의 최대 성능과 실제 차이점을 살펴봅니다.

"TR-4695: FabricPool를 통한 데이터베이스 스토리지 계층화"
Oracle RDBMS(관계형 데이터베이스 관리 시스템)를 비롯한 다양한 데이터베이스를 사용하는 FabricPool의 이점과 구성 옵션에 대해 알아봅니다.

"TR-4899: SnapMirror 액티브 동기화를 사용하여 Oracle 데이터베이스 운영에 영향을 미치지 않음 애플리케이션 페일오버" SnapMirror 액티브 동기식(이전의 SM-BC) 및 Oracle RAC(Real Application Cluster)는 사이트 운영 중단 및 실제 재해 발생 시에도 투명한 애플리케이션 페일오버(TAF)와 연속성을 제공할 수 있습니다. Oracle RAC의 스토리지 구성 요소로 SnapMirror Active Sync를 사용하는 AFF 스토리지 어레이의 구성 지침 및 권장 사례에 대해 알아보십시오.

"TR-4876: ONTAP 솔루션 및 구축 모범 사례를 활용한 Oracle Multitenancy"
ONTAP 스토리지를 사용하여 Oracle 멀티 테넌트 데이터베이스와 ONTAP 소프트웨어의 기능을 모두 최대한 활용하여 Oracle 멀티 테넌트 데이터베이스를 프로비저닝, 관리 및 보호하는 방법에 대한 솔루션 권장 사례에 대해 알아보십시오.

PostgreSQL

PostgreSQL에는 PostgreSQL, PostgreSQL Plus 및 EDB Postgres Advanced Server(EPAS)가 포함된 변종이 함께 제공됩니다. PostgreSQL은 일반적으로 다중 계층 애플리케이션을 위한 백엔드 데이터베이스로 구축됩니다. NetApp ONTAP는 PostgreSQL 데이터베이스를 실행할 때 탁월한 선택으로 신뢰성, 고성능 및 효율적인 데이터 관리 기능을 제공합니다.

"ONTAP 모범 사례에 기반한 PostgreSQL 데이터베이스" PostgreSQL에는 PostgreSQL, PostgreSQL Plus 및 EDB

Postgres Advanced Server(EPAS)를 포함하는 변형이 제공됩니다. PostgreSQL은 일반적으로 다중 계층 애플리케이션을 위한 백엔드 데이터베이스로 구축됩니다. 일반적인 미들웨어 패키지(PHP, Java, Python, Tcl/Tk, ODBC, 또한 JDBC는 오픈 소스 데이터베이스 관리 시스템에서 널리 사용되고 있습니다. ONTAP에서 PostgreSQL을 구축하기 위한 구성 요구 사항과 튜닝 및 스토리지 구성에 대한 지침을 알아봅니다.

이 문서는 ONTAP 모범 사례 _ 에 대해 이전에 게시된 기술 보고서 _TR-4770: PostgreSQL 데이터베이스를 대체합니다.

SAP HANA를 참조하십시오

"ONTAP 기반 SAP HANA 데이터베이스 솔루션" SAP 솔루션의 구성, 관리 및 자동화에 대한 Best Practice는 NetApp SAP 솔루션 페이지에서 확인할 수 있습니다.

대단한

"ONTAP 기반 Epic 모범 사례" 온프레미스와 클라우드에 Epic을 구축하는 데 필요한 모범 사례를 이해하면서 ONTAP에서 적절한 규모로 구축하기 위한 구성 표준을 준수하는 데 필요한 지침을 제공합니다.

이 문서는 이전에 게시된 기술 보고서_TR-3923: Epic_에 대한 NetApp 모범 사례를 대체합니다.

무중단 업무 운영 기술 보고서

NetApp은 애플리케이션 및 데이터 위치를 합리화하여 비용 대비 성능을 비용 효율적으로 개선하는 다양한 솔루션을 제공합니다. 데이터 보호, 복제 및 지속적인 가용성: ONTAP 데이터 관리는 set-it-and-for-get-it 정책 관리로 데이터 보호를 단순화하는 동시에 MetroCluster 및 SnapMirror 활성 동기화를 통해 비즈니스 연속성을 제공합니다.

이러한 기술 보고서는 및 제품 설명서에 대해 자세히 "ONTAP SnapMirror 활성 동기화" "ONTAP MetroCluster" 설명합니다.

SnapMirror 활성 동기식(이전의 SM-BC)

"TR-4878: SnapMirror 액티브 동기화" SnapMirror 액티브 동기화는 AFF 또는 ASA(All SAN 어레이) 스토리지 시스템에서 실행되는 ONTAP에 사용할 수 있는 애플리케이션 레벨 세분화를 갖춘 지속적인 스토리지 솔루션으로, 가장 중요한 비즈니스 애플리케이션의 RPO 0 및 RTO 0 요구사항을 충족합니다.

MetroCluster

"TR-4705: NetApp MetroCluster 솔루션 아키텍처 및 설계"
이 문서에서는 ONTAP의 MetroCluster 기능에 대한 고급 아키텍처 및 설계 개념에 대해 설명합니다.

MetroCluster IP

"TR-4689: NetApp MetroCluster IP" MetroCluster는 FAS 및 AFF 시스템에서 실행되는 ONTAP를 위해 지속적으로 사용할 수 있는 스토리지 솔루션입니다. MetroCluster IP는 이더넷 기반 백엔드 스토리지 패브릭을 사용하는 최신 혁신입니다. MetroCluster IP는 가장 중요한 비즈니스 애플리케이션의 요구 사항을 충족하는 고도로 이중화된 구성을 제공합니다. MetroCluster IP는 ONTAP에 포함되어 있으며 ONTAP 스토리지를 사용하는 클라이언트 및 서버에 NAS 및 SAN 연결을 제공합니다.

MetroCluster FC

"TR-4375: NetApp MetroCluster FC" MetroCluster는 지리적으로 분리된 데이터 센터 전체에서 미션 크리티컬 애플리케이션을 위해 지속적인 데이터 가용성을 제공합니다. MetroCluster FC의 권장 사례, 설계 결정 및 지원 구성에 대해 알아보십시오.

ONTAP 데이터 보호 및 재해 복구 기술 보고서

SnapMirror는 Data Fabric 전반에서 사용하기 쉬운 비용 효율적인 통합 복제 솔루션입니다. LAN 또는 WAN을 통해 데이터를 고속으로 복제합니다. 가상 환경과 기존 환경 모두에서 Microsoft Exchange, Microsoft SQL Server, Oracle 등과 같은 비즈니스 크리티컬 애플리케이션의 데이터 가용성을 높이고 신속한 데이터 복제를 실현할 수 있습니다. 하나 이상의 ONTAP 스토리지 시스템에 데이터를 복제하고 2차 데이터를 지속적으로 업데이트함으로써 데이터가 최신 상태로 유지되고 필요할 때마다 사용할 수 있으며 외부 복제 서버가 필요하지 않습니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP 데이터 보호 및 재해 복구"설명합니다.

SnapMirror를 참조하십시오

SnapMirror 비동기

"TR-4015: SnapMirror 비동기식 구성 및 모범 사례" 볼륨, 일관성 그룹 및 스토리지 가상 머신(SVM 재해 복구)에 대한 SM-A(SnapMirror 비동기식) 복제를 구성하기 위한 권장 사례에 대해 알아보십시오.

"TR-4678: 데이터 보호 및 백업 ONTAP FlexGroup 볼륨"
FlexGroup 볼륨에 대한 권장 데이터 보호 및 백업에 대해 알아보십시오. 이 플레이북에서는 스냅샷 복사본, SnapMirror, 기타 데이터 보호 및 백업 솔루션이 포함되어 있습니다.

SnapMirror Synchronous

"TR-4733: SnapMirror Synchronous 구성 및 모범 사례" SM-S(SnapMirror Synchronous) 복제를 구성하기 위한 권장 방법에 대해 알아봅니다.

SnapMirror 3 - 데이터 센터 **DR**

"TR-4832: ONTAP 9.7용 NetApp SnapMirror를 사용한 데이터 센터 재해 복구 3개" 복제에 ONTAP SnapMirror 기술을 사용하는 3개의 데이터 센터 재해 복구 구성에 대해 알아보십시오.

SnapMirror를 사용하여 애플리케이션 및 인프라 통합

"TR-4900: ONTAP를 사용하는 VMware 사이트 복구 관리자" ONTAP은 2002년에 현대적인 데이터 센터에 선보인 이후 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션으로, 관리 작업을 간소화하는 동시에 비용을 절감할 수 있는 혁신적인 기능을 지속적으로 추가하고 있습니다. 배포를 간소화하고 위험을 줄이며 지속적인 관리를 단순화하기 위한 최신 제품 정보 및 권장 사례를 비롯하여 업계 최고의 VMware DR(재해 복구) 소프트웨어인 VMware SRM(사이트 복구 관리자)에 대한 권장 ONTAP 솔루션에 대해 알아보십시오.

ONTAP 사이버 소산

"ONTAP 사이버 소산" NetApp의 ONTAP 기반 사이버 저장소는 가장 중요한 데이터 자산을 보호하는 포괄적이고 유연한 솔루션을 제공합니다. ONTAP은 강력한 강화 방법론을 통해 논리적 공기 흐름을 활용하여 진화하는 사이버 위협에 맞서 복원력을 갖춘 격리된 보안 스토리지 환경을 만들 수 있도록 지원합니다. ONTAP을 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서 데이터의 기밀성, 무결성, 가용성을 보장할 수 있습니다.

ONTAP FlexCache 및 FlexGroup 볼륨 기술 보고서

NetApp NAS 솔루션은 데이터 관리를 단순화하며 비용을 최적화하는 동시에 규모 확장에 대비할 수 있도록 지원합니다. ONTAP NAS 솔루션은 유니파이드 아키텍처 내에서 무중단 운영과 검증된 효율성, 무한한 확장성을 제공합니다. ONTAP을 기반으로 하는 스케일아웃 NAS는 대규모 ONTAP 에코시스템을 활용하여 혁신을 주도하고 공격적인 미래 혁신을 위한 비전을 실현할 수 있습니다.

이러한 기술 보고서는 및 제품 설명서에 대해 자세히 "ONTAP FlexCache 볼륨" "ONTAP FlexGroup 볼륨" 설명합니다.

FlexCache

"TR-4743: ONTAP의 FlexCache"
FlexCache는 동일하거나 다른 ONTAP 클러스터에서 볼륨의 쓰기 가능한 스파스 복제본을 생성하는 캐싱 기술입니다. 데이터 및 파일을 사용자와 더 가까운 곳에 제공하여 더 적은 설치 공간으로 더 빠른 처리량을 얻을 수 있습니다. FlexCache 사용 방법, 권장 사례, 제한 및 설계 및 구현 고려 사항에 대해 알아보십시오.

FlexCache 다시 쓰기

"FlexCache 다시 쓰기" ONTAP 9.15.1에 도입된 FlexCache Write-Back은 캐시에서 쓰는 대체 작업 모드입니다. Write-back을 사용하면 데이터가 오리진으로 전달될 때까지 기다리지 않고 캐시의 안정적인 스토리지에 쓰기를 커밋하고 클라이언트에서 이를 확인할 수 있습니다. 데이터는 비동기적으로 오리진으로 다시 플러시됩니다. 그 결과, 특정 워크로드 및 환경에서 거의 로컬에 가까운 속도로 쓰기를 수행할 수 있는 전 세계적으로 분산된 파일 시스템이 탄생하여 탁월한 성능 이점을 제공합니다.

FlexGroup 볼륨

"TR-4571: NetApp ONTAP FlexGroup 볼륨 모범 사례 및 구현 가이드"
FlexGroup 볼륨, 권장 사례 및 구현 팁에 대해 알아보십시오. FlexGroup 볼륨은 메타데이터가 많은 워크로드에서 거의 무제한의 용량과 예측 가능하고 짧은 지연 시간의 성능을 결합한 ONTAP 스케일아웃 NAS 컨테이너의 발전된 형태입니다.

"TR-4678: FlexGroup 볼륨의 데이터 보호 및 백업"
스냅샷 복사본, SnapMirror, 기타 데이터 보호 및 백업 솔루션을 포함한 FlexGroup 볼륨의 데이터 보호 및 백업에 대해 알아보십시오.

ONTAP NAS 기술 보고서

NetApp NAS 솔루션은 데이터 관리를 단순화하며 비용을 최적화하는 동시에 규모 확장에 대비할 수 있도록 지원합니다. ONTAP NAS 솔루션은 유니파이드 아키텍처 내에서 무중단 운영, 효율성 및 원활한 확장성을 제공합니다. NetApp ONTAP을 기반으로 하는 스케일아웃 NAS는 대규모 ONTAP 에코시스템을 활용하여 혁신을 주도하고 공격적인 미래 혁신을 위한 비전을 실현할 수 있습니다.

이러한 기술 보고서는 및 제품 설명서에 대해 자세히 "ONTAP NAS 스토리지 관리" "ONTAP S3 스토리지 관리" 설명합니다.

NFS 를 참조하십시오

"TR-4067: ONTAP의 NFS 모범 사례 및 구축 가이드"
ONTAP의 NFS에 대한 기본 개념, 지원 정보, 구성 팁 및 권장 사항에 대해 알아보십시오.

"TR-4962: NFSv4.2 확장 속성"
ONTAP 9.12.1 이상에서 NFSv4.2 확장 속성을 설정하고 사용하는 방법에 대해 알아봅니다.

중소기업

"TR-4740: SMB 3.0 멀티채널"
Microsoft는 SMB1과 SMB2의 성능 및 안정성 한계를 해결함으로써 SMB3 프로토콜의 개선을 목표로 SMB 3.0 프로토콜에 멀티채널을 도입했습니다. ONTAP의 기능, 권장 사례 및 성능 테스트 결과를 비롯한 멀티채널 기능에 대해 알아보십시오.

멀티 프로토콜

"TR-4887: ONTAP의 다중 프로토콜 NAS 개요 및 모범 사례"
ONTAP에서 멀티프로토콜 NAS 액세스가 작동하는 방식과 멀티프로토콜 환경에 대한 권장 사례에 대해 알아보십시오.

ONTAP S3

"TR-4814:S3(ONTAP 모범 사례" ONTAP 소프트웨어와 함께 Amazon S3(Simple Storage Service)를 사용하기 위한 권장 사례와 ONTAP를 네이티브 S3 애플리케이션이 있는 오브젝트 저장소 또는 FabricPool의 계층화 대상으로 사용하기 위한 기능 및 구성에 대해 알아보십시오.

네임 서비스

"TR-4523: ONTAP에서 DNS 로드 밸런싱"
ONTAP의 DNS, 다양한 구성 방법 및 권장 방법을 포함하여 DNS 로드 밸런싱 방법론과 함께 사용하도록 ONTAP를 구성하는 방법에 대해 알아봅니다.

"TR-4668: 서비스 모범 사례 가이드를 이름하십시오"
ONTAP에서 CIFS/SMB 및 NFS와 같은 NAS(Network-Attached Storage) 솔루션을 구축할 때 권장되는 방법, 제한 및 고려 사항에 대해 알아보십시오.

"TR-4835: ONTAP 멀티 프로토콜 NAS ID 관리에서 LDAP를 구성하는 방법"
멀티 프로토콜 NAS를 위해 ONTAP에서 LDAP(Lightweight Directory Access Protocol) ID 관리를 구성하는 방법에 대해 알아봅니다.

NAS 보안

"TR-4616: ONTAP에서 NFS Kerberos"
Active Directory 및 RHEL(Red Hat Enterprise Linux) 클라이언트의 구성 단계를 포함하여 ONTAP에서 NFS Kerberos에 대해 알아보십시오.

ONTAP 네트워킹 기술 보고서

ONTAP는 가장 까다로운 스케일 아웃 애플리케이션을 충족할 수 있도록 다양한 네트워킹 기능과 구성을 제공합니다. 네트워킹 기능 및 기능을 사용하여 안정적이고 안전한 데이터 액세스를 구축할 수 있습니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP 네트워크 관리"설명합니다.

"TR-4949: 데이터 센터에서 ONTAP를 사용하는 BGP/VIP"
ONTAP에서 기본적인 BGP 구성을 빠르게 구축하는 방법을 알아보십시오.

ONTAP SAN 기술 보고서

ONTAP SAN 스토리지는 조직의 미션 크리티컬 데이터베이스와 기타 SAN 워크로드에 고가용성을 제공하는 단순한 SAN 경험을 제공합니다. ONTAP SAN은 Oracle, SAP 및 Microsoft SQL Server 데이터베이스와의 동급 최고의 데이터 서비스 통합 및 VMware 및 기타 주요 하이퍼바이저와 함께 엔터프라이즈 데이터베이스 애플리케이션의 가치 창출 시간을 단축합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP SAN 스토리지 관리"설명합니다.

"TR-4080: ONTAP의 최신 SAN 모범 사례"
ONTAP의 블록 프로토콜과 권장 사항에 대해 자세히 알아보십시오.

"TR-4684: NVMe-oF(NVMe over Fabrics)를 사용하여 최신 SAN 구현 및 구성"
NVMe over Fabrics 전송(NVMe over Fibre Channel 및 NVMe over TCP)을 구축하고 구성하는 방법을 알아보십시오. 이 플레이북에서는 설계, 구축, 구성, 관리 지침, 그리고 NVMe 프로토콜 및 전송을 사용하여 가용성이 높은 최신 SAN 솔루션을 구축하는 데 필요한 권장 지침이 포함되어 있습니다.

"TR-4968: NetApp All-SAN 어레이의 데이터 가용성 및 무결성"
모든 SAN 어레이 시스템의 다양한 데이터 보호 및 데이터 무결성 기능이 어떻게 작동하면서 애플리케이션 가동 시간을 극대화하고 SAN 네트워크를 설계, 구현 및 관리하는 데 권장되는 방법을 익히는지 알아보십시오.

"최신 SAN 클라우드 연결 플래시 솔루션"
이 NetApp 검증 아키텍처는 NetApp, VMware 및 Broadcom에서 공동으로 설계 및 검증되었습니다. 최신 Brocade, Emulex 및 VMware vSphere 기술 솔루션과 NetApp All-Flash 스토리지를 함께 사용하여 엔터프라이즈 SAN 스토리지 및 데이터 보호에 대한 새로운 표준을 정립하고 있으며 이는 탁월한 비즈니스 가치를 이끌어내는 데 도움이 됩니다.

보안

ONTAP 보안 기술 보고서

ONTAP는 보안을 솔루션의 일부로 통합하여 지속적으로 발전하고 있습니다. ONTAP의 최신 릴리즈에는 조직이 하이브리드 클라우드 전체에서 데이터를 보호하고, 랜섬웨어 공격을 방지하고, 업계 권장 사례를 준수하는 데 매우 중요한 새로운 보안 기능이 다수 포함되어 있습니다. 이러한 새로운 기능은 조직의 Zero Trust 모델 전환도 지원합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP 보안 및 데이터 암호화"설명합니다.

ONTAP 사이버 소산

"ONTAP 사이버 소산" NetApp의 ONTAP 기반 사이버 저장소는 가장 중요한 데이터 자산을 보호하는 포괄적이고 유연한 솔루션을 제공합니다. ONTAP은 강력한 강화 방법론을 통해 논리적 공기 흐름을 활용하여 진화하는 사이버 위협에 맞서 복원력을 갖춘 격리된 보안 스토리지 환경을 만들 수 있도록 지원합니다. ONTAP을 사용하면 스토리지 인프라의 민첩성과 효율성을 유지하면서 데이터의 기밀성, 무결성, 가용성을 보장할 수 있습니다.

랜섬웨어

"TR-4572: 랜섬웨어용 NetApp 솔루션" 랜섬웨어의 진화 과정을 알아보고, 랜섬웨어용 NetApp 솔루션을 사용하여 공격을 식별하고, 확산을 방지하고, 최대한 빠르게 복구하는 방법을 살펴보십시오. 이 문서에 제공된 지침과 솔루션은 조직이 사이버 복원력 있는 솔루션을 보유하면서 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 설계되었습니다.

"TR-4526: NetApp SnapLock를 사용한 규정 준수 WORM 스토리지"
많은 기업에서는 규정 준수 요구 사항을 충족하거나 단순히 데이터 보호 전략에 다른 계층을 추가하기 위해 WORM(Write Once, Read Many) 데이터 스토리지를 사용하고 있습니다. ONTAP에서 WORM 솔루션인 SnapLock를 WORM 데이터 스토리지가 필요한 환경에 통합하는 방법에 대해 알아보십시오.

제로 트러스트

"NetApp와 제로 트러스트" 제로 트러스트는 네트워크 중심의 접근 방식으로 MCAP(마이크로 코어 및 경계)를 설계하여 데이터, 서비스, 애플리케이션 또는 자산을 세분화 게이트웨이라고 하는 제어 기능을 사용해 왔습니다. ONTAP는 제로 트러스트에 대한 데이터 중심 접근 방식을 취하며 스토리지 관리 시스템이 세분화 게이트웨이가 되어 고객 데이터의 액세스를 보호하고 모니터링합니다. 특히 FPolicy Zero Trust 엔진과 FPolicy 파트너 에코시스템은 정상 및 비정상적인 데이터 액세스 패턴을 세부적으로 이해하고 내부자 위협을 식별하기 위한 제어 센터가 됩니다.

다단계 인증

"TR-4647: ONTAP 모범 사례 및 구현 가이드의 다중 요소 인증"
System Manager, Active IQ Unified Manager 및 ONTAP SSH(Secure Shell) CLI 인증을 사용하여 관리 액세스에 대한 ONTAP의 다단계 인증 기능에 대해 알아보십시오.

"TR-4717: 공통 액세스 카드를 사용한 ONTAP SSH 인증"
ONTAP에서 CAC(Common Access Card)에 저장된 공개 키를 통해 ONTAP 스토리지 관리자를 인증하기 위해 ActivClient 소프트웨어와 함께 타사 SSH 클라이언트를 구성 및 테스트하는 방법을 알아봅니다.

멀티 테넌시

"TR-4160: ONTAP의 보안 멀티 테넌시"
설계 고려 사항 및 권장 사례를 비롯하여 ONTAP에서 스토리지 VM을 사용하여 보안 멀티 테넌시를 구현하는 방법에 대해 알아보십시오.

표준

"TR-4401: PCI-DSS 4.0 및 ONTAP"
PCI DSS 4.0 표준에 따라 시스템을 검증하고 NetApp ONTAP 시스템에 적용하는 제어 요구 사항을 충족하는 방법에 대해 알아보십시오.

속성 기반 액세스 제어

"ONTAP로 속성 기반 액세스 제어" RBAC(역할 기반 액세스 제어) 및 ABAC(속성 기반 액세스 제어)를 지원하도록 NFSv4.2 보안 레이블 및 확장 속성(xattrs)을 구성하는 방법에 대해 알아봅니다. 이 방법은 사용자, 리소스 및 환경 특성을 기준으로 사용 권한을 정의하는 권한 부여 전략입니다.

랜섬웨어에 대한 **NetApp** 솔루션

랜섬웨어 및 **NetApp**의 보호 포트폴리오

랜섬웨어는 2024년에 조직 중단을 초래하는 가장 중요한 위협 중 하나로 남아 있습니다. 에 따르면 "Sophos, 2024년 랜섬웨어 상태" 랜섬웨어 공격은 설문조사에 참여한 고객의 72%에 영향을 미친 것으로 나타났습니다. 랜섬웨어 공격은 그 영향과 수익을 극대화하기 위해 인공 지능과 같은 고급 기술을 사용하는 위협 공격자로 인해 더 정교하고 타겟이 되도록 진화하고 있습니다.

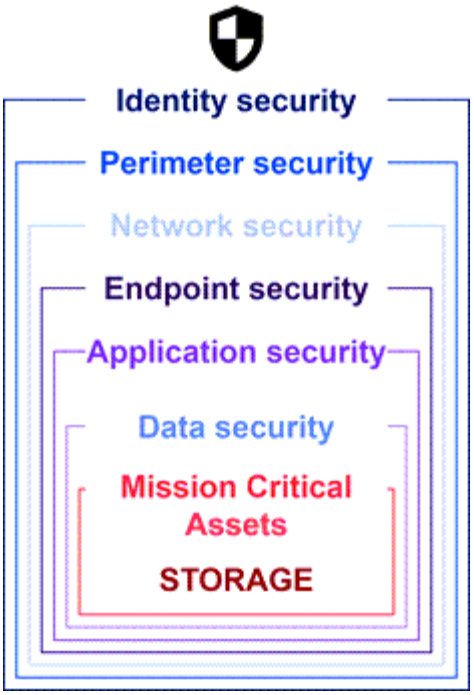
조직은 경계, 네트워크, ID, 애플리케이션, 데이터가 스토리지 수준에서 어디에 있는지, 그리고 이러한 계층을 안전하게 보호해야 합니다. 스토리지 계층에서 사이버 보호에 대한 데이터 중심의 접근 방식을 채택하는 것은 오늘날의 위협 환경에서 매우 중요합니다. 단일 솔루션으로 모든 공격을 차단할 수는 없지만, 파트너 관계 및 타사를 포함한 솔루션 포트폴리오를 사용하면 계층화된 방어 체계를 구축할 수 있습니다.

는 NetApp 제품 포트폴리오에 대해 자세히 살펴봅니다가시성, 감지, 해결을 위한 다양한 효과적인 툴을 제공하므로 랜섬웨어를 조기에 탐지하고 확산을 방지하고 필요한 경우 신속하게 복구하여 비용이 많이 드는 다운타임을 방지할 수 있습니다. 기존의 계층화된 방어 솔루션은 가시성과 감지를 위한 타사 및 파트너 솔루션처럼 널리 사용되고 있습니다. 효과적인 치료는 위협에 대한 대응의 중요한 부분입니다. 변경 불가능한 NetApp 스냅샷 기술 및 SnapLock 논리적 AIR GAP 솔루션을 활용하는 고유한 업계 접근법은 업계 차별화 요소이자 랜섬웨어 수정 기능에 대한 업계 모범 사례입니다.

> 2024년 7월부터 이전에 PDF로 게시되었던 NetApp Ransomware Protection_ 의 기술 보고서 _TR-4572: docs.netapp.com 에서 콘텐츠를 볼 수 있습니다.

데이터는 **1**차 타겟입니다

데이터를 직접 타겟으로 삼는 사이버 범죄자들이 점차 그 가치를 인식하게 되고 있습니다. 경계, 네트워크 및 애플리케이션 보안은 중요하지만 우회할 수 있습니다. 소스에서 데이터를 보호하는 데 중점을 둔 스토리지 계층은 중요한 최종 방어선을 제공합니다. 랜섬웨어 공격의 목표는 운영 데이터에 액세스하여 암호화하거나 액세스할 수 없도록 렌더링하는 것입니다. 이를 위해서는 공격자들이 경계에서 애플리케이션 보안에 이르기까지 오늘날 조직이 배포한 기존의 방어 체계를 이미 뚫어야만 합니다.



안타깝게도 많은 기업들은 데이터 레이어에서 보안 기능을 활용하지 못하고 있습니다. 이것이 바로 NetApp 랜섬웨어 차단 포트폴리오가 제공하는 이유입니다.

랜섬웨어의 실제 비용

몸값 지급 자체는 기업에 미치는 가장 큰 금전적 효과가 아닙니다. 지불액은 중요하지 않지만 랜섬웨어 사고로 인해 발생하는 다운타임 비용과 비교해 볼 수 있습니다.

몸값 지불은 랜섬웨어 이벤트를 처리할 때 복구 비용의 한 요소에 불과합니다. 지불된 모든 랜스를 제외하고, 2024개 조직은 랜섬웨어 공격으로부터 복구하는 평균 비용이 27만 3천 달러로, 2023년 보고된 1.820만 달러에서 거의 100만 달러 "2024 Sophos 랜섬웨어 상태" 증가했습니다. 전자 상거래, 주식 거래, 의료 등 IT 가용성에 크게 의존하는 조직의 경우 비용이 10배 이상 높을 수 있습니다.

보험 비용은 보험 회사를 대상으로 랜섬웨어 공격이 발생할 가능성이 매우 높기 때문에 지속적으로 증가하고 있습니다.

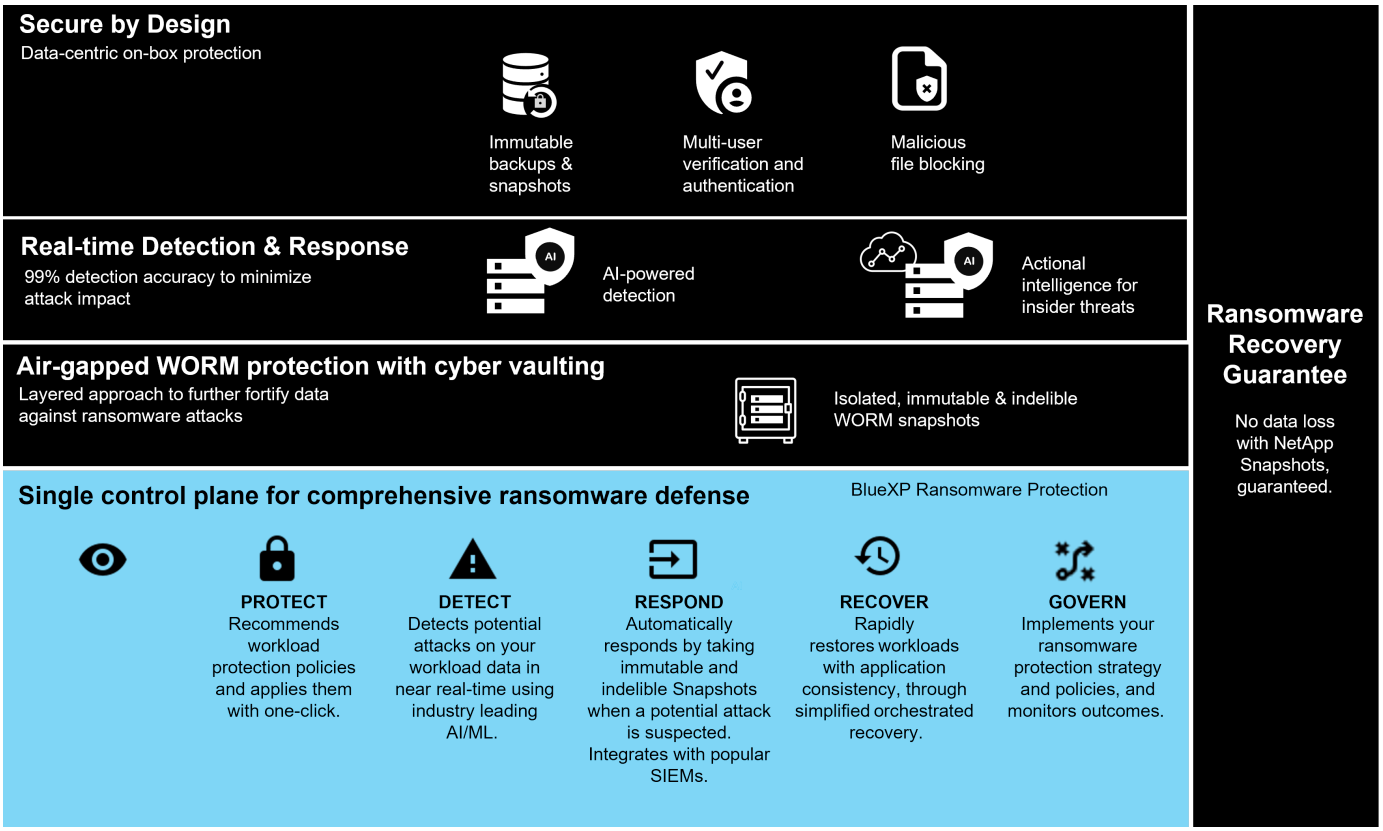
데이터 계층에서 랜섬웨어 방어

NetApp은 스토리지 계층에서 데이터가 상주하는 위치까지 조직 전체에서 광범위하고 심층적인 보안 태세를 이해합니다. 보안 스택은 복잡하며 기술 스택의 모든 수준에서 보안을 제공해야 합니다.

데이터 레이어에서 실시간 보호가 훨씬 더 중요하고 고유한 요구 사항이 있습니다. 효율성을 높이려면 이 계층의 솔루션이 다음과 같은 중요한 속성을 제공해야 합니다.

- * 보안 설계 * 를 통해 공격 성공 가능성을 최소화합니다
- * 실시간 감지 및 응답 * 을 통해 공격이 성공할 경우 미치는 영향을 최소화합니다
- * Air-gapped WORM 보호 * 로 중요한 데이터 백업을 격리합니다
- * 포괄적인 랜섬웨어 방어를 위한 단일 제어 플레인 *

NetApp은 이러한 모든 것을 제공할 수 있습니다.



NetApp의 랜섬웨어 방어 포트폴리오

NetApp는 "랜섬웨어 방지 기능 내장"중요한 데이터를 실시간으로 강력한 다면적인 방어 기능을 제공합니다. 고급 AI 기반 감지 알고리즘은 데이터 패턴을 지속적으로 모니터링하여 99% 정확성으로 잠재적 랜섬웨어 위협을 신속하게 식별합니다. 공격에 신속하게 대응함으로써 신속하게 데이터를 스냅샷하고 복사본을 보호하여 신속한 복구를 보장합니다.

데이터를 더욱 강화하기 위해 NetApp의 "사이버 보관" 기능은 논리적 공극으로 데이터를 격리합니다. 중요한 데이터를 보호함으로써 신속한 비즈니스 연속성을 보장합니다.

NetApp"NetApp 랜섬웨어 보호" 단일 제어 평면을 통해 엔드 투 엔드 워크로드 중심 랜섬웨어 방어를 지능적으로 조정하고 실행하여 운영 부담을 줄여 단 한 번의 클릭으로 위험에 처한 중요한 워크로드 데이터를 식별하고 보호하고, 잠재적 공격의 영향을 제한하기 위해 정확하고 자동으로 감지하고 대응하고, 며칠이 아닌 몇 분 내에 워크로드를 복구하여 귀중한 워크로드 데이터를 보호하고 비용이 많이 드는 중단을 최소화할 수 있습니다.

데이터에 대한 무단 액세스를 보호하기 위한 기본 내장 ONTAP 솔루션에는 "다중 관리자 인증(MAV)"볼륨 삭제, 추가 관리 사용자 생성 또는 스냅샷 삭제와 같은 작업을 적어도 두 번째 지정된 관리자로부터 승인을 받은 후에만 수행할 수 있는 강력한 기능이 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다. 스냅샷을 삭제하기 전에 지정된 관리자 승인자를 원하는 수만큼 구성할 수 있습니다.

NetApp ONTAP는 "다중 요소 인증(MFA)" System Manager와 SSH CLI 인증의 웹 기반 요구사항을 해결합니다.

NetApp의 랜섬웨어 방지 기능은 끊임없이 변화하는 위협 환경에서 안심할 수 있도록 제공합니다. 이 포괄적인 접근 방식은 현재의 랜섬웨어 변종을 방어할 뿐만 아니라 새로운 위협에 대응하여 데이터 인프라에 장기적인 보안을 제공합니다.

다른 보호 옵션에 대해 알아봅니다

- "Digital Advisor 랜섬웨어 방어"
- "Data Infrastructure Insights 스토리지 워크로드 보안"
- "FPolicy를 참조하십시오"
- "SnapLock 및 변조 방지 스냅샷"

랜섬웨어 복구 보장

NetApp은 랜섬웨어 공격이 발생할 경우 스냅샷 데이터의 복원을 보장합니다. 보장: 스냅샷 데이터 복원을 지원할 수 없는 경우 NetApp이 바로잡을 것입니다. 이 보장은 AFF A-Series, AFF C-Series, ASA 및 FAS 시스템을 새로 구매할 때 사용할 수 있습니다.

자세한 정보

- "복구 보장 서비스 설명"
- "랜섬웨어 복구 보장 블로그"..

관련 정보

- "NetApp 지원 사이트 리소스 페이지"
- "NetApp 제품 보안"

랜섬웨어 보호를 위해 **SnapLock** 및 변조 방지 스냅샷

NetApp의 Snap Arsenal에서 중요한 무기는 랜섬웨어 위협을 방어하는 데 매우 효과적인 것으로 입증된 SnapLock입니다. SnapLock는 무단 데이터 삭제를 방지함으로써 추가적인 보안 계층을 제공하여 악의적인 공격이 발생했을 때도 중요 데이터를 그대로 유지하고 액세스할 수 있도록 합니다.

SnapLock 규정 준수

SLC(SnapLock Compliance)는 데이터를 지워지지 않는 보호 기능을 제공합니다. SLC는 관리자가 스토리지를 다시 초기화하려고 시도해도 데이터가 삭제되는 것을 금지합니다. 다른 경쟁 제품과 달리 SnapLock Compliance는 해당 제품의 지원 팀을 통해 사회 공학 해킹에 취약하지 않습니다. SnapLock Compliance 볼륨으로 보호되는 데이터는 만료 날짜에 도달할 때까지 복구할 수 있습니다.

SnapLock를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "SnapLock 설명서"

변조 방지 스냅샷

변조 방지 스냅샷(TPS) 복사본은 악의적인 공격으로부터 데이터를 보호하는 편리하고 빠른 방법을 제공합니다. SnapLock Compliance와 달리 TPS는 일반적으로 사용자가 정해진 시간 동안 데이터를 보호하고 빠른 복구를 위해 로컬에 남겨둘 수 있거나 운영 시스템에서 데이터를 복제할 필요가 없는 운영 시스템에서 사용됩니다. TPS는 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 ONTAP 관리자가 기본 스냅샷을 삭제하지 못하도록 방지합니다. 스냅샷과 SnapLock Compliance 볼륨의 삭제 불가능한 특성이 같지는 않지만 볼륨이 SnapLock를 사용하도록 설정되어 있지 않더라도 스냅샷 삭제는 금지됩니다.

스냅샷을 무단 변경으로부터 보호하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"..

FPolicy 파일 차단

FPolicy는 원치 않는 파일이 엔터프라이즈급 스토리지 어플라이언스에 저장되지 않도록 차단합니다. 또한 FPolicy는 알려진 랜섬웨어 파일 확장자를 차단하는 방법을 제공합니다. 사용자는 여전히 홈 폴더에 대한 모든 액세스 권한을 가지고 있지만 FPolicy는 관리자가 차단으로 표시한 파일을 사용자가 저장할 수 없도록 합니다. 해당 파일이 MP3 파일 또는 알려진 랜섬웨어 파일 확장자인지 여부는 중요하지 않습니다.

FPolicy 기본 모드로 악성 파일 차단

NetApp FPolicy 기본 모드(파일 정책 이라는 이름의 진화)는 파일 확장 차단 프레임워크로, 원치 않는 파일 확장명이 사용자 환경에 유입되는 것을 차단할 수 있습니다. 10년 이상 ONTAP의 일부였으며 랜섬웨어로부터 보호하는 데 매우 유용합니다. 이 제로 트러스트 엔진은 액세스 제어 목록(ACL) 권한을 넘어서는 추가 보안 조치를 취하기 때문에 유용합니다.

ONTAP System Manager와 NetApp Console 에서는 3000개가 넘는 파일 확장자 목록을 참조할 수 있습니다.

> 일부 확장은 사용자의 환경에서 합법적일 수 있으며 이러한 확장을 차단하면 예기치 않은 문제가 발생할 수 있습니다. 기본 FPolicy를 구성하기 전에 환경에 적합한 목록을 생성하십시오.

FPolicy 기본 모드는 모든 ONTAP 라이센스에 포함되어 있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 3부 - 강력한 기본(무료) 툴인 ONTAP FPolicy"

FPolicy 외부 모드로 사용자 및 엔터티 행동 분석(UEBA)을 설정합니다

FPolicy 외부 모드는 파일 활동 알림 및 제어 프레임워크로, 파일 및 사용자 활동에 대한 가시성을 제공합니다. 이러한 알림은 외부 솔루션에서 AI 기반 분석을 수행하여 악의적인 행동을 감지하는 데 사용할 수 있습니다.

특정 작업이 수행되도록 허용하기 전에 FPolicy 서버의 승인을 기다리도록 FPolicy 외부 모드도 구성할 수 있습니다. 이와 같은 여러 정책을 클러스터에서 구성할 수 있으므로 유연성이 크게 향상됩니다.

> FPolicy 서버는 승인을 제공하도록 구성된 경우 FPolicy 요청에 응답해야 합니다. 그렇지 않으면 스토리지 시스템 성능이 저하될 수 있습니다.

FPolicy 외부 모드가 에 포함되어 "모든 ONTAP 라이센스"있습니다.

자세한 정보

- "블로그: 랜섬웨어에 대항하기: 4부 - FPolicy 외부 모드를 사용하는 UBA 및 ONTAP"

Data Infrastructure Insights 스토리지 워크로드 보안

SWS(스토리지 워크로드 보안)는 ONTAP 환경의 보안 태세, 복구 가능성 및 책임성을 크게 향상시키는 NetApp Data Infrastructure Insights 의 기능입니다. SWS는 사용자 중심 접근

방식을 취해 환경 내 모든 인증된 사용자의 모든 파일 활동을 추적합니다. 이 솔루션은 고급 분석을 사용하여 모든 사용자의 일반적이고 계절적인 접속 패턴을 파악합니다. 이러한 패턴은 랜섬웨어 서명이 없어도 의심스러운 동작을 빠르게 식별하는 데 사용됩니다.

SWS가 잠재적인 랜섬웨어나 데이터 삭제를 감지하면 다음과 같은 자동 조치를 취할 수 있습니다.

- 영향을 받는 볼륨의 스냅샷을 생성합니다.
- 악의적인 활동으로 의심되는 사용자 계정 및 IP 주소를 차단합니다.
- 관리자에게 알림을 보냅니다.

내부자 위협을 빠르게 차단하고 모든 파일 활동을 추적하기 위해 자동화된 조치를 취할 수 있기 때문에 SWS를 사용하면 랜섬웨어 이벤트에서 훨씬 더 쉽고 빠르게 복구할 수 있습니다. 사용자는 고급 감사 및 포렌식 도구가 내장되어 있어 공격의 영향을 받은 볼륨 및 파일, 공격이 발생한 사용자 계정 및 수행된 악의적인 작업을 즉시 확인할 수 있습니다. 자동 스냅샷은 손상을 완화하고 파일 복원을 가속화합니다.

ONTAP의 ARP(자율적 랜섬웨어 방어)의 경고도 SWS에서 볼 수 있으므로 ARP와 SWS를 모두 사용하여 랜섬웨어 공격으로부터 보호할 수 있는 단일 인터페이스를 제공합니다.

자세한 정보

- "NetApp Data Infrastructure Insights"

NetApp ONTAP 내장형 AI 기반 감지 및 응답 기능

랜섬웨어 위협이 점점 더 정교해짐에 따라 방어 메커니즘도 갖춰져야 합니다. NetApp의 ARP(자율 랜섬웨어 방어)는 ONTAP에 내장된 지능형 이상 징후 감지 기능을 갖춘 AI를 기반으로 합니다. 이를 통해 사이버 레질리언스에 또 다른 방어 계층을 추가합니다.

ARP 및 ARP/AI는 ONTAP 내장 관리 인터페이스인 System Manager를 통해 구성할 수 있으며 볼륨별로 활성화됩니다.

자율 랜섬웨어 보호(ARP)

9.10.1 이후 내장된 또 다른 네이티브 ONTAP 솔루션인 ARP(자율 랜섬웨어 방어)는 NAS 스토리지 볼륨 워크로드 파일 활동 및 데이터 엔트로피를 연구하여 잠재적 랜섬웨어를 자동으로 감지합니다. ARP는 관리자에게 전례 없는 온박스(on-box) 잠재적인 랜섬웨어 감지를 위한 실시간 감지, 인사이트 및 데이터 복구 지점을 제공합니다.

ARP를 지원하는 ONTAP 9.15.1 및 이전 버전의 경우 ARP는 일반적인 작업 부하 데이터 활동을 학습하기 위해 학습 모드에서 시작됩니다. 대부분의 환경에서 이 작업에는 7일이 걸릴 수 있습니다. 학습 모드가 완료되면 ARP가 자동으로

활성 모드로 전환되어 랜섬웨어가 될 수 있는 비정상적인 워크로드 활동을 찾기 시작합니다.

비정상적인 활동이 감지되면 자동 스냅샷이 즉시 생성되므로 감염된 데이터를 최소화하면서 공격 시간과 최대한 가까운 복원 지점을 제공합니다. 이와 동시에 관리자가 비정상적인 파일 활동을 확인할 수 있도록 자동 경고(구성 가능)가 생성되므로 해당 활동이 실제로 악의적인지 확인하고 적절한 조치를 취할 수 있습니다.

작업이 예상 작업량인 경우 관리자는 이를 가양성 작업으로 쉽게 표시할 수 있습니다. ARP는 이 변경 사항을 정상적인 워크로드 활동으로 인식하여 앞으로 발생할 수 있는 공격 대상으로 더 이상 플래그를 지정하지 않습니다.

ARP를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "자율 랜섬웨어 보호"

자율 랜섬웨어 방어**/AI(ARP/AI)**

ONTAP 9.15.1에서 기술 미리보기로 소개된 ARP/AI는 NAS 스토리지 시스템을 온박스 실시간 감지를 한 차원 높여줍니다. 새로운 AI 기반 감지 기술은 100만 개 이상의 파일과 알려진 다양한 랜섬웨어 공격에 대해 훈련됩니다. ARP에서 사용되는 신호 외에 ARP/AI는 헤더 암호화도 감지합니다. AI 출력 및 추가 신호를 통해 ARP/AI는 99% 이상의 검출 정확도를 제공할 수 있습니다. 이는 ARP/AI가 AAA 등급에서 가장 높은 등급을 받은 독립 테스트 연구소인 SE Labs에 의해 검증되었습니다.

모델을 지속적으로 클라우드에서 훈련하기 때문에 ARP/AI는 학습 모드가 필요하지 않습니다. 이 기능은 켜지는 순간 활성화됩니다. 또한 지속적인 훈련은 새로운 랜섬웨어 공격이 발생했을 때 ARP/AI가 항상 검증된다는 것을 의미합니다. ARP/AI에는 모든 고객에게 새로운 매개 변수를 제공하여 랜섬웨어 탐지를 최신 상태로 유지하는 자동 업데이트 기능도 제공됩니다. ARP의 다른 모든 탐지, 인사이트 및 데이터 복구 지점 기능은 ARP/AI에 대해 유지됩니다.

ARP/AI를 활성화하려면 "ONTAP 1 을 참조하십시오"라이센스가 필요합니다.

자세한 정보

- "블로그:NetApp의 AI 기반 실시간 랜섬웨어 감지 솔루션은 AAA 등급을 획득했습니다"

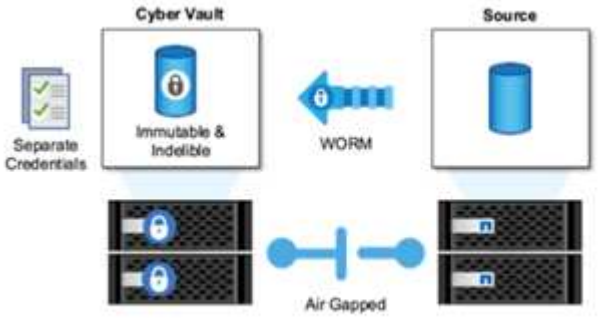
ONTAP의 사이버 보관을 이용한 에어갭 **WORM** 보호

NetApp의 사이버 소산 접근 방식은 논리적으로 에어갭 사이버 틈새를 위해 특별 제작된 참조 아키텍처입니다. 이 접근 방식은 보안 강화 및 SnapLock 같은 규정 준수 기술을 활용하여 변경 불가능하며 지워지지 않는 스냅샷을 허용합니다.

SnapLock Compliance과 논리적 격차가 있는 사이버 소산

공격자가 백업 사본을 폐기하고 경우에 따라 암호화하는 경향이 증가하고 있습니다. 따라서 사이버 보안 업계의 많은 기업들이 전반적인 사이버 복원력 전략의 일환으로 에어 갭 백업을 사용하도록 권장합니다.

문제는 기존 공기 격차(테이프 및 오프라인 미디어)가 복원 시간을 크게 증가시켜 가동 중지 시간과 전반적인 관련 비용을 증가시킬 수 있다는 것입니다. 에어 갭 솔루션에 대한 보다 현대적인 접근 방식도 문제가 될 수 있습니다. 예를 들어, 새 백업 복사본을 받기 위해 백업 볼트가 일시적으로 열렸다가 기본 데이터에 대한 네트워크 연결을 끊고 다시 한 번 "공기 차단"하는 경우 공격자는 임시 열기의 이점을 활용할 수 있습니다. 연결이 온라인 상태일 때 공격자는 데이터를 손상시키거나 파괴할 수 있습니다. 이러한 유형의 구성은 일반적으로 원치 않는 복잡성을 가중시킵니다. 논리적 공기 격차는 백업을 온라인 상태로 유지하면서 동일한 보안 보호 원칙을 가지고 있기 때문에 전통적인 또는 현대적인 공기 격차의 훌륭한 대안이 됩니다. NetApp를 사용하면 논리적 공기 가핑을 사용하여 테이프 또는 디스크 공기 게핑의 복잡성을 해결할 수 있으며, 이 작업은 변경 불가능한 스냅샷과 NetApp SnapLock Compliance로 달성할 수 있습니다.



NetApp은 10년 이상 SnapLock 기능을 발표하여 HIPAA(Health Insurance Portability and Accountability Act), 사베인즈 옥슬리(Sarbanes-Oxley) 및 기타 규정 데이터 규정 준수 요구 사항을 해결했습니다. 또한 기본 스냅샷을 SnapLock 볼륨에 저장하여 복사본을 WORM에 커밋하여 삭제를 방지할 수 있습니다. SnapLock 라이센스 버전은 SnapLock Compliance 및 SnapLock Enterprise의 두 가지입니다. 랜섬웨어 보호를 위해 NetApp은 ONTAP 관리자 또는 NetApp 지원팀에서도 스냅샷이 잠겨 있고 삭제할 수 없는 특정 보존 기간을 설정할 수 있으므로 SnapLock Compliance를 권장합니다.

자세한 정보

- "블로그: ONTAP 사이버 소산 개요"

변조 방지 스냅샷

SnapLock Compliance를 논리적 AIR Gap으로 활용하면 공격자가 백업 복사본을 삭제하지 못하도록 완벽하게 보호할 수 있지만, SnapVault를 사용하여 스냅샷을 2차 SnapLock 지원 볼륨으로 이동해야 합니다. 결과적으로 많은 고객이 네트워크를 통한 보조 스토리지에 이 구성을 구현합니다. 따라서 기본 스토리지에서 기본 볼륨 스냅샷을 복원하는 것보다 복원 시간이 더 길 수 있습니다.

ONTAP 9.12.1부터 무단 변경 방지 스냅샷은 기본 스토리지 및 기본 볼륨의 스냅샷에 대해 SnapLock Compliance 수준에 가까운 보호 기능을 제공합니다. SnapVault를 사용하여 스냅샷을 보조 SnapLocked 볼륨에 볼트할 필요가 없습니다. 변조 방지 스냅샷은 SnapLock 기술을 사용하여 동일한 SnapLock 보존 만료 기간을 사용하는 전체 ONTAP 관리자가 기본 스냅샷을 삭제하지 못하도록 방지합니다. 따라서 복원 시간이 빨라지고 무단 변경 방지 및 보호된 스냅샷으로 FlexClone 볼륨을 백업할 수 있습니다. 기존의 SnapLock Compliance 저장 스냅샷으로는 할 수 없는 작업입니다.

SnapLock Compliance 스냅샷과 무단 변경 방지 스냅샷의 주요 차이점은 만료 날짜에 도달하지 않은 SnapLock Compliance 볼륨에 저장된 스냅샷이 있을 경우 SnapLock Compliance에서는 ONTAP 어레이를 초기화하고 초기화할 수 없다는 것입니다. 스냅샷을 무단 변경으로부터 보호하려면 SnapLock Compliance 라이센스가 필요합니다.

자세한 정보

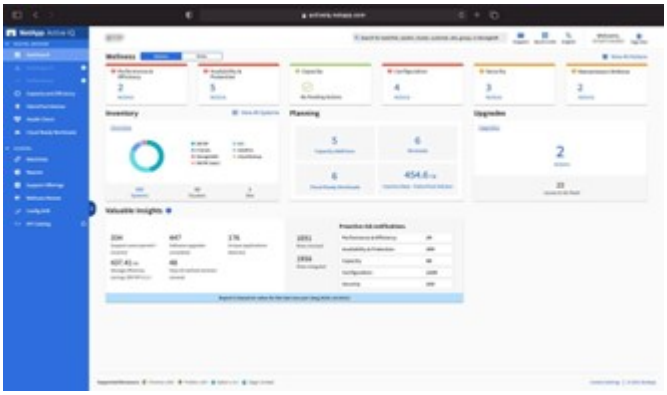
- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"

Digital Advisor 랜섬웨어 방어

Active IQ 기반 Digital Advisor는 실행 가능한 인텔리전스를 통해 최적의 데이터 관리를 지원하여 NetApp 스토리지의 사전 예방적 관리 및 최적화를 간소화합니다. 다양한 설치 기반에서 수집된 원격 측정 데이터를 활용하여 고급 AI 및 ML 기술을 통해 스토리지 환경의 위험을 줄이고 성능 및 효율성을 개선할 수 있는 기회를 발견합니다.

이 "NetApp 디지털 자문" 방법은 도움이 될 뿐만 "보안 취약점을 제거합니다" 아니라 랜섬웨어로부터 보호하는 것과 관련된 통찰력과 지침도 제공합니다. 전용 웰니스 카드는 필요한 조치와 해결된 위험을 보여줍니다. 따라서 시스템이

이러한 모범 사례 권장 사항을 충족하는지 확인할 수 있습니다.



랜섬웨어 방어 웰빙 페이지에서 추적된 위험 및 작업은 다음과 같습니다.

- 볼륨 스냅샷 수가 적기 때문에 잠재적인 랜섬웨어 방어가 줄어듭니다.
- NAS 프로토콜용으로 구성된 모든 SVM(스토리지 가상 머신)에 FPolicy가 사용되지 않는다.

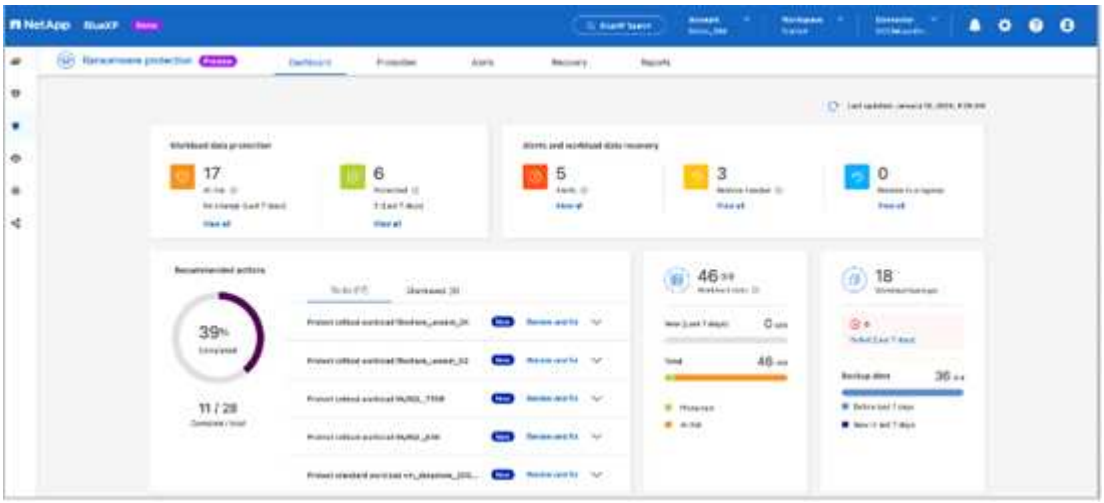
랜섬웨어 방어의 실제 적용 사례를 보려면 을 참조하십시오."디지털 자문업체"

NetApp 랜섬웨어 보호로 포괄적인 복원력 제공

랜섬웨어는 확산을 막고 비용이 많이 드는 가동 중지 시간을 피하기 위해 가능한 한 일찍 감지하는 것이 중요합니다. 그러나 효과적인 랜섬웨어 탐지 전략에는 단일 계층 이상의 보호가 포함되어야 합니다. NetApp의 랜섬웨어 보호는 NetApp Console 사용하여 데이터 서비스로 확장되는 실시간 온박스 기능과 사이버 보관을 위한 격리된 계층형 솔루션을 포함하는 포괄적인 접근 방식을 취합니다.

NetApp 랜섬웨어 보호

NetApp Console 포괄적이고 워크로드 중심의 랜섬웨어 방어를 지능적으로 조율하는 단일 제어 평면입니다. NetApp 랜섬웨어 보호는 ARP, FPolicy, 변조 방지 스냅샷과 같은 ONTAP 의 강력한 사이버 복원력 기능과 NetApp Backup and Recovery 와 같은 NetApp 데이터 서비스를 통합합니다. 또한 단일 UI를 통해 종단 간 방어를 제공하기 위해 자동화된 워크플로를 통해 권장 사항과 지침을 추가합니다. 공격이 발생한 경우 비즈니스를 운영하는 애플리케이션이 보호되고 최대한 빨리 복구될 수 있도록 워크로드 수준에서 작동합니다.



고객 이점:

- 랜섬웨어 대비 지원을 통해 운영 오버헤드를 줄이고 효율성을 높일 수 있습니다
- AI/ML을 통한 이상 징후 탐지는 정확성을 높이고 위험을 억제하기 위한 더 빠른 응답을 제공합니다
- 안내된 애플리케이션 정합성이 보장된 복원을 통해 몇 분 내에 워크로드를 더 쉽게 복구할 수 있습니다

"NetApp 랜섬웨어 보호"NIST 기능을 더 쉽게 구현할 수 있습니다.

- NetApp 스토리지의 데이터를 자동으로 검색 * 하고 우선 순위를 정할 수 있습니다 *.
- * 상위 워크로드 데이터 백업, 변경 불가, 보안 구성, 악성 파일 차단 및 다양한 보안 도메인에 대한 원 클릭 보호 *.
- * 차세대 AI 기반 이상 징후 감지 * 를 사용하여 * 랜섬웨어를 최대한 빠르게 * 감지합니다 *
- 응답 및 워크플로우 자동화, 최고의 * SIEM 및 XDR 솔루션 * 과의 통합
- 간소화된 * 오케스트레이션 * 을 통해 데이터를 빠르게 복원하여 애플리케이션 가동 시간을 단축합니다.
- 랜섬웨어 보호 * 전략 * 및 * 정책 * 을 구현하고 * 결과를 모니터링 * 하십시오.

NetApp와 제로 트러스트

NetApp와 제로 트러스트

제로 트러스트는 일반적으로 마이크로 코어 및 주변 장치(MCAP)를 설계하여 데이터, 서비스, 애플리케이션 또는 자산을 세그먼트 게이트웨이라고 하는 제어 기능으로 보호하는 네트워크 중심 접근 방식이었습니다. NetApp ONTAP는 제로 트러스트에 대한 데이터 중심 접근 방식을 취하고 있습니다. 제로 트러스트는 스토리지 관리 시스템이 세분화 게이트웨이가 되어 고객 데이터의 액세스 보호 및 모니터링을 수행합니다. 특히 FPolicy Zero Trust 엔진과 FPolicy 파트너 에코시스템은 정상 및 비정상적인 데이터 액세스 패턴을 세부적으로 이해하고 내부자 위협을 식별하기 위한 제어 센터가 됩니다.

2024년 7월부터 NetApp과 제로 트러스트: 데이터 중심의 제로 트러스트 모델 활성화 _ 의 내용이 docs.netapp.com 에서 제공됩니다. 이 모델은 이전에 PDF로 게시되었습니다.

데이터는 조직의 가장 중요한 자산입니다. 2022년 기준 내부자 위협은 데이터 침해의 18%가 원인입니다. "Verizon 데이터 침해 조사 보고서" 조직은 NetApp ONTAP 데이터 관리 소프트웨어를 사용하여 데이터에 관한 업계 최고 수준의 제로 트러스트 제어를 구현하여 경계를 강화할 수 있습니다.

Zero Trust란 무엇입니까??

제로 트러스트 모델은 Forrester Research의 John Kindervag에 의해 처음 개발되었습니다. 네트워크 보안은 외부에서 들어오는 것이 아니라 내부 외부로부터의 네트워크 보안을 지향합니다. 인사이드아웃 제로 트러스트 방식에서는 마이크로코어 및 경계(MCAP)를 식별합니다. MCAP는 포괄적인 제어 집합으로 보호할 데이터, 서비스, 애플리케이션 및 자산의 내부 정의입니다. 안전한 외주개념은 더 이상 유효하지 않습니다. 신뢰할 수 있고 경계를 통해 성공적으로 인증할 수 있는 엔터티는 조직이 공격에 취약해질 수 있습니다. 내부자는 정의상 이미 보안 경계의 내부에 있습니다. 직원, 계약업체 및 파트너는 내부자이며 조직의 인프라 내에서 역할을 수행하기 위해서는 적절한 제어하에 작업을 수행할 수 있어야 합니다.

제로 트러스트는 2019년 9월 DoD에 약속을 제공하는 기술로 언급되었습니다. "FY19-23 DoD 디지털 현대화 전략" 제로 트러스트를 데이터 침해를 막기 위해 아키텍처 전체에 보안을 통합하는 사이버 보안 전략인 "로 정의합니다. 이

데이터 중심 보안 모델은 신뢰할 수 있거나 신뢰할 수 없는 네트워크, 장치, 사용자 또는 프로세스의 개념을 없애고, 최소 권한 액세스라는 개념 하에서 인증 및 권한 부여 정책을 가능하게 하는 다중 속성 기반 신뢰 수준으로 전환합니다. 제로 트러스트를 구현하려면 기존 인프라를 사용하여 보안을 구현하는 방법을 보다 간단하고 효율적인 방식으로 설계하고 방해받지 않는 운영을 가능하게 해야 합니다."

2020년 8월 NIST 발표 "SPECIAL Pub 800-207 제로 트러스트 아키텍처" (ZTA), ZTA는 네트워크 위치가 더 이상 리소스의 보안 태세의 주요 구성 요소로 간주되지 않기 때문에 네트워크 세그먼트가 아닌 리소스 보호에 중점을 둡니다. 리소스는 데이터와 컴퓨팅입니다. ZTA 전략은 엔터프라이즈 네트워크 설계자를 위한 것입니다. ZTA는 원래 Forrester 개념에서 몇 가지 새로운 용어를 소개합니다. PDP(Policy Decision Point)와 PEP(Policy Enforcement Point)라는 보호 메커니즘은 Forrester 세그멘테이션 게이트웨이와 유사합니다. ZTA는 네 가지 배포 모델을 도입합니다.

- 장치 에이전트 또는 게이트웨이 기반 배포
- 독립 기반 구축(Forrester MCAP와 다소 유사함)
- 리소스 포털 기반 배포
- 장치 응용 프로그램 샌드박싱

이 설명서의 목적상 당사는 NIST ZTA 대신 Forrester Research의 개념과 용어를 사용합니다.

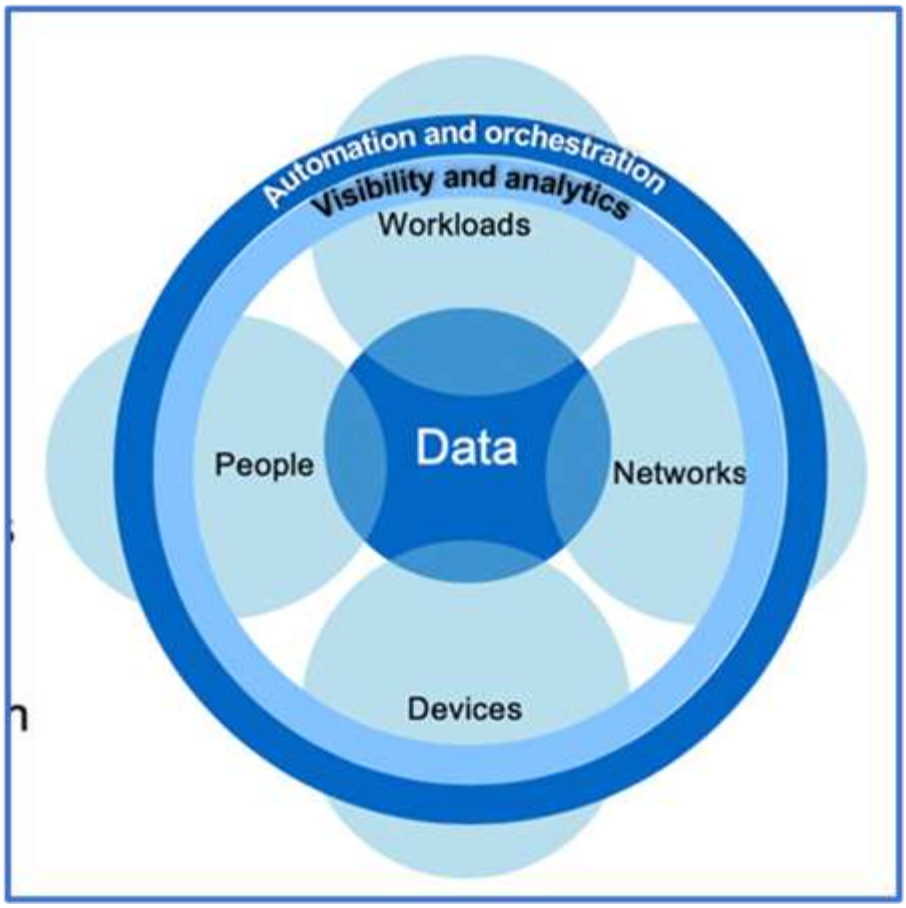
보안 리소스

취약성 및 사고 보고, NetApp 보안 응답 및 고객 기밀성에 대한 자세한 내용은 를 참조하십시오 "NetApp 보안 포털".

ONTAP로 제로 트러스트에 대한 데이터 중심 접근 방식 설계

제로 트러스트 네트워크는 데이터 중심 접근 방식으로 정의되며, 보안 제어는 데이터와 최대한 가까운 위치에 있어야 합니다. ONTAP의 기능을 NetApp FPolicy 파트너 에코시스템과 결합하여 데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공할 수 있습니다.

ONTAP는 NetApp의 보안이 풍부한 데이터 관리 소프트웨어이며, FPolicy 제로 트러스트 엔진은 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다.



제로 트러스트 데이터 중심 **MCAP** 설계

데이터 중심의 제로 트러스트 MCAP를 설계하려면 다음 단계를 따르십시오.

1. 모든 조직 데이터의 위치를 식별합니다.
2. 데이터를 분류합니다.
3. 더 이상 필요하지 않은 데이터는 안전하게 폐기합니다.
4. 데이터 분류에 액세스해야 하는 역할을 이해합니다.
5. 최소 권한 원칙을 적용하여 액세스 제어를 적용합니다.
6. 관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오.
7. 유휴 데이터와 사용 중인 데이터에 암호화 사용
8. 모든 액세스를 모니터링하고 기록합니다.
9. 의심스러운 액세스 또는 행동을 경고합니다.

모든 조직 데이터의 위치를 식별합니다

ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석에 대한 자세한 내용은 모든 액세스 모니터링 및 로그에서 설명합니다. 데이터가 어디에 있고 누가 데이터에 액세스할 수 있는지 모르는 경우 사용자 행동 분석을 통해 경험적 관찰을 통해 분류 및 정책을 수립할 수 있습니다.

데이터를 분류합니다

Zero Trust 모델의 용어로, 데이터 분류에는 유해 데이터를 식별하는 것이 포함됩니다. 유해 데이터는 조직 외부에 노출될 의도가 없는 민감한 데이터입니다. 유해 데이터가 공개되면 규정 준수에 문제가 생기고 조직의 평판이 손상될 수 있습니다. 규정 준수 측면에서 독성 데이터에는 카드 소지자 데이터가 포함됩니다. "PCI-DSS(Payment Card Industry Data Security Standard)" , EU의 개인 데이터 "일반 데이터 보호 규정(GDPR)" 또는 의료 데이터 "HIPAA(Health Insurance Portability and Accountability Act)" . NetApp 사용할 수 있습니다 "NetApp Data Classification" (이전 명칭: Cloud Data Sense)는 데이터를 자동으로 스캔, 분석, 분류하는 AI 기반 툴킷입니다.

더 이상 필요하지 않은 데이터는 안전하게 폐기합니다

조직의 데이터를 분류한 후 일부 데이터가 더 이상 필요하지 않거나 조직의 기능과 관련이 없다는 것을 알게 될 수 있습니다. 불필요한 데이터의 보유는 책임이며, 그러한 데이터는 삭제되어야 한다. 데이터를 암호화하여 삭제하는 고급 메커니즘은 저장된 데이터 암호화의 보안 삭제 설명을 참조하십시오.

데이터 분류에 액세스해야 하는 역할을 이해하고 액세스 제어를 적용하기 위해 최소 권한 원칙을 적용합니다

중요한 데이터에 대한 액세스를 매핑하고 최소 권한 원칙을 적용하면 조직 내 사용자가 작업을 수행하는 데 필요한 데이터만 액세스할 수 있습니다. 이 프로세스에는 역할 기반 액세스 제어가 포함되는데, 이 제어는 ("RBAC"데이터 액세스 및 관리 액세스에 적용됩니다.

ONTAP를 사용하면 스토리지 가상 머신(SVM)을 ONTAP 클러스터 내의 테넌트가 조직 데이터 액세스를 분할하는 데 사용할 수 있습니다. RBAC는 데이터 액세스뿐만 아니라 SVM에 대한 관리 액세스에도 적용할 수 있습니다. RBAC는 클러스터 관리 레벨에서 적용할 수도 있습니다.

RBAC와 더불어 MAV(ONTAP)를 사용하면 한 명 이상의 관리자가 또는 같은 명령을 승인하도록 할 수 있습니다 "다중 관리자 인증" `volume delete` `volume snapshot delete`. MAV가 활성화되면 MAV를 수정하거나 사용하지 않도록 하려면 MAV 관리자의 승인이 필요합니다.

스냅샷을 보호하는 또 다른 방법은 ONTAP를 "스냅샷 잠금"사용하는 것입니다. 스냅샷 잠금은 볼륨 스냅샷 정책에 대한 보존 기간에 수동 또는 자동으로 스냅샷을 지울 수 없는 SnapLock 기능입니다. 스냅샷 잠금은 무단 변경 방지 스냅샷 잠금이라고도 합니다. 스냅샷 잠금의 목적은 악의적인 관리자 또는 신뢰할 수 없는 관리자가 운영 및 보조 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 하는 것입니다. 랜섬웨어에 의해 손상된 볼륨을 복원하기 위해 기본 시스템에서 잠긴 스냅샷의 신속한 복구를 수행할 수 있습니다.

관리 액세스 및 데이터 액세스에 다단계 인증을 사용하십시오

클러스터 관리 RBAC 외에도 "다단계 인증(MFA)" ONTAP 웹 관리 액세스 및 SSH(Secure Shell) 명령줄 액세스용으로 구축할 수 있습니다. 관리 액세스를 위한 MFA는 미국 공공 부문 조직 또는 PCI-DSS를 준수해야 하는 조직의 요구 사항입니다. MFA를 사용하면 공격자가 사용자 이름과 암호만 사용하여 계정을 손상시킬 수 없습니다. MFA를 인증하려면 두 개 이상의 독립적인 요소가 필요합니다. 2단계 인증의 예로는 개인 키와 같이 사용자가 소유한 것과 암호 등 사용자가 알고 있는 것을 들 수 있습니다. ONTAP System Manager 또는 ActiveIQ Unified Manager에 대한 관리 웹 액세스는 SAML(Security Assertion Markup Language) 2.0을 통해 활성화됩니다. SSH 명령줄 액세스는 공개 키 및 암호와 함께 연결된 2단계 인증을 사용합니다.

ONTAP의 ID 및 액세스 관리 기능을 사용하여 API를 통해 사용자 및 시스템 액세스를 제어할 수 있습니다.

- 사용자:
  - 인증 및 권한 부여 SMB 및 NFS용 NAS 프로토콜 기능을 사용합니다.
  - * 감사 * 액세스 및 이벤트의 syslog. 인증 및 권한 부여 정책을 테스트하기 위한 CIFS 프로토콜에 대한 자세한 감사 로깅 파일 수준에서 세부적인 NAS 액세스에 대한 FPolicy 감사
- 장치:

- * 인증. * API 액세스를 위한 인증서 기반 인증.
- * 승인. * 기본 또는 맞춤형 역할 기반 액세스 제어(RBAC)
- * 감사 * 수행한 모든 작업의 syslog.

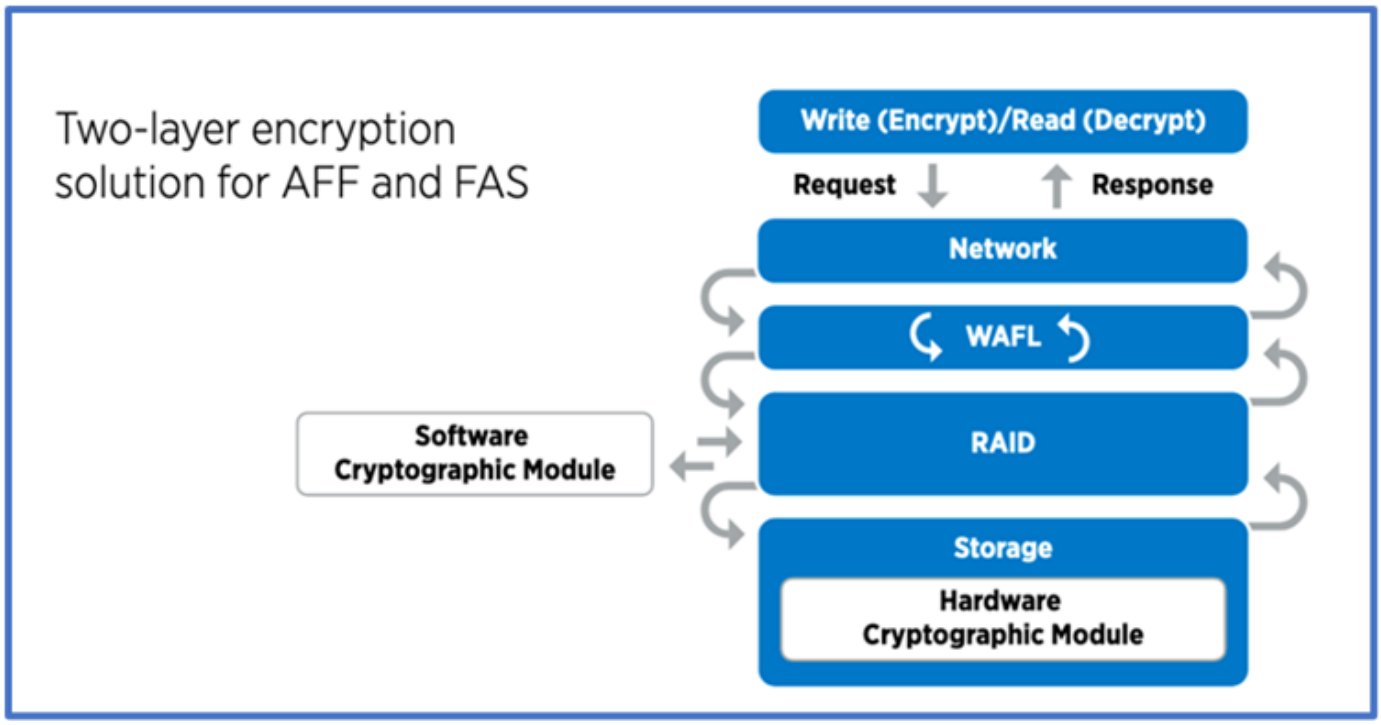
유휴 데이터와 사용 중인 데이터에 암호화 사용

유휴 데이터의 암호화

조직에서 드라이브의 용도를 변경하거나 결함 있는 드라이브를 반환하거나 판매 또는 거래하여 대용량 드라이브로 업그레이드하는 경우, 스토리지 시스템의 위험과 인프라 격차를 줄이기 위한 새로운 요구사항이 있습니다. 스토리지 엔지니어는 데이터의 관리자이자 운영자로서 라이프사이클 전반에서 데이터를 안전하게 관리하고 유지해야 합니다. "NetApp 스토리지 암호화(NSE) 및 AMP, #44, NetApp 볼륨 암호화(NVE) 및 AMP, #44, NetApp 애그리게이트 암호화" 독성 여부와 관계없이 일상 작업에 영향을 주지 않고 유휴 데이터를 항상 암호화할 수 있도록 지원합니다. "NSE를 선택합니다" 는 FIPS 140-2 레벨 2 검증된 자체 암호화 드라이브를 사용하는 ONTAP 하드웨어 "사용되지 않는 데이터" 솔루션입니다. "NVE와 NAE" 는 를 사용하는 ONTAP 소프트웨어 "사용되지 않는 데이터" "FIPS 140-2 Level 1 검증 NetApp 암호화 모듈"솔루션입니다. NVE와 NAE에서는 하드 드라이브 또는 Solid State Drive를 유휴 데이터 암호화에 사용할 수 있습니다. 또한 NSE 드라이브를 사용하여 암호화 이중화와 추가 보안을 제공하는 네이티브 계층화된 암호화 솔루션을 제공할 수 있습니다. 한 계층이 침해되더라도 두 번째 계층은 여전히 데이터를 보호합니다. 이러한 기능을 통해 ONTAP은 에 대한 유리한 위치를 점할 수 "양자 지원 암호화"있습니다.

NVE는 기밀 파일이 기밀이 아닌 볼륨에 작성될 때 데이터 유출로부터 독성 데이터를 암호화 방식으로 제거하는 기능을 "안전한 제거" 제공합니다.

ONTAP에 내장된 키 관리자인 를 "온보드 키 관리자(OKM)"사용하거나 "승인됨" , NSE 및 NVE와 함께 타사 "외부 키 관리자" 를 사용하여 키 자료를 안전하게 저장할 수 있습니다.



위의 그림에서 볼 수 있듯이 하드웨어 및 소프트웨어 기반 암호화를 결합할 수 있습니다. 이 기능으로 인해 는 "기밀 프로그램을 위한 NSA의 상용 솔루션에 대한 ONTAP 검증" 최고 비밀 데이터를 저장할 수 있게 되었습니다.

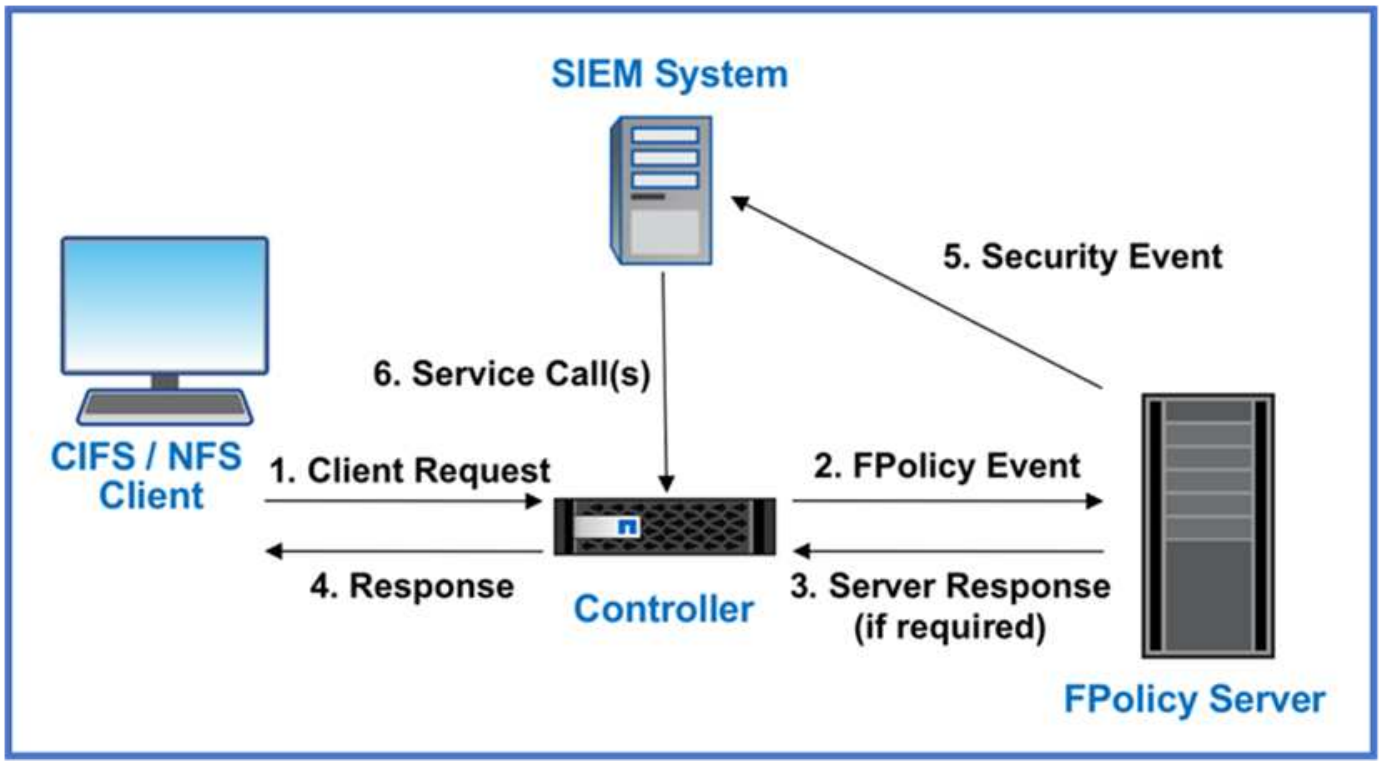
전송 중인 데이터 암호화

ONTAP의 전송 중인 데이터 암호화는 사용자 데이터 액세스 및 제어 플레인 액세스를 보호합니다. 사용자 데이터 액세스는 Microsoft CIFS 공유 액세스의 경우 SMB 3.0 암호화 또는 NFS Kerberos 5의 경우 krb5P로 암호화될 수 있습니다. CIFS, NFS 및 iSCSI에 대해 사용자 데이터 액세스를 암호화할 수도 "IPsec을 선택합니다" 있습니다. 컨트롤 플레인 액세스는 TLS(Transport Layer Security)로 암호화됩니다. ONTAP는 제어 플레인 액세스를 위한 규정 준수 모드를 제공하여 "FIPS 를 참조하십시오"FIPS 승인 알고리즘을 활성화하고 FIPS가 승인되지 않은 알고리즘을 비활성화합니다. 데이터 복제는 로 암호화됩니다. "클러스터 피어 암호화" ONTAP SnapVault 및 SnapMirror 기술에 대한 암호화를 제공합니다.

모든 액세스를 모니터링하고 기록합니다

RBAC 정책을 적용한 후에는 활성 모니터링, 감사 및 알림을 배포해야 합니다. NetApp ONTAP의 FPolicy 제로 트러스트 엔진을 과 결합하여 "NetApp FPolicy 파트너 에코시스템"데이터 중심 제로 트러스트 모델에 필요한 제어 기능을 제공합니다. NetApp ONTAP는 보안이 풍부한 데이터 관리 소프트웨어이며 "FPolicy를 참조하십시오" , 세부적인 파일 기반 이벤트 알림 인터페이스를 제공하는 업계 최고의 ONTAP 기능입니다. NetApp FPolicy 파트너는 이 인터페이스를 사용하여 ONTAP 내의 데이터 액세스를 더욱 잘 파악할 수 있습니다. ONTAP의 FPolicy 기능과 FPolicy 파트너의 NetApp 제휴 파트너 에코시스템과 결합하여 조직의 데이터가 어디에 있고 누가 액세스하는지를 파악할 수 있습니다. 이 작업은 데이터 액세스 패턴의 유효성 여부를 식별하는 사용자 행동 분석을 통해 수행됩니다. 사용자 행동 분석을 사용하여 정상적인 패턴에서 벗어난 의심스럽거나 잘못된 데이터 액세스를 경고하고 필요한 경우 액세스를 거부하기 위한 조치를 취할 수 있습니다.

FPolicy 파트너는 사용자 행동 분석을 넘어 머신 러닝(ML) 및 인공 지능(AI)으로 이동하여 이벤트 충실도를 높이고 오탐률을 줄이고 있습니다. 모든 이벤트는 syslog 서버 또는 ML 및 AI를 활용할 수 있는 SIEM(Security Information and Event Management) 시스템에 로깅해야 합니다.



NetApp의 "DII 스토리지 워크로드 보안" 클라우드와 온프레미스 ONTAP 스토리지 시스템 모두에서 FPolicy 인터페이스와 사용자 행동 분석을 활용하여 악의적인 사용자 행동에 대한 실시간 알림을 제공합니다. 스토리지 워크로드 보안은 고급 머신 러닝과 이상 감지를 통해 악의적이거나 손상된 사용자가 조직 데이터를 오용하는 것을 방지합니다. 스토리지 워크로드 보안은 랜섬웨어 공격이나 기타 악의적인 행위를 식별하고 스냅샷을 호출하고 악의적인 사용자를 격리할 수 있습니다. 스토리지 워크로드 보안에는 사용자 및 엔터티 활동을 매우 자세히 볼 수 있는 포렌식 기능도

있습니다. 스토리지 워크로드 보안은 NetApp Data Infrastructure Insights 의 일부입니다.

ONTAP에는 스토리지 워크로드 보안뿐만 아니라 (ARP)라고 하는 온보드 랜섬웨어 감지 기능이 "자율 랜섬웨어 보호" 있습니다. ARP는 머신 러닝을 사용하여 비정상적인 파일 활동이 랜섬웨어 공격이 진행 중임을 나타내고 스냅샷을 호출하고 관리자에게 경고를 보냅니다. 스토리지 워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 외부 NetApp 보안 자동화 및 오케스트레이션 제어

자동화를 통해 최소한의 인적 지원만으로 프로세스 또는 절차를 수행할 수 있습니다. 조직은 자동화를 통해 제로 트러스트 구축을 수동 절차를 훨씬 넘어 확장할 수 있으므로 자동화되는 악의적인 활동을 방지할 수 있습니다.

Ansible은 오픈 소스 소프트웨어 프로비저닝, 구성 관리 및 애플리케이션 배포 툴입니다. 많은 유닉스와 유사한 시스템에서 실행되며, 유닉스와 유사한 시스템과 Microsoft Windows를 모두 구성할 수 있습니다. 시스템 구성을 설명하는 고유한 선언적 언어가 포함되어 있습니다. Ansible은 Michael DeHaan이 작성했으며 2015년에 Red Hat에 인수되었습니다. Ansible은 에이전트가 없습니다. SSH 또는 Windows 원격 관리를 통해 일시적으로 원격으로 연결하여 원격 PowerShell 실행 허용 을 수행할 수 있습니다. NetApp은 그 이상을 개발했으며 "ONTAP 소프트웨어용 Ansible 모듈 150개"Ansible 자동화 프레임워크와 추가적인 통합을 가능하게 했습니다. NetApp용 Ansible 모듈은 원하는 상태를 정의하고 타겟 NetApp 환경에 전달하는 방법에 관한 일련의 지침을 제공합니다. 이들 모듈은 라이센스 설정, 애그리게이트 및 스토리지 가상 머신 생성, 볼륨 생성, 스냅샷 복원 등의 작업을 지원할 목적으로 개발되었습니다. Ansible 역할은 NetApp DoD UC(Unified Capabilities "GitHub에 게시되었습니다") 배포 가이드에 따라 다릅니다.

사용자는 사용 가능한 모듈 라이브러리를 통해 쉽게 Ansible 플레이북을 개발하고 고유한 애플리케이션 및 비즈니스 요구사항에 맞게 맞춤화하여 일상적인 작업을 자동화할 수 있습니다. 플레이북을 작성한 후 특정 작업을 수행하도록 실행하면 시간이 절약되고 생산성이 향상됩니다. NetApp은 직접 사용하거나 필요에 맞게 맞춤화할 수 있는 샘플 플레이북을 마련하여 공유했습니다.

Data Infrastructure Insights 는 전체 인프라에 대한 가시성을 제공하는 인프라 모니터링 도구입니다. Data Infrastructure Insights 사용하면 퍼블릭 클라우드 인스턴스와 프라이빗 데이터 센터를 포함한 모든 리소스를 모니터링하고, 문제를 해결하고, 최적화할 수 있습니다. Data Infrastructure Insights 해결에 걸리는 평균 시간을 90%까지 단축하고 클라우드 문제의 80%가 최종 사용자에게 영향을 미치지 않도록 예방할 수 있습니다. 또한 실행 가능한 인텔리전스로 데이터를 보호함으로써 클라우드 인프라 비용을 평균 33% 절감하고 내부 위협에 대한 노출도 줄일 수 있습니다. Data Infrastructure Insights 의 스토리지 워크로드 보안 기능을 사용하면 AI와 ML을 활용한 사용자 행동 분석을 통해 내부 위협으로 인해 비정상적인 사용자 행동이 발생할 때 경고를 받을 수 있습니다. ONTAP 의 경우, 스토리지 워크로드 보안은 Zero Trust FPolicy 엔진을 활용합니다.

제로 트러스트 및 하이브리드 클라우드 구축

NetApp 은 하이브리드 클라우드의 데이터 권위자입니다. NetApp Amazon Web Services(AWS), Microsoft Azure, Google Cloud 및 기타 주요 클라우드 공급업체와 협력하여 온프레미스 데이터 관리 시스템을 하이브리드 클라우드로 확장하기 위한 다양한 옵션을 제공합니다. NetApp 하이브리드 클라우드 솔루션은 온프레미스 ONTAP 시스템 및 ONTAP Select 소프트웨어 정의 스토리지에서 사용할 수 있는 것과 동일한 Zero Trust 보안 제어를 지원합니다.

AWS(FSxN), Google Cloud(GCNV), Microsoft Azure용 Azure NetApp Files 등 엔터프라이즈급 클라우드 기반 파일 서비스를 사용하면 일반적인 CAPEX 제약 없이 퍼블릭 클라우드에서 용량을 쉽게 확장할 수 있습니다. 분석 및 DevOps와 같은 데이터 집약적 워크로드에 적합한 이러한 클라우드 데이터 서비스는 NetApp 의 탄력적인 온디맨드

스토리지 서비스와 ONTAP 데이터 관리를 완벽하게 관리되는 제품으로 결합합니다.

ONTAP NetApp SnapMirror 데이터 복제 소프트웨어를 통해 온프레미스 ONTAP 시스템과 AWS, Google Cloud 또는 Azure 스토리지 환경 간에 데이터를 이동할 수 있도록 합니다.

속성 기반 액세스 제어

ONTAP로 속성 기반 액세스 제어

9.12.1부터 ONTAP를 NFSv4.2 보안 레이블 및 확장 속성(xattrs)으로 구성하여 특성 및 ABAC(속성 기반 액세스 제어)를 포함하는 RBAC(역할 기반 액세스 제어)를 지원할 수 있습니다.

ABAC는 사용자 속성, 리소스 속성 및 환경 조건을 기반으로 사용 권한을 정의하는 권한 부여 전략입니다. ONTAP와 NFS v4.2 보안 레이블 및 xattrs의 통합은 NIST 특별 간행물 800-162에 명시된 ABAC 솔루션에 대한 NIST 표준을 준수합니다.

NFS v4.2 보안 레이블 및 xattrs를 사용하여 파일에 사용자 정의 속성 및 레이블을 할당할 수 있습니다. ONTAP는 ABAC 지향 ID 및 액세스 관리 소프트웨어와 통합하여 이러한 속성 및 레이블을 기반으로 세분화된 파일 및 폴더 액세스 제어 정책을 적용할 수 있습니다.

관련 정보

- "ABAC에 대한 ONTAP의 접근 방식"
- "NFS in NetApp ONTAP: 모범 사례 및 구축 가이드"

ONTAP의 ABAC(속성 기반 액세스 제어)에 대한 접근 방식입니다

ONTAP는 NFS v4.2 보안 레이블 및 NFS를 사용한 확장 특성(xattrs)을 비롯하여 파일 수준 ABAC(속성 기반 액세스 제어)를 달성하는 데 사용할 수 있는 몇 가지 접근 방식을 제공합니다.

NFS v4.2 보안 레이블

ONTAP 9.9.1부터 NFS라는 이름의 NFS v4.2 기능이 지원됩니다.

NFS v4.2 보안 레이블은 SELinux 레이블 및 MAC(필수 액세스 제어)를 사용하여 세분화된 파일 및 폴더 액세스를 관리하는 방법입니다. 이러한 MAC 레이블은 파일과 폴더와 함께 저장되며 UNIX 권한 및 NFS v4.x ACL과 함께 작동합니다.

NFS v4.2 보안 레이블을 지원한다는 것은 ONTAP가 이제 NFS 클라이언트의 SELinux 레이블 설정을 인식하고 이해한다는 것을 의미합니다. NFS v4.2 보안 레이블은 RFC-7204에 설명되어 있습니다.

NFS v4.2 보안 레이블의 사용 사례는 다음과 같습니다.

- 가상 머신(VM) 이미지의 MAC 레이블 지정
- 공공 부문의 데이터 보안 분류(비밀, 최고 비밀 및 기타 분류)
- 보안 규정 준수
- 디스크 없는 Linux

NFS v4.2 보안 레이블을 사용하도록 설정합니다

다음 명령을 사용하여 NFS v4.2 보안 레이블을 설정하거나 해제할 수 있습니다(고급 권한 필요).

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

에 대한 자세한 내용은 `vserver nfs modify` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS v4.2 보안 레이블에 대한 적용 모드입니다

ONTAP 9.9.1부터 ONTAP는 다음 적용 모드를 지원합니다.

- 제한된 서버 모드: ONTAP는 라벨을 적용할 수 없지만 라벨을 저장 및 전송할 수 있습니다.

  MAC 레이블을 변경하는 기능은 클라이언트에 달려 있습니다.

- * 게스트 모드 *: 클라이언트가 NFS-Aware(v4.1 이하)로 표시되지 않으면 MAC 레이블이 전송되지 않습니다.

  ONTAP는 현재 전체 모드를 지원하지 않습니다(MAC 레이블 저장 및 적용).

NFS v4.2 보안 레이블 예

다음 예제 구성은 Red Hat Enterprise Linux 릴리스 9.3(Plow)을 사용하는 개념을 보여 줍니다.

John R. Smith의 자격 증명을 기반으로 생성된 사용자는 `jrsmith` 다음과 같은 계정 Privileges를 가지고 있습니다.

- 사용자 이름 = `jrsmith`
- Privileges= `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

다음 MLS Privileges 표에 설명된 대로 권한이 있는 사용자인 관리자 계정과 사용자라는 두 가지 역할이 있습니다. `jrsmith`

사용자	역할	유형	레벨
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

이 예제 환경에서는 사용자가 `jrsmith` 에 있는 `s3` 수준의 파일에 액세스할 수 `s0` 있습니다. 관리자가 사용자 관련 데이터에 액세스하지 못하도록 하기 위해 아래에 설명된 대로 기존 보안 분류를 개선할 수 있습니다.

- S0 = 권한 관리자 사용자 데이터
- S0 = 분류되지 않은 데이터
- S1 = 대외비
- S2 = 비밀 데이터

- S3 = 상위 암호 데이터

MCS를 사용하는 **NFS v4.2** 보안 레이블 예

MLS(다중 수준 보안) 외에도 MCS(다중 범주 보안)라는 또 다른 기능을 사용하여 프로젝트와 같은 범주를 정의할 수 있습니다.

NFS 보안 레이블	값
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

확장 속성**(xattrs)**

ONTAP 9.12.1부터 ONTAP는 xattrs.xattrs를 지원하므로 ACL(액세스 제어 목록) 또는 사용자 정의 속성과 같이 시스템에서 제공하는 것 이상의 파일 및 디렉토리와 메타데이터를 연결할 수 있습니다.

xattrs를 구현하려면 Linux에서 및 `getfattr` 명령줄 유틸리티를 사용할 수 `setfattr` 있습니다. 이러한 도구는 파일과 디렉토리에 대한 추가 메타데이터를 관리하는 강력한 방법을 제공합니다. 부적절하게 사용하면 예기치 않은 동작 또는 보안 문제가 발생할 수 있으므로 주의하여 사용해야 합니다. 자세한 사용 지침은 항상 `setfattr` 및 `getfattr` man 페이지 또는 기타 신뢰할 수 있는 문서를 참조하십시오.

ONTAP 파일 시스템에서 xattrs가 활성화된 경우 사용자는 파일에 대한 임의의 속성을 설정, 수정 및 검색할 수 있습니다. 이러한 특성은 액세스 제어 정보와 같은 표준 파일 속성 집합으로 캡처되지 않은 파일에 대한 추가 정보를 저장하는 데 사용할 수 있습니다.

ONTAP에서 xattrs를 사용하기 위한 몇 가지 요구 사항과 제한 사항이 있습니다.

- Red Hat Enterprise Linux 8.4 이상
- Ubuntu 22.04 이상
- 각 파일에는 최대 128개의 xattrs를 포함할 수 있습니다
- Xattr 키는 255바이트로 제한됩니다
- 결합된 키 또는 값 크기는 xattr 당 1,729바이트입니다
- 디렉터리 및 파일에는 xattrs가 있을 수 있습니다
- xattrs를 설정 및 검색하려면 `w` 사용자 및 그룹에 대해 쓰기 모드 비트를 활성화해야 합니다

Xattrs는 사용자 네임스페이스 내에서 활용되며 ONTAP 자체에는 고유한 의미를 부여하지 않습니다. 대신 실제 애플리케이션은 파일 시스템과 상호 작용하는 클라이언트측 애플리케이션에 의해 결정되고 관리됩니다.

Xattr 사용 사례 예:

- 파일 생성을 담당하는 응용 프로그램의 이름을 기록합니다
- 파일을 가져온 이메일 메시지에 대한 참조 유지 관리
- 파일 객체 구성을 위한 범주화 프레임워크 설정
- 원본 다운로드 소스의 URL로 파일 레이블 지정

xattrs 관리 명령입니다

- `setfattr` 파일 또는 디렉토리의 확장 속성을 설정합니다.

  `setfattr -n <attribute_name> -v <attribute_value> <file or directory name>`

  명령 예:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` 특정 확장 특성의 값을 검색하거나 파일 또는 디렉토리의 모든 확장 특성을 나열합니다.

  특정 속성:
  `getfattr -n <attribute_name> <file or directory name>`

  모든 속성:
  `getfattr <file or directory name>`

  명령 예:

  ```
  getfattr -n user.comment example.txt
  ```

Xattr 키 값 쌍의 예

다음 표에서는 두 개의 xattr 키 값 쌍의 예를 보여 줍니다.

문자 수	값
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

xattrs에 대한 **ACE**의 사용자 권한

ACE(액세스 제어 항목)는 파일 또는 디렉터리와 같은 특정 리소스에 대해 개별 사용자 또는 사용자 그룹에 부여된 액세스 권한이나 권한을 정의하는 ACL 내의 구성 요소입니다. 각 ACE는 허용 또는 거부된 액세스 유형을 지정하며 특정 보안 주체(사용자 또는 그룹 ID)와 연결됩니다.

xattrs에 **ACE(**액세스 제어 항목**)**가 필요합니다

- xattr 검색: 사용자가 파일이나 디렉터리의 확장 속성을 읽는 데 필요한 권한입니다. "R"은 읽기 권한이 필요하다는 것을 나타냅니다.
- xattrs 설정: 확장 속성을 수정하거나 설정하는 데 필요한 권한. "a,""w" 및 "T"는 추가, 쓰기 및 xattrs와 관련된 특정 사용 권한 등 다양한 사용 권한의 예를 나타냅니다.
- 파일: 사용자는 확장 속성을 설정하려면 추가, 쓰기 및 xattrs와 관련된 특수 권한이 필요합니다.

- 디렉토리: 확장 속성을 설정하려면 특정 권한 "T"가 필요합니다.

파일 형식	**xattr**를 검색합니다	**xattrs**를 설정합니다
파일	R	a, w, T, 키
디렉토리	R	T

ABAC ID 및 액세스 제어 소프트웨어와의 통합

ABAC의 기능을 최대한 활용하기 위해 ONTAP는 ABAC 중심의 ID 및 액세스 관리 소프트웨어와 통합할 수 있습니다.

ABAC 시스템에서는 PEP(Policy Enforcement Point)와 PDP(Policy Decision Point)가 중요한 역할을 합니다. PEP는 액세스 제어 정책을 적용하는 역할을 담당하며 PDP는 정책에 따라 액세스 허용 또는 거부 여부를 결정합니다.

실용적인 환경에서 조직은 NFS 보안 레이블과 xattrs를 혼합하여 사용할 수 있습니다. 이러한 메타데이터는 분류, 보안, 애플리케이션, 콘텐츠 등 다양한 메타데이터를 나타내는 데 사용되며, 이는 모두 ABAC 결정에 중요한 역할을 합니다. 예를 들어 xattrs는 PDP가 의사 결정 프로세스에 사용하는 리소스 속성을 저장하는 데 사용될 수 있습니다. 파일의 분류 수준(예: "분류되지 않음", "기밀", "비밀" 또는 "최고 비밀")을 나타내도록 속성을 정의할 수 있습니다. 그런 다음 PDP는 이 속성을 활용하여 사용자가 분류 수준이 허용 수준 이하인 파일만 액세스하도록 제한하는 정책을 적용할 수 있습니다.

> 이 컨텐츠는 고객의 ID, 인증 및 액세스 서비스에 최소한 파일 시스템에 대한 액세스를 위한 중개인 역할을 하는 PEP와 PDP가 포함되어 있다고 가정합니다.

ABAC에 대한 프로세스 흐름의 예

1. 사용자가 PEP에 대한 시스템 액세스에 대한 자격 증명(예: PKI, OAuth, SAML)을 제공하고 PDP에서 결과를 가져옵니다.

   PEP의 역할은 사용자의 액세스 요청을 가로채서 PDP로 전달하는 것입니다.

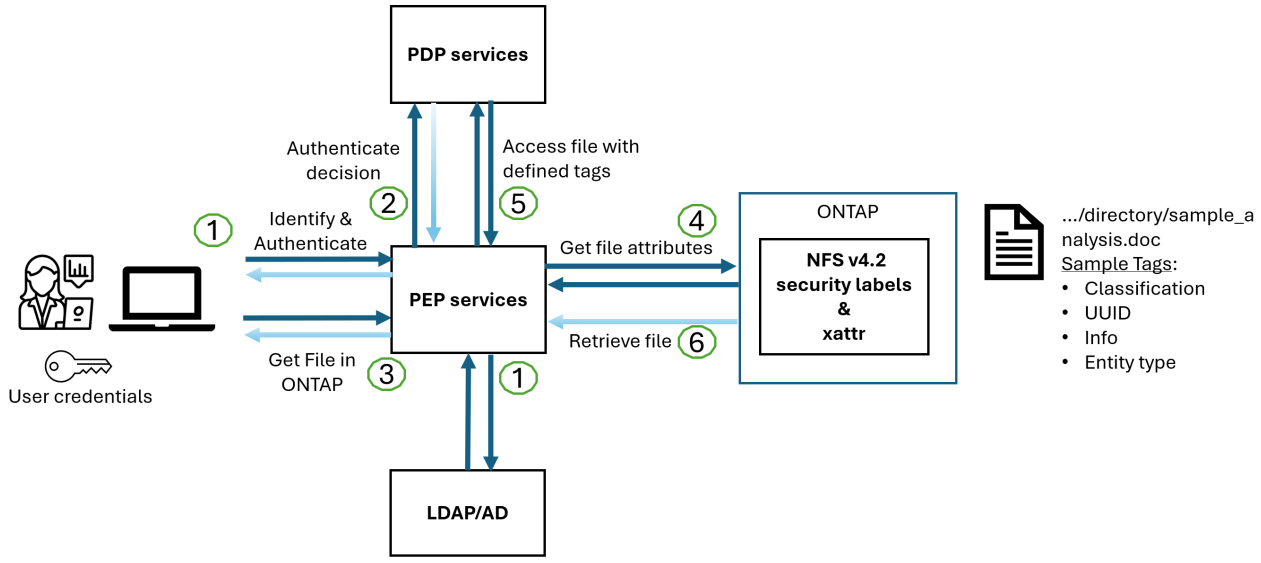
2. 그런 다음 PDP는 설정된 ABAC 정책에 대해 이 요청을 평가합니다.

   이러한 정책에서는 사용자, 해당 리소스 및 주변 환경과 관련된 다양한 특성을 고려합니다. 이러한 정책에 따라 PDP는 액세스 권한을 허용하거나 거부하도록 결정한 다음 이 결정을 다시 PEP에 전달합니다.

   PDP는 PEP에 적용할 정책을 제공합니다. 그런 다음 PEP는 PDP의 결정에 따라 사용자의 액세스 요청을 허용하거나 거부하여 이 결정을 적용합니다.

3. 요청이 성공하면 사용자는 ONTAP에 저장된 파일(예: AFF, AFF-C)을 요청합니다.
4. 요청이 성공하면 PEP는 문서에서 미세 입자 액세스 제어 태그를 가져옵니다.
5. PEP는 해당 사용자의 인증서를 기반으로 사용자에 대한 정책을 요청합니다.
6. PEP는 사용자가 파일에 액세스할 수 있고 사용자가 파일을 검색할 수 있는 경우 정책 및 태그에 따라 결정합니다.

> 실제 액세스는 토큰을 사용하여 수행할 수 있습니다.



ONTAP 클론 복제 및 **SnapMirror**

ONTAP의 클론 생성 및 SnapMirror 기술은 파일 데이터의 모든 측면을 보존하고 파일과 함께 전송할 수 있도록 효율적이고 안정적인 데이터 복제 및 복제 기능을 제공하도록 설계되었습니다. xattrs는 보안 레이블, 액세스 제어 정보, 사용자 정의 데이터 등 파일과 관련된 추가 메타데이터를 저장하는 데 있어 중요한 역할을 합니다.

ONTAP의 FlexClone 기술을 사용하여 볼륨을 클론 복제하면 볼륨의 쓰기 가능한 정확한 복제본이 생성됩니다. 이 복제 프로세스는 즉각적이고 공간 효율적이며 모든 파일 데이터와 메타데이터가 포함되어 xattrs가 완전히 복제되도록 합니다. 마찬가지로, SnapMirror는 데이터가 완벽한 충실도로 보조 시스템에 미러링되도록 보장합니다. 여기에는 이 메타데이터에 의존하는 응용 프로그램이 올바르게 작동하는 데 중요한 xattrs가 포함됩니다.

NetApp ONTAP는 클론 복제 및 복제 작업에 xattrs를 포함함으로써 모든 특성을 갖춘 전체 데이터 세트를 운영 및 2차 스토리지 시스템에서 일관되게 사용할 수 있도록 보장합니다. 일관된 데이터 보호, 빠른 복구, 규정 준수 및 규정 준수 표준을 준수해야 하는 조직에는 이러한 포괄적인 데이터 관리 접근 방식이 필수적입니다. 또한 온프레미스와 클라우드에서 다양한 환경에서 데이터 관리를 간소화하여 이러한 프로세스 중에 데이터가 완전하고 변경되지 않았다는 확신을 사용자에게 제공합니다.

NFS v4.2 보안 레이블에는 에 정의된 문제점이 NFS v4.2 보안 레이블있습니다.

라벨에 대한 변경 감사

xattrs 또는 NFS 보안 레이블의 변경 사항을 감사하는 것은 파일 시스템 관리 및 보안의 중요한 부분입니다. 표준 파일 시스템 감사 툴을 사용하면 xattrs 및 보안 레이블 수정을 비롯하여 파일 시스템에 대한 모든 변경 사항을 모니터링하고 기록할 수 있습니다.

Linux 환경에서 `auditd` 데몬은 일반적으로 파일 시스템 이벤트에 대한 감사를 설정하는 데 사용됩니다. 관리자는, `lsetxattr` 등의 xattr 변경과 관련된 특정 시스템 호출을 감시하고 `fsetxattr`, 특성을 설정하고 `removexattr`, `lremovexattr` `fremovexattr` 속성을 제거하는 규칙을 구성할 수 `setxattr` 있습니다.

ONTAP FPolicy는 파일 작업을 실시간으로 모니터링하고 제어하기 위한 강력한 프레임워크를 제공하여 이러한 기능을 확장합니다. 다양한 xattr 이벤트를 지원하도록 FPolicy를 구성하여 파일 작업을 세부적으로 제어하고 포괄적인 데이터 관리 정책을 적용할 수 있습니다.

특히 NFS v3 및 NFS v4 환경에서 xattrs를 사용하는 사용자의 경우 특정 파일 작업 및 필터 조합만 모니터링에

지원됩니다. NFS v3 및 NFS v4 파일 액세스 이벤트의 FPolicy 모니터링을 위해 지원되는 파일 작업 및 필터 조합 목록은 아래에 자세히 설명되어 있습니다.

지원되는 파일 작업	지원되는 필터
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

SetAttr 작업에 대한 **auditd** 로그 스니펫의 예:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

"ONTAP FPolicy를 사용해 보십시오"xattrs로 작업하는 사용자를 위해 파일 시스템의 무결성과 보안을 유지하는 데 필수적인 가시성과 제어 계층을 제공합니다. FPolicy의 고급 모니터링 기능을 활용하면 xattrs에 대한 모든 변경 사항을 추적하고 감사하며 보안 및 규정 준수 표준에 부합하도록 할 수 있습니다. 파일 시스템 관리에 대한 이러한 사전 예방적 접근 방식 때문에 데이터 거버넌스 및 보호 전략을 개선하려는 모든 조직에 ONTAP FPolicy를 사용하도록 적극 권장합니다.

데이터에 대한 액세스를 제어하는 예

John R. Smith의 PKI 인증서에 저장된 데이터에 대한 다음 예제 항목은 NetApp의 접근 방식을 파일에 적용하고 세분화된 액세스 제어를 제공하는 방법을 보여 줍니다.

> 이러한 예는 설명을 위한 것이며 NFS v4.2 보안 레이블 및 xattrs와 관련된 메타데이터를 결정하는 것은 고객의 책임입니다. 업데이트 및 레이블 보존에 대한 자세한 내용은 간단한 사용을 위해 생략됩니다.

- PKI 인증서 값 예 *

키	값
entitySecurityMark를 클릭합니다	T:s01 = 분류되지 않음

키	값

정보	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

사양	"DoD"
UUID입니다	b4111349-7875-4115-AD30-0928565f2e15

관리자 조직	{
	"value": "DoD"
	}

키	값

브리핑	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

시민 상태	{
	"value": "US"
	}

여유값	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

국가/지역 제휴	[
	{
	"value": "USA"
	}
	]

키	값

디지털 식별자입니다	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

파종	<pre>{
	  "value": "DoD"
	}</pre>

DutyOrganization(이중 조직	<pre>{
	  "value": "DoD"
	}</pre>

entityType 을 선택합니다	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControls를 참조하십시오	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

이러한 PKI 권한은 데이터 유형 및 특성을 포함한 John R. Smith의 액세스 세부 정보를 보여 줍니다.

IC-TDF 메타데이터가 파일과 별도로 저장되는 시나리오에서 NetApp는 세분화된 액세스 제어 계층을 추가로 지원합니다. 여기에는 디렉토리 레벨 및 각 파일과 관련된 액세스 제어 정보가 모두 저장됩니다. 예를 들어, 파일에 연결된 다음 태그를 고려해 보십시오.

- NFS v4.2 보안 레이블: 보안 결정을 내리는 데 사용됩니다
- xattrs: 파일 및 조직 프로그램 요구 사항과 관련된 보충 정보를 제공합니다

다음 키-값 쌍은 xattrs로 저장될 수 있는 메타데이터의 예이며 파일의 생성자 및 관련 보안 분류에 대한 자세한 정보를 제공합니다. 이 메타데이터는 클라이언트 응용 프로그램에서 정보에 기반한 액세스 결정을 내리고 조직의 표준 및 요구 사항에 따라 파일을 구성하는 데 활용될 수 있습니다.

- xattr 키-값 쌍의 예 *

키	값
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

키	값

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

키	값
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

관련 정보

- "NFS in NetApp ONTAP: 모범 사례 및 구축 가이드"
- "ONTAP 명령 참조입니다"
- 설명 요청(RFC)
  - "RFC 7204: 레이블이 지정된 NFS에 대한 요구 사항"
  - "RFC 2203: RPCSEC_GSS 프로토콜 사양"
  - "RFC 3530: NFS(Network File System) 버전 4 프로토콜"

보안 강화

ONTAP 보안 강화 가이드

이러한 기술 보고서에서는 NetApp ONTAP 및 다른 NetApp 제품의 보안 강화 방법에 대한 지침을 제공합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP 보안 및 데이터 암호화"설명합니다.

강화 가이드

"TR-4569: NetApp ONTAP 보안 강화 가이드" 조직이 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 NetApp ONTAP를 구성하는 방법에 대해 알아보십시오.

"VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드" 조직에서 정보 시스템 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 VMware vSphere용 ONTAP 툴을 구성하는 방법에 대해 알아보십시오.

"TR-4957: NetApp SnapCenter 보안 강화 가이드"
조직에서 정보 시스템 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 NetApp SnapCenter 소프트웨어를 구성하는 방법을 알아보십시오.

"TR-4963: 보안 강화 가이드: 애플리케이션을 위한 NetApp Backup and Recovery"조직이 정보 시스템의 기밀성, 무결성 및 가용성에 대한 규정된 보안 목표를 충족할 수 있도록 NetApp Cloud Backup for Applications를 구성하는 방법을 알아보세요.

"TR-4943: NetApp Active IQ Unified Manager 보안 강화 가이드"
조직에서 정보 시스템 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 NetApp Active IQ Unified Manager를 구성하는 방법을 알아보십시오.

"TR-4945: NetApp Manageability SDK에 대한 보안 강화 가이드"
조직에서 정보 시스템 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 NetApp Manageability SDK(NMSDK)를 구성하는 방법에 대해 알아보십시오.

"MetroCluster Tiebreaker 호스트 및 데이터베이스에 대한 보안 강화 가이드" 조직에서 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 NetApp MetroCluster Tiebreaker 호스트 및 데이터베이스를 구성하는 방법에 대해 알아보십시오.

ONTAP 보안 강화 지침

ONTAP 보안 강화 개요

ONTAP에서 제공하는 제어 기능을 사용하면 업계 최고의 데이터 관리 소프트웨어인 ONTAP 스토리지 운영 체제를 강화할 수 있습니다. ONTAP의 지침 및 구성 설정을 사용하여 조직에서 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 지원하십시오.

현재 위협 환경의 진화는 조직이 가장 중요한 자산인 데이터와 정보를 보호하기 위한 고유한 과제를 안고 있습니다. 우리가 직면하고 있는 지능적이고 동적인 위협과 취약성은 갈수록 정교해지고 있습니다. 잠재적 침입자의 측면에서 난독

처리 및 정찰 기법의 효과성이 높아짐에 따라 시스템 관리자는 사전에 데이터 및 정보의 보안을 다루어야 합니다.

2024년 7월부터 이전에 PDF로 게시되었던 ONTAP_ 보안 강화 가이드의 내용은 docs.netapp.com 에서 확인할 수 있습니다.

ONTAP 이미지 검증

ONTAP는 업그레이드 및 부팅 시 ONTAP 이미지가 유효한지 확인하는 메커니즘을 제공합니다.

이미지 검증 업그레이드

코드 서명을 활용하면 무중단 이미지 업데이트 또는 자동화된 무중단 이미지 업데이트, CLI 또는 ONTAP API를 통해 설치된 ONTAP 이미지가 NetApp에서 실제로 생성되며 무단 변경이 이뤄지지 않았는지 확인할 수 있습니다. 업그레이드 이미지 검증 기능은 ONTAP 9.3에 도입되었습니다.

이 기능은 ONTAP 업그레이드 또는 재버전에 대한 터치 없는 보안 향상 기능입니다. 사용자는 최상위 서명을 선택적으로 확인하는 경우를 제외하고 다른 작업을 수행할 수 `image.tgz` 없습니다.

부팅 시간 이미지 검증

ONTAP 9.4부터는 UEFI(통합 확장 펌웨어 인터페이스) 보안 부팅이 NetApp AFF A800, AFF A220, FAS2750, FAS2720 시스템과 UEFI BIOS를 사용하는 후속 차세대 시스템에서 지원됩니다.

전원을 켜는 동안 부트로더는 로드된 각 모듈과 연결된 서명을 사용하여 보안 부팅 키의 화이트리스트 데이터베이스를 검증합니다. 각 모듈이 검증되고 로드된 후 부팅 프로세스는 ONTAP 초기화를 계속합니다. 모듈에 대한 서명 검증이 실패하면 시스템이 재부팅됩니다.

이러한 항목은 ONTAP 이미지 및 플랫폼 BIOS에 적용됩니다.

로컬 스토리지 관리자 계정

ONTAP 역할, 응용 프로그램 및 인증

ONTAP는 보안을 중시하는 기업에 다양한 로그인 응용 프로그램 및 방법을 통해 다양한 관리자에게 세분화된 액세스를 제공할 수 있는 기능을 제공합니다. 이를 통해 고객은 데이터 중심의 제로 트러스트 모델을 만들 수 있습니다.

다음은 관리자 및 스토리지 가상 머신 관리자가 사용할 수 있는 역할입니다. 로그인 응용 프로그램 방법과 로그인 인증 방법이 지정됩니다.

역할

사용자는 역할 기반 액세스 제어(RBAC)를 사용하여 직무 역할 및 기능에 필요한 시스템 및 옵션에만 액세스할 수 있습니다. ONTAP의 RBAC 솔루션은 사용자의 관리 액세스를 정의된 역할에 허용된 수준으로 제한하므로 관리자가 할당된 역할별로 사용자를 관리할 수 있습니다. ONTAP는 몇 가지 미리 정의된 역할을 제공합니다. 운영자와 관리자는 사용자 지정 액세스 제어 역할을 생성, 수정 또는 삭제할 수 있으며 특정 역할에 대한 계정 제한을 지정할 수 있습니다.

클러스터 관리자를 위한 사전 정의된 역할

이 역할은...	이 수준의 액세스 권한...	명령 또는 명령 디렉토리로 이동합니다
admin	모두	모든 명령 디렉토리(DEFAULT)
admin-no-fsa (ONTAP 9.12.1부터 사용 가능)	읽기/쓰기	• 모든 명령 디렉토리(DEFAULT) • security login rest-role • security login role
읽기 전용	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	없음
volume file show-disk-usage	autosupport	모두
• set • system node autosupport	없음	기타 모든 명령 디렉토리(DEFAULT)
backup	모두	vserver services ndmp

읽기 전용	volume	없음
기타 모든 명령 디렉토리(DEFAULT)	readonly	모두
• security login password 사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다 • set	없음	security
읽기 전용	기타 모든 명령 디렉토리(DEFAULT)	none

autosupport`역할은 AutoSupport OnDemand에서 사용하는 미리 정의된 `autosupport 계정에 할당됩니다. ONTAP에서는 사용자가 계정을 수정하거나 삭제할 수 autosupport 없습니다. 또한 ONTAP에서는 다른 사용자 계정에 역할을 할당할 수 autosupport 없습니다.

스토리지 가상 머신**(SVM)** 관리자를 위한 사전 정의된 역할

역할 이름	제공합니다
vsadmin	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 및 파일을 관리합니다 • LUN 관리 • 권한 있는 삭제를 제외하고 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다

`vsadmin-volume`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 및 파일을 관리합니다 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
`vsadmin-protocol`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • LUN 관리 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
`vsadmin-backup`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • NDMP 작업을 관리합니다 • 복원된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 스냅샷 관리 • 볼륨 및 네트워크 정보를 봅니다
`vsadmin-snaplock`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 및 파일을 관리합니다 • 권한 있는 삭제를 포함한 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS 및 SMB • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다

vsadmin-readonly	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • SVM의 상태를 모니터링합니다 • 네트워크 인터페이스를 모니터링합니다 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

응용 프로그램 방법

응용 프로그램 메서드는 로그인 메서드의 액세스 유형을 지정합니다. 가능한 값에는 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 및 `telnet`가 포함됩니다.

이 매개 변수를 설정하면 `service-processor` 사용자에게 서비스 프로세서에 대한 액세스 권한이 부여됩니다. 이 매개 변수를 로 설정할 `service-processor -authentication-method` 경우 서비스 프로세서가 인증만 지원하므로 매개 변수를 로 설정해야 `password` 합니다. `password` SVM 사용자 계정은 서비스 프로세서에 액세스할 수 없습니다. 따라서 이 매개 변수가 로 설정된 경우 연산자 및 관리자는 매개 변수를 사용할 수 `-vserver` `service-processor`없습니다.

에 대한 액세스를 더 제한하려면 `service-processor` 명령을 `system service-processor ssh add-allowed-addresses`사용하십시오. 명령을 `system service-processor api-service` 사용하여 구성 및 인증서를 업데이트할 수 있습니다.

NetApp에서는 보안 원격 액세스를 위해 SSH(보안 셸)를 권장하므로 보안상의 이유로 Telnet 및 RSH(원격 셸)는 기본적으로 비활성화되어 있습니다. 텔넷 또는 RSH에 대한 요구 사항이나 고유한 요구 사항이 있는 경우 이를 활성화해야 합니다.

이 `security protocol modify` 명령은 RSH 및 Telnet의 기존 클러스터 전체 구성을 수정합니다. 활성화된 필드를 로 설정하여 클러스터에서 RSH 및 텔넷을 활성화합니다 `true`.

인증 방법

authentication method 매개 변수는 로그인에 사용되는 인증 방법을 지정합니다.

인증 방법	설명
`cert`	SSL 인증서 인증
`community`	SNMP 커뮤니티 문자열
`domain`	Active Directory 인증
`nsswitch`	LDAP 또는 NIS 인증
`password`	암호
`publickey`	공개 키 인증
`usm`	SNMP 사용자 보안 모델입니다

프로토콜 보안의 약점으로 인해 NIS를 사용하지 않는 것이 좋습니다.

ONTAP 9.3부터 및 을 두 가지 인증 방법으로 사용하는 로컬 SSH 계정에 대해 연결된 2단계 인증을 사용할 수 `admin`

publickey password 있습니다. 명령의 필드 외에 -authentication-method security login 이라는 새 필드가 -second-authentication-method 추가되었습니다. publickey`또는 `password 로 지정할 수 있습니다 -authentication-method -second-authentication-method. 그러나 SSH 인증 중에 순서는 항상 부분 인증과 함께 진행되며, 그 다음에 publickey 전체 인증을 위한 암호 프롬프트가 나타납니다.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

ONTAP 9.4부터 를 nsswitch 와 함께 두 번째 인증 방법으로 사용할 수 `publickey`있습니다.

ONTAP 9.12.1부터 FIDO2는 YubiKey 하드웨어 인증 장치 또는 기타 FIDO2 호환 장치를 사용하는 SSH 인증에도 사용할 수 있습니다.

ONTAP 9.13.1부터:

- domain 계정은 에서 두 번째 인증 방법으로 사용할 `publickey`수 있습니다.
- 시간 기반 일회용 암호 (totp)는 현재 시간을 두 번째 인증 방법의 인증 요소 중 하나로 사용하는 알고리즘에 의해 생성된 임시 암호입니다.
- 공개 키 취소는 SSH 공개 키와 SSH 중에 만료/해지 여부를 확인하는 인증서를 통해 지원됩니다.

ONTAP System Manager, Active IQ Unified Manager, SSH를 위한 다단계 인증(MFA)에 대한 자세한 내용은 를 참조하십시오. "TR-4647: ONTAP 9의 다단계 인증"

기본 관리 계정

관리자 역할은 모든 응용 프로그램을 사용하여 액세스할 수 있으므로 관리자 계정을 제한해야 합니다. diag 계정은 시스템 쉘에 액세스할 수 있으며 기술 지원 부서의 문제 해결 작업을 수행하기 위한 목적으로만 예약되어야 합니다.

기본 관리 계정에는 및 의 두 admin `diag`가지가 있습니다.

고립된 계정은 권한 에스컬레이션을 비롯한 취약점을 유발하는 주요 보안 수단입니다. 이러한 계정은 사용자 계정 저장소에 남아 있는 불필요하고 사용되지 않는 계정입니다. 이러한 계정은 기본적으로 사용되지 않았거나 암호가 업데이트 또는 변경되지 않은 기본 계정입니다. 이 문제를 해결하기 위해 ONTAP에서는 계정 제거 및 이름 변경을 지원합니다.

내장 계정은 삭제하거나 이름을 변경할 수 없습니다. 관리자가 계정을 삭제하더라도 재부팅 시 내장 계정이 다시 생성됩니다. **NetApp**에서는 불필요한 내장 계정은 lock 명령을 사용하여 잠그는 것을 권장합니다.

고아 계정은 심각한 보안 문제이지만, **NetApp**에서는 로컬 계정 저장소에서 계정을 제거했을 때의 영향을 테스트해 볼 것을 강력히 권장합니다.

로컬 계정을 나열합니다

로컬 계정을 나열하려면 security login show 명령을 실행합니다.

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application  Method    Role Name         Locked Group
---------------- -----------  --------- ----------------- ------ -----------
admin            console      password  admin             no     no
admin            http         password  admin             no     no
admin            ontapi       password  admin             no     no
admin            service-processor password admin         no     no
admin            ssh          password  admin             no     no
autosupport      console      password  autosupport       no     no
6 entries were displayed.
```

진단**(diag)** 계정 암호를 설정합니다

라는 진단 계정이 diag 스토리지 시스템과 함께 제공됩니다. 계정을 사용하여 에서 문제 해결 작업을 수행할 수 diag systemshell`있습니다. 이 `diag 계정은 권한이 있는 명령을 통해 시스템 쉘에 액세스하는 데 사용할 수 있는 유일한 계정입니다. diag systemshell

시스템 셸 및 관련 diag 계정은 저수준 진단 목적으로 사용됩니다. 이러한 액세스 권한은 진단 권한 수준이 필요하며, 기술 지원 부서의 지침에 따라 문제 해결 작업을 수행할 수 있는 경우에만 사용됩니다. 계정과 은 일반 관리 목적으로 사용할 수 diag systemshell 없습니다.

시작하기 전에

에 액세스하기 전에 systemshell`명령을 사용하여 계정 암호를 설정해야 `diag security login password 합니다. 강력한 암호 원칙을 사용하고 정기적으로 암호를 변경해야 diag 합니다.

단계

1. 계정 사용자 암호 설정 diag :

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

다중 관리 검증

ONTAP 9.11.1부터 MAV(Multi-admin Verification)를 사용하여 지정된 관리자의 승인 후에만 볼륨 또는 스냅샷 삭제와 같은 특정 작업을 실행할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

MAV 구성은 다음과 같이 구성됩니다.

- "하나 이상의 관리자 승인 그룹을 만드는 중입니다"..
- "다중 관리자 인증 기능 활성화"..
- "규칙 추가 또는 수정"..

초기 구성 후 MAV 승인 그룹(MAV 관리자)의 관리자만 이러한 요소를 수정할 수 있습니다.

MAV가 활성화된 경우 모든 보호된 작업을 완료하려면 다음 세 단계를 수행해야 합니다.

1. 사용자가 작업을 시작하면 가 "요청이 생성됩니다"나타납니다.
2. 이 명령을 실행하기 전에 필요한 개수"MAV 관리자가 승인해야 합니다".
3. 승인 후 사용자가 작업을 완료합니다.

MAV는 자동화 작업이 완료되기 전에 승인이 필요하기 때문에 높은 자동화가 필요한 볼륨이나 워크플로에는 사용할 수 없습니다. 자동화와 MAV를 함께 사용하려는 경우 NetApp에서는 특정 MAV 작업에 대해 쿼리를 사용하는 것이 좋습니다. 예를 들어, 자동화가 관련되지 않은 볼륨에만 MAV 규칙을 적용할 수 `volume delete` 있으며 특정 명명 체계를 사용하여 해당 볼륨을 지정할 수 있습니다.

MAV에 대한 자세한 내용은 를 "ONTAP 다중 관리자 인증 문서"참조하십시오.

스냅샷 잠금

스냅샷 잠금은 볼륨 스냅샷 정책에 대한 보존 기간에 수동 또는 자동으로 스냅샷을 지울 수 없는 SnapLock 기능입니다. 스냅샷 잠금의 목적은 악의적인 관리자 또는 신뢰할 수 없는 관리자가 운영 또는 보조 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 하는 것입니다.

스냅샷 잠금은 ONTAP 9.12.1에 도입되었습니다. 스냅샷 잠금은 무단 변경 방지 스냅샷 잠금이라고도 합니다. SnapLock 라이센스와 컴플라이언스 클록의 초기화가 필요하지만 스냅샷 잠금은 SnapLock Compliance 또는 SnapLock Enterprise와 관련이 없습니다. SnapLock Enterprise에서와 같이 신뢰할 수 있는 스토리지 관리자는 없으며 SnapLock 규정 준수와 같이 기본 물리적 스토리지 인프라를 보호하지 않습니다. 이는 스냅샷을 보조 시스템에 대한 SnapVaulting에 비해 향상된 기능입니다. 1차 시스템에서 잠긴 스냅샷을 빠르게 복구하여 랜섬웨어에 의해 손상된 볼륨을 복원할 수 있습니다.

자세한 내용은 를 참조하십시오"스냅샷 잠금 설명서".

인증서 기반 **API** 액세스를 설정합니다

REST API 또는 ONTAP에 대한 NetApp Manageability SDK API 액세스에 대한 사용자 ID 및 암호 인증 대신 인증서 기반 인증을 사용해야 합니다.

REST API에 대한 인증서 기반 인증 대신 사용 "OAuth 2.0 토큰 기반 인증")

이 단계에 설명된 대로 ONTAP에서 자체 서명된 인증서를 생성하고 설치할 수 있습니다.

단계

1. OpenSSL을 사용하여 다음 명령을 실행하여 인증서를 생성합니다.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

   이 명령은 라는 공용 인증서와 `test.pem` 라는 개인 키를 `key.out`생성합니다. 일반 이름인 CN은 ONTAP 사용자 ID에 해당합니다.

2. 다음 명령을 실행하고 메시지가 표시되면 인증서의 내용을 붙여 넣어 ONTAP의 PEM(Privacy Enhanced mail) 형식으로 공용 인증서 내용을 설치합니다.

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. ONTAP를 활성화하여 SSL을 통한 클라이언트 액세스를 허용하고 API 액세스에 대한 사용자 ID를 정의합니다.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

다음 예에서는 사용자 ID가 `cert_user` 인증서 인증 API 액세스를 사용할 수 있게 되었습니다. ONTAP 버전을 표시하기 위해 사용하는 간단한 관리 SDK Python 스크립트는 `cert_user` 다음과 같습니다.

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

스크립트의 출력에 ONTAP 버전이 표시됩니다.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. ONTAP REST API를 사용하여 인증서 기반 인증을 수행하려면 다음 단계를 완료하십시오.

   a. ONTAP에서 http 액세스에 대한 사용자 ID를 정의합니다.

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

   b. Linux 클라이언트에서 다음 명령을 실행하여 ONTAP 버전을 출력으로 생성합니다.

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

추가 정보

- "ONTAP용 NetApp 관리 SDK를 사용한 인증서 기반 인증"..

REST API에 대한 **ONTAP OAuth 2.0** 토큰 기반 인증

인증서 기반 인증 대신 REST API에 OAuth 2.0 토큰 기반 인증을 사용할 수 있습니다.

ONTAP 9.14.1부터 OAuth 2.0(Open Authorization 2.0) 프레임워크를 사용하여 ONTAP 클러스터에 대한 액세스를 제어할 수 있습니다. 이 기능은 ONTAP CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성할 수 있습니다. 그러나 OAuth 2.0 권한 부여 및 액세스 제어 결정은 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때만 적용할 수 있습니다.

OAuth 2.0 토큰은 사용자 계정 인증을 위한 암호를 대체합니다.

OAuth 2.0 사용에 대한 자세한 내용은 를 "OAuth 2.0을 사용한 인증 및 권한 부여에 대한 ONTAP 문서"참조하십시오.

로그인 및 암호 매개 변수

효과적인 보안 체계는 확립된 조직 정책, 지침 및 조직에 적용되는 모든 거버넌스 또는 표준을 준수합니다. 이러한 요구 사항의 예로는 사용자 이름 수명, 암호 길이 요구 사항, 문자 요구 사항 및 이러한 계정의 저장 등이 있습니다. ONTAP 솔루션은 이러한 보안 구조를 처리하는 기능을

제공합니다.

새로운 로컬 계정 기능

거버넌스를 포함하여 조직의 사용자 계정 정책, 지침 또는 표준을 지원하기 위해 ONTAP에서 지원되는 기능은 다음과 같습니다.

- 최소 숫자, 소문자 또는 대문자를 사용하도록 암호 정책 구성
- 로그인 시도 실패 후 지연이 필요합니다
- 계정 비활성 한도 정의
- 사용자 계정 만료
- 암호 만료 경고 메시지 표시
- 잘못된 로그인에 대한 알림입니다

구성 가능한 설정은 보안 로그인 역할 config modify 명령을 사용하여 관리합니다.

SHA-512 지원

암호 보안을 강화하기 위해 ONTAP 9에서는 SHA-2 암호 해시 기능을 지원하며, 새로 생성되거나 변경된 암호를 해시하는 데 기본적으로 SHA-512를 사용합니다. 운영자와 관리자는 필요에 따라 계정을 만료하거나 잠글 수도 있습니다.

암호가 변경되지 않은 기존 ONTAP 9 사용자 계정은 ONTAP 9.0 이상으로 업그레이드한 후에도 MD5 해시 기능을 계속 사용합니다. 그러나 NetApp에서는 사용자가 암호를 변경하도록 하여 이러한 사용자 계정을 보다 안전한 SHA-512 솔루션으로 마이그레이션할 것을 적극 권장합니다.

암호 해시 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정 표시:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 지정된 해시 함수(예: MD5)를 사용하는 계정을 만료시켜 사용자가 다음 로그인 시 암호를 변경해야 합니다.

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 지정된 해시 함수를 사용하는 암호로 계정을 잠급니다.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

클러스터의 관리 SVM에서 내부 사용자가 암호 해시 기능을 알 수 없습니다 `autosupport` . 이 문제는 외관상 문제입니다. 이 내부 사용자에게는 기본적으로 구성된 암호가 없으므로 해시 기능을 알 수 없습니다.

  - 사용자의 암호 해시 기능을 보려면 `autosupport` 다음 명령을 실행합니다.

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

  - 암호 해시 기능(기본값: SHA512)을 설정하려면 다음 명령을 실행합니다.

```
::> security login password -username autosupport
```

암호가 무엇으로 설정되어 있는지는 중요하지 않습니다.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

암호 매개 변수

ONTAP 솔루션은 조직 정책 요구 사항 및 지침을 다루고 지원하는 암호 매개 변수를 지원합니다.

9.14.1부터는 ONTAP의 새 설치에만 적용되는 암호의 복잡성 및 잠금 규칙이 증가합니다.

모든 암호는 사용자 이름과 달라야 합니다.

속성	설명	기본값	범위
`username-minlength`	최소 사용자 이름 길이가 필요합니다	3	3-16 을 참조하십시오
`username-alphanum`	사용자 이름 영숫자	사용 안 함	활성화/비활성화
`passwd-minlength`	최소 암호 길이가 필요합니다	8	3-64 을 참조하십시오
`passwd-alphanum`	암호 영숫자	활성화됨	활성화/비활성화
`passwd-min-special-chars`	암호에 필요한 최소 특수 문자 수입니다	0	0-64 을 참조하십시오
`passwd-expiry-time`	암호 만료 시간(일)	무제한 - 암호가 만료되지 않습니다	0 - 무제한 0 = 지금 만료
`require-initial-passwd-update`	첫 번째 로그인 시 초기 암호 업데이트가 필요합니다	사용 안 함	활성화/비활성화 콘솔 또는 SSH를 통해 변경이 허용됩니다
`max-failed-login-attempts`	최대 시도 실패 횟수입니다	0, 계정을 잠그지 마십시오	-

속성	설명	기본값	범위
lockout-duration	최대 잠금 기간(일)	기본값은 0입니다. 즉, 계정이 하루 동안 잠겨 있습니다	-
disallowed-reuse	마지막 N 암호를 허용하지 않습니다	6	최소값은 6입니다
change-delay	암호 변경 간격(일)	0	-
delay-after-failed-login	로그인 시도 실패 후 지연(초)	4	-
passwd-min-lowercase-chars	암호에 필요한 최소 소문자 알파벳 문자 수입니다	0으로, 소문자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-min-uppercase-chars	알파벳 대문자 최소 개수여야 합니다	0 - 대문자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-min-digits	암호에 필요한 최소 자릿수입니다	0으로, 숫자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-expiry-warn-time	암호 만료 전에 경고 메시지 표시(일)	Unlimited(무제한) - 암호 만료에 대해 경고하지 않습니다	0: 로그인할 때마다 암호 만료에 대해 사용자에게 경고합니다
account-expiry-time	계정이 N일 후에 만료됩니다	무제한. 즉, 계정이 만료되지 않습니다	계정 만료 시간은 계정 비활성 제한보다 커야 합니다
account-inactive-limit	계정 만료 전 최대 비활성 기간(일)	무제한 - 비활성 계정은 만료되지 않습니다	계정 비활성 한도는 계정 만료 시간보다 작아야 합니다

예

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

시스템 관리 방법

이는 ONTAP 시스템 관리를 강화하는 중요한 매개 변수입니다.

명령줄 액세스

보안 솔루션을 유지 관리하려면 시스템에 대한 보안 액세스를 설정하는 것이 중요합니다. 가장 일반적인 명령줄 액세스 옵션은 SSH, Telnet 및 RSH입니다. 이 중에서 SSH는 원격 명령줄 액세스를 위한 가장 안전한 업계 표준 모범 사례입니다. NetApp에서는 ONTAP 솔루션에 대한 명령줄 액세스를 위해 SSH를 사용할 것을 적극 권장합니다.

SSH 구성

`security ssh show`명령은 클러스터 및 SVM에 대한 SSH 키 교환 알고리즘, 암호, MAC 알고리즘의 구성을 보여줍니다. 키 교환 방법은 이러한 알고리즘과 암호를 사용하여 암호화 및 인증을 위해 1회성 세션 키가 생성되는 방법과 서버 인증이 수행되는 방법을 지정합니다.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

로그인 배너

조직은 로그인 배너를 사용하여 모든 운영자, 관리자, 범법자를 막론하고 모두에게 사용 약관을 제공하고 시스템에 액세스 할 수 있는 사람을 표시 할 수 있습니다. 이 접근 방식은 시스템 액세스 및 사용에 대한 기대치를 설정하는 데 유용합니다. `security login banner modify`이 명령은 로그인 배너를 수정합니다. 로그인 배너는 SSH 및 콘솔 장치 로그인 프로세스 중 인증 단계 바로 앞에 표시됩니다. 배너 텍스트는 다음 예에 표시된 것처럼 큰따옴표("")로 묶어야 합니다.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

로그인 배너 매개 변수

매개 변수	설명
`vserver`	이 매개 변수를 사용하여 수정된 배너가 있는 SVM을 지정합니다. 클러스터 관리자 SVM의 이름을 사용하여 클러스터 레벨 메시지를 수정하십시오. 클러스터 레벨 메시지는 메시지가 정의되지 않은 데이터 SVM에 대한 기본값으로 사용됩니다.
`message`	이 선택적 매개 변수는 로그인 배너 메시지를 지정하는 데 사용할 수 있습니다. 클러스터에 로그인 배너 메시지가 설정된 경우 클러스터 로그인 배너는 모든 데이터 SVM에서 사용됩니다. 데이터 SVM의 로그인 배너를 설정하면 클러스터 로그인 배너의 디스플레이가 재정의됩니다. 데이터 SVM 로그인 배너를 사용하여 클러스터 로그인 배너를 재설정하려면 이 매개 변수를 "-" 값과 함께 사용하십시오. 이 매개 변수를 사용하는 경우 로그인 배너에 줄 바꿈(줄 끝 [EOL] 또는 줄 바꿈)을 포함할 수 없습니다. 새 줄이 있는 로그인 배너 메시지를 입력하려면 매개 변수를 지정하지 마십시오. 메시지를 대화형으로 입력하라는 메시지가 표시됩니다. 대화형으로 입력된 메시지에는 줄 바꿈을 포함할 수 있습니다. ASCII가 아닌 문자는 유니코드 UTF-8을 사용해야 합니다.

매개 변수	설명
`uri`	`(ftp
http):///(hostname	IPv4` 이 매개 변수를 사용하여 로그인 배너를 다운로드할 URI를 지정합니다. 메시지의 길이는 2048바이트를 초과할 수 없습니다. 비 ASCII 문자는 유니코드 UTF-8로 제공되어야 합니다.

오늘의 메시지

이 `security login motd modify` 명령은 MOTD(오늘의 메시지)를 업데이트합니다.

MOTD에는 클러스터 레벨 MOTD와 데이터 SVM 레벨 MOTD라는 두 가지 범주가 있습니다. 데이터 SVM의 클러스터 쉘에 로그인하는 사용자는 클러스터 레벨 MOTD 다음에 해당 SVM에 대한 SVM 레벨 MOTD라는 두 가지 메시지를 볼 수 있습니다.

클러스터 관리자는 필요한 경우 각 SVM에서 개별적으로 클러스터 수준 MOTD를 사용하거나 사용하지 않도록 설정할 수 있습니다. 클러스터 관리자가 SVM에 대해 클러스터 레벨 MOTD를 사용하지 않도록 설정하면 SVM에 로그인한 사용자에게 클러스터 레벨 메시지가 표시되지 않습니다. 클러스터 관리자만 클러스터 레벨 메시지를 설정 또는 해제할 수 있습니다.

MOTD 매개 변수입니다	설명
SVM	이 매개변수를 사용하여 MOTD가 수정되는 SVM을 지정합니다. 클러스터 관리자 SVM의 이름을 사용하여 클러스터 레벨 메시지를 수정하십시오.

MOTD 매개 변수입니다	설명
메시지	이 선택적 매개 변수는 메시지를 지정하는 데 사용할 수 있습니다. 이 매개변수를 사용하면 MOTD에 줄 바꿈을 포함할 수 없습니다. 매개 변수 이외의 매개 변수를 지정하지 `-vserver` 않으면 메시지를 대화형으로 입력하라는 메시지가 표시됩니다. 대화형으로 입력된 메시지에는 줄 바꿈을 포함할 수 있습니다. 비 ASCII 문자는 유니코드 UTF-8로 제공되어야 합니다. 메시지에는 다음과 같은 이스케이프 시퀀스를 사용하여 동적으로 생성된 콘텐츠가 포함될 수 있습니다. • `\\` - 단일 백래시 문자 • `\b` - 출력 없음(Linux와의 호환성을 위해서만 지원됨) • `\C` - 클러스터 이름입니다 • `\d` - 로그인 노드에 설정된 현재 날짜입니다 • `\t` - 로그인 노드에 설정된 현재 시간입니다 • `\I` - 수신 LIF IP 주소(로그인용 콘솔 인쇄 `console`) • `\l` - 로그인 장치 이름(로그인을 위해 콘솔을 인쇄함 `console`) • `\L` - 클러스터의 모든 노드에서 사용자에 대한 마지막 로그인입니다 • `\m` - 기계 아키텍처 • `\n` - 노드 또는 데이터 SVM 이름 • `\N` - 로그인한 사용자의 이름입니다 • `\o` - \O와 동일합니다 Linux 호환성을 위해 제공됩니다. • `\O` - 노드의 DNS 도메인 이름입니다. 출력은 네트워크 구성에 따라 달라지며 비어 있을 수 있습니다. • `\r` - 소프트웨어 릴리스 번호 • `\s` - 운영 체제 이름입니다 • `\u` - 로컬 노드의 활성 클러스터 셸 세션 수입니다. 클러스터 관리자의 경우: 모든 클러스터 셸 사용자. 데이터 SVM 관리자의 경우: 해당 데이터 SVM에 대한 액티브 세션만 지원됩니다. • `\U` - 와 같지만 `\u`또는 가 `user users` 추가됩니다 • `\v` - 효과적인 클러스터 버전 문자열 • `\W` - 사용자가 로그인할 수 있도록 클러스터 전체에서 활성 세션 (`who`사용)

ONTAP에서 오늘의 메시지를 구성하는 방법에 대한 자세한 내용은 를 참조하십시오 "오늘의 메시지에 대한 ONTAP 문서".

CLI 세션 시간 초과

기본 CLI 세션 시간 초과는 30분입니다. 시간 초과는 부실 세션 및 세션 피기백킹을 방지하는 데 중요합니다.

명령을 사용하여 `system timeout show` 현재 CLI 세션 시간 초과를 봅니다. 시간 초과 값을 설정하려면 `system timeout modify -timeout <minutes>` 명령을 사용합니다.

NetApp ONTAP System Manager를 통한 웹 액세스

ONTAP 관리자가 클러스터를 액세스하고 관리하는 데 CLI 대신 그래픽 인터페이스를 사용하려는 경우 NetApp ONTAP System Manager를 사용하십시오. 기본적으로 활성화되며 브라우저를 통해 액세스할 수 있는 웹 서비스로 ONTAP에 포함되어 있습니다. DNS를 사용하는 경우 브라우저에서 호스트 이름을 가리키거나 를 통해 IPv4 또는 IPv6 주소를 `https://cluster-management-LIF`지정합니다.

클러스터에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없음을 나타내는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 인식하거나 서버 인증을 위해 클러스터에 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다.

ONTAP 9.3부터 SAML(Security Assertion Markup Language) 인증은 ONTAP System Manager의 옵션입니다.

ONTAP System Manager에 대한 SAML 인증

SAML 2.0은 타사 SAML 호환 ID 공급자(IDP)가 기업에서 선택한 IDP에 고유한 메커니즘을 사용하고 SSO(Single Sign-On)의 소스로 MFA를 수행할 수 있도록 하는 널리 채택된 업계 표준입니다.

SAML 사양에는 Principal, IDP 및 Service Provider의 세 가지 역할이 정의되어 있습니다. ONTAP 구현에서 주체는 클러스터 관리자가 ONTAP System Manager 또는 NetApp Active IQ Unified Manager를 통해 ONTAP에 액세스할 수 있도록 하는 것입니다. IDP는 타사 IDP 소프트웨어입니다. ONTAP 9.3부터 Microsoft ADFS(Active Directory Federated Services)와 오픈 소스 Shibboleth IDP가 지원됩니다. ONTAP 9.12.1부터 Cisco Duo는 IDP를 지원합니다. 서비스 공급자는 ONTAP에 내장된 SAML 기능으로, ONTAP System Manager 또는 Active IQ Unified Manager 웹 애플리케이션에서 사용됩니다.

SSH 2단계 구성 프로세스와 달리, SAML 인증이 활성화된 후 ONTAP System Manager 또는 ONTAP 서비스 프로세서 액세스에 모든 기존 관리자는 SAML IDP를 통해 인증해야 합니다. 클러스터 사용자 계정을 변경할 필요가 없습니다. SAML 인증이 활성화되면 및 응용 프로그램에 대한 관리자 역할이 있는 기존 사용자에게 의 새로운 인증 방법이 `saml` `http` `ontapi` 추가됩니다.

SAML 인증을 사용하도록 설정한 후 SAML IDP 액세스가 필요한 추가 새 계정을 ONTAP에서 관리자 역할 및 및 및 응용 프로그램에 대한 SAML 인증 방법으로 `http` `ontapi` 정의해야 합니다. 특정 시점에 SAML 인증이 비활성화된 경우 이러한 새 계정은 `password` 및 응용 프로그램에 대한 관리자 역할을 `http` `ontapi` 정의하고 로컬 ONTAP 인증을 위한 응용 프로그램을 ONTAP 시스템 관리자에 추가해야 `console` 합니다.

SAML IDP를 사용하도록 설정하면 IDP는 LDAP(Lightweight Directory Access Protocol), AD(Active Directory), Kerberos, 암호 등과 같이 IDP에 사용 가능한 방법을 사용하여 ONTAP 시스템 관리자 액세스에 대한 인증을 수행합니다. 사용 가능한 방법은 IDP에 고유합니다. ONTAP에 구성된 계정에는 IDP 인증 방법에 매핑되는 사용자 ID가 있어야 합니다.

NetApp에서 검증한 IDP는 Microsoft ADFS, Cisco Duo 및 오픈 소스 Shibboleth IDP입니다.

ONTAP 9.14.1부터 Cisco Duo를 SSH의 두 번째 인증 요소로 사용할 수 있습니다.

ONTAP System Manager, Active IQ Unified Manager 및 SSH를 위한 MFA에 대한 자세한 내용은 를 참조하십시오. "TR-4647: ONTAP 9의 다단계 인증"

ONTAP System Manager의 통찰력

ONTAP 9.11.1부터 ONTAP System Manager는 클러스터 관리자가 일상 작업을 간소화하는 데 도움이 되는 통찰력을 제공합니다. 보안 정보는 이 기술 보고서의 권장 사항을 기반으로 합니다.

보안 통찰력	결정
텔넷이 활성화되었습니다	보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다.
원격 셸(RSH)이 활성화되었습니다	NetApp에서는 보안 원격 액세스에 SSH를 권장합니다.
AutoSupport가 안전하지 않은 프로토콜을 사용하고 있습니다	AutoSupport가 HTTPS 링크를 통해 전송되도록 구성되지 않았습니다.
로그인 배너가 클러스터 레벨의 클러스터에 구성되어 있지 않습니다	로그인 배너가 클러스터에 대해 구성되지 않은 경우 경고.
SSH가 안전하지 않은 암호를 사용하고 있습니다	SSH에서 안전하지 않은 암호를 사용하는 경우 경고
구성된 NTP 서버가 너무 적습니다	구성된 NTP 서버 수가 3개 미만인 경우 경고
기본 관리자 사용자가 잠기지 않았습니다	기본 관리 계정(admin 또는 diag)을 사용하여 System Manager에 로그인하지 않고 이러한 계정이 잠겨 있지 않은 경우 계정을 잠그는 것이 좋습니다.
랜섬웨어 방어: 볼륨에 스냅샷 정책이 없습니다	하나 이상의 볼륨에 적절한 스냅샷 정책이 연결되어 있지 않습니다.
랜섬웨어 방어: 스냅샷 자동 삭제를 사용하지 않습니다	스냅샷 자동 삭제는 하나 이상의 볼륨에 대해 설정되어 있습니다.
랜섬웨어 공격을 위해 볼륨을 모니터링하지 않고 있습니다	자율적 랜섬웨어 방어는 여러 볼륨에서 지원되지만 아직 구성되지 않았습니다.
SVM은 자율적 랜섬웨어 방어에 대해 구성되지 않습니다	여러 SVM에서 자율적 랜섬웨어 보호가 지원되지만 아직 구성되지 않았습니다.
기본 FPolicy가 구성되지 않았습니다	NAS SVM에 FPolicy가 설정되지 않았습니다.
자율적 랜섬웨어 방어 활성 모드를 활성화합니다	여러 볼륨이 학습 모드를 완료했으며 활성 모드를 켤 수 있습니다
글로벌 FIPS 140-2 규정 준수가 비활성화되었습니다	글로벌 FIPS 140-2 규정 준수는 사용되지 않습니다.
클러스터가 알림에 대해 구성되지 않았습니다	이메일, Webhook 또는 SNMP traphosts가 알림을 수신하도록 구성되지 않았습니다.

ONTAP System Manager 인사이트에 대한 자세한 내용은 를 "ONTAP System Manager 인사이트 설명서 "참조하십시오.

System Manager 세션 시간이 초과되었습니다

System Manager 세션 비활성 시간 초과를 변경할 수 있습니다. 기본 비활성 시간 제한은 30분입니다. 시간 초과는 부실 세션 및 세션 피기백킹을 방지하는 데 중요합니다.

SAML이 구성된 경우 IdP의 설정에 의해 비활성 시간 초과가 제어됩니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. UI settings * 에서 를 선택합니다.
3. Inactivity timeout * 상자에 2에서 180 사이의 분 값을 입력하거나 "0"을 입력하여 시간 초과를 비활성화합니다.
4. 저장 * 을 선택합니다.

ONTAP 자율 랜섬웨어 방어

스토리지 워크로드 보안에 대한 사용자 행동 분석을 보완하기 위해 ONTAP 자율적 랜섬웨어 방어는 볼륨 워크로드와 엔트로피를 분석하여 랜섬웨어를 탐지하고 스냅샷을 생성하여 공격이 의심되면 관리자에게 알립니다.

ONTAP 9.10.1은 NetApp Data Infrastructure Insights Storage Workload Security 및 NetApp FPolicy 파트너 에코시스템을 활용한 외부 FPolicy 사용자 행동 분석(UBA)을 사용한 랜섬웨어 탐지 및 예방 기능 외에도 자율적인 랜섬웨어 보호 기능을 도입했습니다. ONTAP 자율형 랜섬웨어 보호 기능은 볼륨 워크로드 활동과 데이터 엔트로피를 모두 고려하여 랜섬웨어를 자동으로 감지하는 내장형 머신 러닝(ML) 기능을 사용합니다. UBA에서 감지하지 못하는 공격을 감지할 수 있도록 UBA와 다른 활동을 모니터링합니다.

이 기능에 대한 자세한 내용은 "바로 랜섬웨어용 NetApp 솔루션입니다" 또는 을 참조하십시오"ONTAP 자율적 랜섬웨어 방어 문서화".

스토리지 관리 시스템 감사

ONTAP 이벤트를 원격 syslog 서버로 오프로드하여 이벤트 감사의 무결성을 보장합니다. 이 서버는 Splunk와 같은 보안 정보 이벤트 관리 시스템이 될 수 있습니다.

syslog를 보냅니다

로그 및 감사 정보는 지원 및 가용성의 관점에서 조직에 매우 중요합니다. 또한 로그(syslog) 및 감사 보고서/출력에 포함된 정보와 세부 정보는 일반적으로 민감한 특성입니다. 보안 제어 및 상태를 유지하려면 조직에서 로그 및 감사 데이터를 안전하게 관리해야 합니다.

syslog 정보의 오프로드는 침입의 범위 또는 설치 공간을 단일 시스템 또는 솔루션으로 제한하는 데 필요합니다. 따라서 syslog 정보를 안전한 스토리지 또는 보존 위치로 안전하게 오프로딩하는 것이 좋습니다.

로그 전달 대상을 생성합니다

명령을 사용하여 `cluster log-forwarding create` 원격 로깅을 위한 로그 전달 대상을 생성할 수 있습니다.

매개 변수

다음 매개 변수를 사용하여 `cluster log-forwarding create` 명령을 구성합니다.

- * 대상 호스트. * 이 이름은 로그를 전달할 서버의 호스트 이름 또는 IPv4 또는 IPv6 주소입니다.

```
-destination <Remote InetAddress>
```

- * 대상 포트. * 대상 서버가 수신 대기하는 포트입니다.

```
[-port <integer>]
```

- * 로그 전달 프로토콜. * 이 프로토콜은 메시지를 대상으로 보내는 데 사용됩니다.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

로그 전달 프로토콜은 다음 값 중 하나를 사용할 수 있습니다.

  - `udp-unencrypted`.. 보안이 없는 사용자 데이터그램 프로토콜.
  - `tcp-unencrypted`.. 보안 기능이 없는 TCP.
  - `tcp-encrypted`.. TLS(Transport Layer Security)를 사용하는 TCP.

- * 대상 서버 ID를 확인하십시오. * 이 매개 변수를 true로 설정하면 해당 인증서의 유효성을 확인하여 로그 전달 대상의 ID를 확인합니다. 프로토콜 필드에서 값을 선택한 경우에만 이 값을 TRUE로 설정할 수 `tcpencrypted` 있습니다.

```
[-verify-server \{true|false}]
```

- * Syslog 기능. * 이 값은 전달된 로그에 사용할 syslog 기능입니다.

```
[-facility <Syslog Facility>]
```

- * 연결 테스트를 건너뜁니다. * 일반적으로 이 `cluster log-forwarding create` 명령은 ICMP(Internet Control Message Protocol) ping을 보내 대상에 연결할 수 있는지 확인하고 도달할 수 없는 경우 실패합니다. 이 값을 설정하면 `true` Ping 검사를 무시하여 대상에 도달할 수 없을 때 구성할 수 있습니다.

```
[-force [true]]
```

NetApp에서는 명령을 사용하여 유형에 강제로 연결하는 것이 `cluster log-forwarding -tcp -encrypted` 좋습니다.

이벤트 알림

시스템에서 나가는 정보와 데이터의 보호는 시스템의 보안 상태를 유지하고 관리하는 데 있어 매우 중요합니다. ONTAP 솔루션에 의해 생성되는 이벤트는 솔루션이 마주치는 내용, 처리되는 정보 등에 대한 풍부한 정보를 제공합니다. 데이터가 활발하게 사용됨에 따라 데이터를 안전하게 관리하고 마이그레이션해야 할 필요성이 대두되었습니다.

이 `event notification create` 명령은 이벤트 필터로 정의된 일련의 이벤트에 대한 새 알림을 하나 이상의 알림 대상으로 보냅니다. 다음 예에서는 구성된 이벤트 알림 필터 및 대상을 표시하는 이벤트 알림 구성 및 `event notification show` 명령을 보여 줍니다.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

ONTAP에서의 스토리지 암호화

디스크 도난, 반환 또는 용도 변경 시 기밀 데이터를 보호하려면 하드웨어 기반 NetApp 스토리지 암호화나 소프트웨어 기반 NetApp 볼륨 암호화/NetApp 애그리게이트 암호화를 사용하십시오. 두 메커니즘 모두 FIPS-140-2 검증을 거쳤으며 소프트웨어 기반 메커니즘과 함께 하드웨어 기반 메커니즘을 사용할 경우 CSfC(Commercial Solutions for Classified) 프로그램에 적합합니다. 하드웨어 및 소프트웨어 계층 모두에서 저장된 비밀 데이터와 주요 기밀 데이터에 대한 보안 보호 기능이 강화됩니다.

유휴 데이터 암호화는 디스크 도난, 반환 또는 용도 변경이 발생할 경우 중요한 데이터를 보호하는 데 중요합니다.

ONTAP 9에는 세 가지 FIPS(Federal Information Processing Standard) 140-2를 준수하는 유휴 데이터 암호화 솔루션이 있습니다.

- NetApp Storage Encryption(NSE)은 자체 암호화 드라이브를 사용하는 하드웨어 솔루션입니다.
- NetApp Volume Encryption(NVE)은 각 볼륨의 고유 키를 사용하여 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.
- NetApp Aggregate Encryption(NAE)은 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

NSE, NVE, NAE는 외부 키 관리 또는 온보드 키 관리자(OKM)를 사용할 수 있습니다. NSE, NVE, NAE를 사용할 경우 ONTAP 스토리지 효율성 기능에 영향을 미치지 않습니다. 하지만, NVE 볼륨은 애그리게이트 중복제거에서 제외됩니다. NAE 볼륨은 애그리게이트 중복제거가 사용되며 이를 통해 더 많은 이점을 누리고 있습니다.

OKM은 NSE, NVE, NAE와 함께 유휴 데이터를 위한 모든 구성요소가 완비된 암호화 솔루션을 제공합니다.

NVE, NAE 및 OKM은 ONTAP CryptoMod를 사용합니다. CryptoMod는 CMVP FIPS 140-2 검증 모듈 목록에 나열되어 있습니다. 을 "FIPS 140-2 인증 #4144"참조하십시오.

OKM 구성을 시작하려면 `security key-manager onboard enable` 명령을 사용합니다. 외부 키 관리 상호 운용성 프로토콜(KMIP) 키 관리자를 구성하려면 `security key-manager external enable` 명령을 사용하십시오. ONTAP 9.6부터 멀티 테넌시가 외부 키 관리자를 위해 지원됩니다. 매개 변수를 사용하여 `-vserver <vserver name>` 특정 SVM에 대한 외부 키 관리를 활성화합니다. 9.6 이전 버전에서는 `security key-manager setup` OKM과 외부 키 관리자를 모두 구성하기 위해 명령을 사용했습니다. 온보드 키 관리를 위해 이 구성은 운영자 또는 관리자에게 OKM 구성을 위한 암호 설정과 추가 매개 변수를 안내합니다.

구성의 일부가 다음 예에 나와 있습니다.

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

ONTAP 9.4부터는 의 true 옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 요구할 수 `-enable-cc-mode` `security key-manager setup` 있습니다. ONTAP 9.6 이상에서 명령 구문은 입니다 `security key-manager onboard enable -cc-mode-enabled yes`.

ONTAP 9.4부터 고급 권한의 기능을 사용하여 NVE 지원 볼륨에서 데이터를 중단 없이 "스크럽" 할 수 `secure-purge` 있습니다. 암호화된 볼륨의 데이터를 스크러빙하면 물리적 미디어에서 데이터를 복구할 수 없습니다. 다음 명령을 실행하면 SVM VS1의 vol1에서 삭제된 파일이 안전하게 제거됩니다.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

ONTAP 9.7부터 VE 라이센스가 설정되어 있고 OKM 또는 외부 키 관리자가 구성되어 있고 NSE가 사용되지 않는 경우 NAE와 NVE가 기본적으로 활성화됩니다. NAE 볼륨은 NAE 애그리게이트에 대해 기본적으로 생성되며, 비 NAE 애그리게이트에 NVE 볼륨이 기본적으로 생성됩니다. 다음 명령을 입력하여 이를 재정의할 수 있습니다.

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

ONTAP 9.6부터 SVM 범위를 사용하여 클러스터에 있는 데이터 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 이는

각 테넌트가 데이터를 제공하기 위해 다른 SVM(또는 SVM 세트)을 사용하는 멀티테넌트 환경에 가장 적합합니다. 지정된 테넌트의 SVM 관리자만 해당 테넌트의 키에 액세스할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 "ONTAP 9.6 이상에서 외부 키 관리를 활성화합니다" 참조하십시오.

ONTAP 9.11.1부터는 SVM에서 기본 및 보조 키 서버를 지정하여 클러스터된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 "클러스터된 외부 키 서버를 구성합니다" 참조하십시오.

ONTAP 9.13.1부터 시스템 관리자에서 외부 키 관리자 서버를 구성할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 "외부 키 관리자를 관리합니다" 참조하십시오.

데이터 복제 암호화

저장 데이터 암호화를 보완하기 위해 SnapMirror, SnapVault 또는 FlexCache에 대해 사전 공유 키와 함께 TLS를 사용하여 클러스터 간 ONTAP 데이터 복제 트래픽을 암호화할 수 있습니다.

재해 복구, 캐싱 또는 백업을 위해 데이터를 복제할 때 ONTAP 클러스터 간에 유선으로 데이터를 전송하는 동안 해당 데이터를 보호해야 합니다. 이렇게 하면 전송 중일 때 기밀 데이터에 대한 악의적인 메시지 가로채기 공격을 방지할 수 있습니다.

ONTAP 9.6부터 클러스터 피어링 암호화는 SnapMirror, SnapVault, FlexCache와 같은 ONTAP 데이터 복제 기능에 대해 TLS 1.2 AES-256 GCM 암호화 지원을 제공합니다. 암호화는 두 클러스터 피어 간의 사전 공유 키(PSK)를 통해 설정됩니다.

ONTAP 9.15.1부터 클러스터 피어링 암호화는 SnapMirror, SnapVault, FlexCache와 같은 ONTAP 데이터 복제 기능에 대해 TLS 1.3 AES-256 GCM 암호화 지원을 제공합니다. 암호화는 두 클러스터 피어 간의 사전 공유 키(PSK)를 통해 설정됩니다.

NSE, NVE 및 NAE와 같은 기술을 사용하여 저장된 데이터를 보호하는 고객은 ONTAP 9.6 이상으로 업그레이드하여 클러스터 피어링 암호화를 사용함으로써 엔드 투 엔드 데이터 암호화를 사용할 수도 있습니다.

클러스터 피어링은 클러스터 피어 간의 모든 데이터를 암호화합니다. 예를 들어 SnapMirror를 사용하는 경우 소스 및 타겟 클러스터 피어 간의 모든 피어링 정보와 모든 SnapMirror 관계가 암호화됩니다. 클러스터 피어링 암호화가 활성화된 경우 클러스터 피어 간에 평문 데이터를 전송할 수 없습니다.

ONTAP 9.6부터는 새로운 클러스터 피어 관계에 기본적으로 암호화가 활성화됩니다. ONTAP 9.6 이전에 생성된 클러스터 피어 관계에 암호화를 활성화하려면 소스 및 타겟 클러스터를 9.6으로 업그레이드해야 합니다. 또한, `cluster peer modify` 명령을 사용하여 소스 및 타겟 클러스터 피어 모두 클러스터 피어링 암호화를 사용하도록 변경해야 합니다.

ONTAP 9.6에서는 다음 예시와 같이 기존 피어 관계를 클러스터 피어링 암호화를 사용하도록 변환할 수 있습니다.

```
On the destination cluster peer:

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the source cluster peer:

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

전송 중인 **IPsec** 데이터 암호화

데이터 복제 트래픽을 위해 NSE(NetApp Storage Encryption), NVE(NetApp Volume Encryption), CPE(클러스터 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 를 사용하여 하이브리드 멀티 클라우드 Data Fabric 전반에서 클라이언트와 스토리지 간에 엔드 투 엔드 암호화를 사용할 수 있습니다 IPsec을 선택합니다. IPsec은 NFS 또는 SMB/CIFS 암호화에 대한 대안을 제공하며 iSCSI 트래픽에 대한 전송 중인 유일한 암호화 옵션입니다.

경우에 따라 유선을 통해(또는 전송 중인) ONTAP SVM으로 전송되는 모든 클라이언트 데이터를 보호해야 할 필요가 있을 수 있습니다. 이렇게 하면 전송 중에 중요 데이터에 대한 재생 및 악의적인 메시지 가로채기 공격이 방지됩니다.

ONTAP 9.8부터 IPsec(인터넷 프로토콜 보안)은 클라이언트와 ONTAP SVM 간의 모든 IP 트래픽에 엔드 투 엔드 암호화 지원을 제공합니다. 모든 IP 트래픽에 대한 IPsec 데이터 암호화에는 NFS, iSCSI 및 SMB/CIFS 프로토콜이 포함됩니다. IPsec은 iSCSI 트래픽에 대해 전송 중인 유일한 암호화 옵션을 제공합니다.

유선을 통해 NFS 암호화를 제공하는 것은 IPsec의 주요 사용 사례 중 하나입니다. ONTAP 9.8 이전에는 NFS 유선 암호화 기능이 krb5p를 사용하여 전송 중인 NFS 데이터를 암호화하도록 Kerberos를 설정하고 구성해야 했습니다. 모든 고객 환경에서 이것이 항상 단순하거나 쉽게 달성되는 것은 아닙니다.

데이터 복제 트래픽을 위해 NSE(NetApp Storage Encryption), NVE(NetApp Volume Encryption), CPE(클러스터 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 를 사용하여 하이브리드 멀티 클라우드 Data Fabric 전반에서 클라이언트와 스토리지 간에 엔드 투 엔드 암호화를 사용할 수 있습니다 IPsec을 선택합니다.

IPSec은 IETF 표준입니다. ONTAP는 전송 모드에서 IPsec을 사용합니다. 또한 IPv4 또는 IPv6를 사용하여 클라이언트와 ONTAP 간의 키 자료를 협상하기 위해 사전 공유 키(PSK)를 사용하는 IKE(인터넷 키 교환) 프로토콜 버전 2를 활용합니다. 기본적으로 IPsec은 Suite-B AES-GCM 256비트 암호화를 사용합니다. 256비트 암호화를 지원하는 Suite-B AES-GMAC256 및 AES-CBC256도 지원됩니다.

클러스터에서 IPsec 기능을 활성화해야 하지만 SPD(보안 정책 데이터베이스) 항목을 사용하여 개별 SVM IP 주소에 적용됩니다. 정책(SPD) 항목에는 클라이언트 IP 주소(원격 IP 서브넷), SVM IP 주소(로컬 IP 서브넷), 사용할 암호화 암호 그룹 및 IKEv2를 통해 인증하고 IPsec 연결을 설정하는 데 필요한 사전 공유 암호(PSK)가 포함됩니다. 트래픽이 IPsec 연결을 통해 전달되기 전에 IPsec 정책 항목 외에 클라이언트가 동일한 정보(로컬 및 원격 IP, PSK 및 암호 그룹

)로 구성되어야 합니다. ONTAP 9.10.1부터 IPsec 인증서 인증 지원이 추가되었습니다. 이렇게 하면 IPsec 정책 제한이 제거되고 IPsec에 대한 Windows OS 지원이 활성화됩니다.

클라이언트와 SVM IP 주소 사이에 방화벽이 있는 경우 IKEv2 협상이 성공하고 IPsec 트래픽을 허용하려면 ESP 및 UDP(포트 500 및 4500) 프로토콜(인바운드(수신) 및 아웃바운드(송신) 모두 허용해야 합니다.

NetApp SnapMirror 및 클러스터 피어링 트래픽 암호화의 경우, 유선으로 전송되는 안전한 이동을 위해 IPsec보다 CPE(클러스터 피어링 암호화)를 사용하는 것이 좋습니다. CPE는 이러한 워크로드에 대해 IPsec보다 우수한 성능을 제공합니다. IPsec에 대한 라이선스가 필요하지 않으며 가져오기 또는 내보내기 제한이 없습니다.

다음 예에 표시된 것처럼 클러스터에서 IPsec을 활성화하고 단일 클라이언트 및 단일 SVM IP 주소에 대한 SPD 항목을 만들 수 있습니다.

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

관련 정보

"ONTAP 네트워크에서 IP 보안 사용을 준비합니다"

ONTAP의 FIPS 모드 및 TLS 및 SSL 관리

FIPS 140-2 표준은 컴퓨터 및 통신 시스템의 민감한 정보를 보호하는 보안 시스템 내의 암호화 모듈에 대한 보안 요구 사항을 지정합니다. FIPS 140-2 표준은 제품, 아키텍처, 데이터 또는 에코시스템이 아닌 암호화 모듈에 _ 구체적으로 _ 적용됩니다. 암호화 모듈은 NIST에서 승인한 보안 기능을 구현하는 특정 구성 요소(하드웨어, 소프트웨어, 펌웨어 또는 세 가지 구성 요소의 조합)입니다.

FIPS 140-2 규정 준수를 활성화하면 ONTAP 9 내부 및 외부 시스템과 통신할 수 있습니다. NetApp에서는 콘솔 액세스 권한이 있는 비프로덕션 시스템에서 이러한 설정을 테스트하는 것이 좋습니다.

ONTAP 9.11.1 및 TLS 1.3 지원부터 FIPS 140-3을 검증할 수 있습니다.

FIPS 구성은 ONTAP 및 플랫폼 BMC에 적용됩니다.

NetApp ONTAP의 FIPS 모드 구성

NetApp ONTAP에는 컨트롤 플레인에 추가 보안 수준을 인스턴스화하는 FIPS 모드 구성이 있습니다.

- FIPS 140-2 준수 모드가 활성화되면 ONTAP 9.11.1부터 TLSv1, TLSv1.1 및 SSLv3이 비활성화되고 TSLv1.2 및 TSLv1.3만 활성화됩니다. ONTAP 9 내부와 외부의 다른 시스템 및 통신에 영향을 줍니다. FIPS 140-2 규정 준수 모드를 활성화한 후 이후에 사용하지 않도록 설정하는 경우 TLSv1, TLSv1.1 및 SSLv3은 비활성화 상태로 유지됩니다. TLSv1.2 또는 TLSv1.3은 이전 구성에 따라 활성화된 상태로 유지됩니다.

- FIPS 140-2 준수 모드가 활성화된 경우 9.11.1 이전 버전의 ONTAP에서는 TLSv1 및 SSLv3이 모두 비활성화되고 TLSv1.1 및 TLSv1.2만 활성화됩니다. ONTAP를 사용하면 FIPS 140-2 규정 준수 모드가 활성화된 경우 TLSv1 및 SSLv3을 모두 사용할 수 없습니다. FIPS 140-2 규정 준수 모드를 활성화한 후 나중에 비활성화하면 TLSv1 및 SSLv3은 비활성화 상태로 유지되지만 TLSv1.2 또는 TLSv1.1 및 TLSv1.2는 이전 구성에 따라 모두 활성화됩니다.
- "NetApp 암호화 보안 모듈(NCSM)"FIPS 140-2 레벨 1에서 검증된 소프트웨어 기반 규정 준수를 제공합니다.

NIST는 FIPS-140-3 표준을 제출했으며, NCSM은 FIPS-140-2 및 FIPS-140-3 검증을 거치게 됩니다. 모든 FIPS 140-2 검증은 2026년 9월 21일에 기록적인 상태로 전환되며, 이는 새 인증서 제출의 마지막 날보다 5년 후입니다.

FIPS-140-2 및 **FIPS-140-3** 규정 준수 모드를 사용합니다

ONTAP 9부터 클러스터 전체 컨트롤 플레인 인터페이스에 대해 FIPS-140-2 및 FIPS-140-3 규정 준수 모드를 활성화할 수 있습니다.

- "FIPS를 활성화합니다"
- "FIPS 상태를 봅니다"

FIPS 지원 및 프로토콜

`security config modify`명령을 사용하여 기존 클러스터 차원의 보안 구성을 수정할 수 있습니다. `FIPS` 호환 모드를 활성화하면 클러스터에서 `TLS` 프로토콜만 자동으로 선택됩니다.

- `-supported-protocols`FIPS 모드와 별개로 TLS 프로토콜을 포함하거나 제외하려면 매개 변수를 사용하십시오. 기본적으로 FIPS 모드는 비활성화되고 TLSv1.3(ONTAP 9.11.1로 시작) 및 TLSv1.2 프로토콜은 활성화됩니다.
- 이전 ONTAP 릴리스에는 기본적으로 다음과 같은 TLS 프로토콜이 활성화되어 있었습니다.
  - TLSv1.1(ONTAP 9.12.1부터 기본적으로 비활성화됨)
  - TLSv1(ONTAP 9.8부터 기본적으로 비활성화됨)
- 이전 버전과의 호환성을 위해 ONTAP는 FIPS 모드가 비활성화된 경우 지원되는 프로토콜 목록에 SSLv3을 추가할 수 있도록 지원합니다.

FIPS 지원 및 암호화

- 매개 변수를 사용하여 `-supported-cipher-suites` AES(Advanced Encryption Standard) 또는 AES 및 3DES 만 구성합니다.
- 를 지정하여 RC4와 같은 약한 암호를 비활성화할 수 `!RC4` 있습니다. 기본적으로 지원되는 암호화 설정은 입니다 `ALL:!LOW:!aNULL:!EXP:!eNULL`. 이 설정은 인증, 암호화, 내보내기 없음 및 저암호화 암호화 암호화 암호화 그룹이 없는 64비트 또는 56비트 암호화 알고리즘을 사용하는 경우를 제외하고 프로토콜에 대해 지원되는 모든 암호화 제품군을 사용하도록 설정합니다.
- 선택한 해당 프로토콜에서 사용할 수 있는 암호 그룹을 선택합니다. 잘못된 구성으로 인해 일부 기능이 제대로 작동하지 않을 수 있습니다.
- 올바른 암호 문자열 구문은 "암호 페이지" OpenSSL 소프트웨어 재단에서 게시한 on OpenSSL을 참조하십시오. ONTAP 9.9.1 이상 릴리스부터 보안 구성을 수정한 후 더 이상 모든 노드를 수동으로 재부팅할 필요가 없습니다.

SSH 및 **TLS** 보안 강화

ONTAP 9의 SSH 관리를 위해서는 OpenSSH 클라이언트 5.7 이상이 필요합니다. SSH 클라이언트가 연결에 성공하려면 ECDSA(Elliptic Curve Digital Signature Algorithm) 공개 키 알고리즘과 협상해야 합니다.

TLS 보안을 강화하려면 TLS 1.2만 활성화하고 PFS(Perfect Forward Secrecy)가 가능한 암호 그룹을 사용합니다. PFS는 TLS 1.2와 같은 암호화 프로토콜과 함께 사용할 경우 공격자가 클라이언트와 서버 간의 모든 네트워크 세션을 해독하지 못하도록 하는 키 교환 방법입니다.

TLSv1.2 및 **PFS** 지원 암호화 제품군을 활성화합니다

TLS 1.2 및 PFS 지원 암호 그룹만 활성화하려면 `security config modify` 고급 권한 수준의 명령을 사용합니다.

SSL 인터페이스 구성을 변경하기 전에 ONTAP에 연결할 때 클라이언트가 ONTAP와의 연결을 유지하기 위해 DHE 및 ECDHE 암호화를 지원하는지 확인하십시오.

예

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

`y`각 프롬프트에 대해 확인합니다. `PFS`에 대한 자세한 내용은 다음을 `https://blog.netapp.com/protecting-your-data-perfect-forward-secrecy-pfs-with-netapp-ontap/`["NetApp 블로그"^]참조하십시오.

관련 정보

"FIPS(Federal Information Processing Standard) Publication 140"

CA 서명 디지털 인증서를 만듭니다

대부분의 조직에서 ONTAP 웹 액세스용 자체 서명된 디지털 인증서는 InfoSec 정책을 준수하지 않습니다. 운영 시스템에서는 클러스터 또는 SVM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치하는 것이 NetApp 모범 사례입니다.

명령을 사용하여 CSR(인증서 서명 요청)을 생성하고 명령을 사용하여 CA에서 받은 인증서를 설치할 수 `security certificate generate-csr` `security certificate install` 있습니다.

단계

1. 조직의 CA에서 서명한 디지털 인증서를 만들려면 다음을 실행합니다.
   a. CSR을 생성합니다.
   b. 조직의 절차에 따라 조직의 CA에서 CSR을 사용하여 디지털 인증서를 요청합니다. 예를 들어 Microsoft Active Directory 인증서 서비스 웹 인터페이스를 사용하여 로 `<CA_server_name>/certsrv` 이동하여 인증서를 요청합니다.
   c. ONTAP에 디지털 인증서를 설치합니다.

온라인 인증서 상태 프로토콜입니다

OCSP(온라인 인증서 상태 프로토콜)를 사용하면 LDAP 또는 TLS와 같은 TLS 통신을 사용하는 ONTAP 애플리케이션이 OCSP가 설정된 경우 디지털 인증서 상태를 수신할 수 있습니다. 응용 프로그램에서 요청된 인증서가 양호하거나 해지되었거나 알 수 없음을 나타내는 서명된 응답을 받습니다.

OCSP를 사용하면 인증서 해지 목록(CRL) 없이도 디지털 인증서 상태를 확인할 수 있습니다.

기본적으로 OCSP 인증서 상태 확인은 사용되지 않습니다. 앱 이름은 , , , , , , 로 설정할 수 있는 명령을 사용하여 켤 수 `security config ocsp enable -app name`있습니다. `autosupport audit_log fabricpool ems kmip ldap_ad ldap_nis_namemap`, 또는 `all` 이 명령에는 advanced 권한 수준이 필요합니다.

SSHv2 관리

이 `security ssh modify` 명령을 실행하면 클러스터에 대한 SSH 키 교환 알고리즘, 암호 또는 MAC 알고리즘의 기존 구성을 지정한 구성 설정으로 대체합니다.

NetApp에서 권장하는 사항은 다음과 같습니다.

- 사용자 세션에 암호를 사용합니다.
- 컴퓨터 액세스에 공개 키를 사용합니다.

지원되는 암호 및 키 교환

암호입니다	키 교환
AES256-CTR	Diffie-Hellman-group-exchange-SHA256(SHA-2)
AES192 - CTR	Diffie-Hellman-group-exchange-SHA1(SHA-1)
AES128-CTR	Diffie-Hellman-group14-SHA1(SHA-1)
AES256 - CBC	Diffie-Hellman-group1-SHA1(SHA-1)
AES192 - CBC	-
AES128 - CBC	-
AES128-GCM을 참조하십시오	-
AES256-GCM을 참조하십시오	-
3DES-CBC입니다	-

AES 및 **3DES** 대칭 암호화가 지원됩니다

ONTAP는 다음 유형의 AES 및 3DES 대칭 암호화(암호라고도 함)도 지원합니다.

- HMAC-SHA1
- HMAC-SHA1-96
- HMAC-MD5 를 참조하십시오

- HMAC-MD5-96
- HMAC-RIPEMD160
- umac-64
- umac-64
- umac-128
- HMAC-SHA2-256
- HMAC-SHA2-512
- HMAC-SHA1-ETM
- HMAC-SHA1-96-ETM
- HMAC-SHA2-256-ETM
- HMAC-SHA2-512-ETM
- HMAC-MD5-ETM의 약어입니다
- HMAC-MD5-96-ETM
- HMAC-RIPEMD160-ETM
- umac-64-ETM
- umac-128-ETM

SSH 관리 구성은 ONTAP 및 플랫폼 BMC에 적용됩니다.

NetApp AutoSupport를 참조하십시오

ONTAP의 AutoSupport 기능을 사용하면 시스템의 상태를 사전에 모니터링하고 메시지와 세부 정보를 NetApp 기술 지원, 조직의 내부 지원 팀 또는 지원 파트너에게 자동으로 보낼 수 있습니다. 기본적으로 스토리지 시스템을 처음 구성하면 NetApp 기술 지원에 보내는 AutoSupport 메시지가 사용하도록 설정됩니다. 또한 AutoSupport는 NetApp 기술 지원이 활성화된 후 24시간 후에 메시지를 보내기 시작합니다. 이 24시간 기간은 구성 가능합니다. 조직의 내부 지원 팀과의 통신을 활용하려면 메일 호스트 구성을 완료해야 합니다.

클러스터 관리자만 AutoSupport 관리(구성)를 수행할 수 있습니다. SVM 관리자는 AutoSupport에 액세스할 수 없습니다. AutoSupport 기능을 비활성화할 수 있습니다. 하지만 NetApp 스토리지 시스템에서 문제가 발생하는 경우 AutoSupport가 문제를 더 빠르게 식별하고 해결할 수 있도록 이 기능을 사용하도록 설정하는 것이 좋습니다. 기본적으로 시스템은 AutoSupport 정보를 수집하여 사용자가 AutoSupport를 사용하지 않도록 설정한 경우에도 로컬에 저장합니다.

다양한 메시지에 포함된 내용 및 다양한 유형의 메시지가 전송되는 위치를 비롯하여 AutoSupport 메시지에 대한 자세한 내용은 설명서를 참조하십시오. "NetApp 디지털 자문"

AutoSupport 메시지에는 다음 항목을 포함하되 이에 국한되지 않는 중요한 데이터가 포함됩니다.

- 로그 파일
- 특정 하위 시스템과 관련된 상황에 맞는 데이터입니다
- 구성 및 상태 데이터

- 성능 데이터

AutoSupport는 전송 프로토콜에 HTTPS 및 SMTP를 지원합니다. AutoSupport 메시지는 기본적으로 민감하므로 NetApp 지원에 AutoSupport 메시지를 보낼 때 HTTPS를 기본 전송 프로토콜로 사용하는 것이 좋습니다.

또한 명령을 활용하여 `system node autosupport modify` AutoSupport 데이터의 타겟을 지정해야 합니다(예: NetApp 기술 지원, 조직의 내부 운영, 파트너). 이 명령을 사용하여 보낼 특정 AutoSupport 세부 정보(예: 성능 데이터, 로그 파일 등)를 지정할 수도 있습니다.

AutoSupport를 완전히 해제하려면 `system node autosupport modify -state disable` 명령을 사용합니다.

Network Time Protocol의 약어입니다

ONTAP를 사용하면 클러스터에서 시간대, 날짜 및 시간을 수동으로 설정할 수 있지만 적어도 3개의 외부 NTP 서버와 클러스터 시간을 동기화하도록 NTP(네트워크 시간 프로토콜) 서버를 구성해야 합니다.

클러스터 시간이 정확하지 않을 수 있습니다. ONTAP를 사용하면 클러스터에서 시간대, 날짜 및 시간을 수동으로 설정할 수 있지만 클러스터 시간을 외부 NTP 서버와 동기화하도록 NTP(네트워크 시간 프로토콜) 서버를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 구성할 수 있습니다.

명령을 사용하여 최대 10개의 외부 NTP 서버를 연결할 수 `cluster time-service ntp server create` 있습니다. 시간 서비스의 이중화 및 품질을 위해 최소 3개의 외부 NTP 서버를 클러스터에 연결해야 합니다.

ONTAP에서 NTP 구성에 대한 자세한 내용은 을 참조하십시오 "클러스터 시간 관리(클러스터 관리자만 해당)".

NAS 파일 시스템 로컬 계정(CIFS 작업 그룹)

워크그룹 클라이언트 인증은 기존의 도메인 인증 방식과 동일하게 ONTAP 솔루션에 추가적인 보안 계층을 제공합니다. 명령을 사용하면 `vserver cifs session show` IP 정보, 인증 메커니즘, 프로토콜 버전 및 인증 유형을 비롯한 다양한 상태 관련 세부 정보를 표시할 수 있습니다.

ONTAP 9부터 로컬로 정의된 사용자 및 그룹을 사용하여 서버에 인증하는 CIFS 클라이언트를 사용하여 작업 그룹에 CIFS 서버를 구성할 수 있습니다. 워크그룹 클라이언트 인증은 기존의 도메인 인증 방식과 동일하게 ONTAP 솔루션에 추가적인 보안 계층을 제공합니다. CIFS 서버를 구성하려면 명령을 사용합니다 `vserver cifs create` . CIFS 서버를 생성한 후에는 CIFS 도메인에 연결하거나 작업 그룹에 연결할 수 있습니다. 작업 그룹에 참여하려면 `-workgroup` 매개 변수를 사용합니다. 다음은 구성의 예입니다.

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

작업 그룹 모드의 CIFS 서버는 Windows NT LAN Manager(NTLM) 인증만 지원하며 Kerberos 인증은 지원하지 않습니다.

NetApp은 NTLM 인증 기능을 CIFS 작업 그룹과 함께 사용하여 조직의 보안 상태를 유지할 것을 권장합니다. NetApp은 명령을 사용하여 CIFS 보안 상태를 검증하기 위해 IP 정보, 인증 메커니즘, 프로토콜 버전 및 인증 유형 등의 다양한 상태 관련 세부 정보를 표시할 것을 `vserver cifs session show` 권장합니다.

NAS 파일 시스템 감사

NAS 파일 시스템이 차지하는 공간 증가 오늘날의 위협 환경에서 감사 기능은 가시성을 지원하는 데 매우 중요합니다.

보안에는 검증이 필수적입니다. ONTAP는 솔루션 전반에 걸쳐 향상된 감사 이벤트와 세부 정보를 제공합니다. 오늘날의 위협 환경에서 NAS 파일 시스템의 비중이 점점 커지고 있기 때문에 가시성을 확보하기 위해서는 감사 기능이 매우 중요합니다. ONTAP의 향상된 감사 기능 덕분에 CIFS 감사 세부 정보가 그 어느 때보다 풍부해졌습니다. 다음과 같은 주요 세부 정보가 생성된 이벤트와 함께 기록됩니다:

- 파일, 폴더 및 공유 액세스
- 생성, 수정 또는 삭제된 파일
- 파일 읽기 액세스가 성공했습니다
- 파일 읽기 또는 쓰기 시도가 실패했습니다
- 폴더 권한 변경

감사 구성을 생성합니다

감사 이벤트를 생성하려면 CIFS 감사를 설정해야 합니다. 명령을 사용하여 `vserver audit create` 감사 구성을 생성합니다. 기본적으로 감사 로그는 크기에 따라 순환 방법을 사용합니다. Rotation Parameters(회전 매개변수) 필드에 지정된 경우 시간 기반 회전 옵션을 사용할 수 있습니다. 추가 로그 감사 회전 구성 세부 정보에는 회전 일정, 회전 제한, 주중 회전 날짜 및 회전 크기가 포함됩니다. 다음 텍스트는 12:30에 모든 요일에 대해 예약된 월별 시간 기반 순환을 사용하는 감사 구성을 보여 주는 예제 구성을 제공합니다.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS 감사 이벤트입니다

CIFS 감사 이벤트는 다음과 같습니다.

- * File share *: CIFS 네트워크 공유가 추가, 수정 또는 삭제될 때 관련 명령을 사용하여 감사 이벤트를 `vserver cifs share` 생성합니다.
- * 감사 정책 변경 *: 감사 정책이 비활성화, 활성화 또는 수정된 경우 관련 명령을 사용하여 감사 이벤트를 `vserver audit` 생성합니다.
- * 사용자 계정 *: 로컬 CIFS 또는 UNIX 사용자가 생성 또는 삭제되거나, 로컬 사용자 계정이 활성화, 비활성화 또는 수정되거나, 암호가 재설정되거나 변경될 때 감사 이벤트를 생성합니다. 이 이벤트는 `vserver cifs users-and-groups local-group` 명령 또는 관련 `vserver services name-service unix-user` 명령을 사용합니다.
- * Security group *: 명령 또는 관련 명령을 사용하여 로컬 CIFS 또는 UNIX 보안 그룹을 생성하거나 삭제할 때 감사 이벤트를 `vserver cifs users-and-groups local-group` `vserver services name-service`

`unix-group` 생성합니다.

- * 권한 부여 정책 변경 *: 명령을 사용하여 CIFS 사용자 또는 CIFS 그룹에 대한 권한이 부여되거나 취소될 때 감사 이벤트를 `vserver cifs users-and-groups privilege` 생성합니다.

> 이 기능은 시스템 감사 기능을 기반으로 합니다. 이 기능을 사용하면 관리자가 데이터 사용자의 관점에서 시스템에서 허용하고 수행하는 작업을 검토할 수 있습니다.

REST API가 **NAS** 감사에 미치는 영향

ONTAP에는 관리자 계정이 REST API를 사용하여 SMB/CIFS 또는 NFS 파일에 액세스하고 조작할 수 있는 기능이 포함되어 있습니다. REST API는 ONTAP 관리자만 실행할 수 있지만 REST API 명령은 시스템 NAS 감사 로그를 무시합니다. 또한 REST API를 사용할 때 ONTAP 관리자가 파일 권한을 무시할 수도 있습니다. 그러나 파일에 대한 REST API를 사용한 관리자의 작업은 시스템 명령 기록 로그에 기록됩니다.

액세스할 수 없는 **REST API** 역할을 생성합니다

REST를 통해 ONTAP 볼륨에 액세스할 수 없는 REST API 역할을 생성하여 ONTAP 관리자가 파일 액세스에 REST API를 사용하지 못하도록 할 수 있습니다. 이 역할을 프로비저닝하려면 다음 단계를 완료하십시오.

> /api/storage/volumes REST API는 파일 액세스 이상의 용도로 사용됩니다. System Manager 및 기타 GUI 인터페이스에서 볼륨을 생성, 조회 및 수정하는 데 사용됩니다.

단계

1. 스토리지 볼륨에 대한 액세스 권한이 없지만 다른 모든 REST API 액세스가 가능한 새 REST 역할을 생성합니다.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 이전 단계에서 만든 새 REST API 역할에 관리자 계정을 할당합니다.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

> 기본 제공 ONTAP 클러스터 관리자 계정에서 파일 액세스에 REST API를 사용하지 않으려면 먼저 해야 "새 관리자 계정을 만들고 기본 제공 계정을 사용 안 함 또는 삭제합니다"합니다.

CIFS SMB 서명 및 봉인을 구성하고 사용하도록 설정합니다

스토리지 시스템과 클라이언트 간의 트래픽이 재생 공격이나 메시지 가로채기 공격으로 인해 손상되지 않도록 하여 Data Fabric의 보안을 보호하는 SMB 서명을 구성하고 사용하도록 설정할 수 있습니다. SMB 서명은 SMB 메시지에 유효한 서명이 있는지 확인하여 보호합니다.

이 작업에 대해

파일 시스템 및 아키텍처의 일반적인 위협 벡터는 SMB 프로토콜에 있습니다. 이 문제를 해결하기 위해 ONTAP 9 솔루션은 업계 표준 SMB 서명 및 봉인을 사용합니다. SMB 서명을 활용하면 스토리지 시스템과 클라이언트 사이의 트래픽이 재생 공격이나 메시지 가로채기 공격으로 인해 손상되지 않도록 하여 Data Fabric의 보안을 보호할 수 있습니다. 이는 SMB 메시지에 포함되는 유효한 서명이 있는지 확인하는 것으로 간주됩니다.

SMB 서명은 성능을 위해 기본적으로 비활성화되어 있지만 NetApp에서는 이를 사용하도록 설정하는 것이 좋습니다. 또한 ONTAP 솔루션은 봉인이라고도 하는 SMB 암호화를 지원합니다. 이 접근 방식을 사용하면 공유별로 데이터를 안전하게 전송할 수 있습니다. 기본적으로 SMB 암호화는 비활성화되어 있습니다. 그러나 NetApp는 SMB 암호화를 활성화할 것을 권장합니다.

이제 SMB 2.0 이상에서 LDAP 서명 및 봉인이 지원됩니다. 서명(변조 방지)과 봉인(암호화)을 통해 SVM과 Active Directory 서버 간의 안전한 통신을 지원합니다. 이제 SMB 3.0 이상에서 AES 새 명령(Intel AES NI) 암호화가 지원됩니다. 더욱 개선된 AES 알고리즘인 Intel AES NI는 지원되는 프로세서 제품군에서 데이터 암호화의 성능을 높여 줍니다.

단계

1. SMB 서명을 구성하고 사용하도록 설정하려면 명령을 사용하고 `vserver cifs security modify` 매개 변수가 (으)로 설정되어 있는지 `-is-signing-required` `true`확인하십시오. 다음 예제 구성을 참조하십시오.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. SMB 봉인 및 암호화를 구성하고 사용하도록 설정하려면 명령을 사용하여 `vserver cifs security modify` 매개 변수가 으로 설정되어 있는지 `-is-smb-encryption-required` `true`확인하십시오. 다음 예제 구성을 참조하십시오.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFS 보안

내보내기 규칙은 엑스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성하는 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청과 일치합니다. 클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 엑스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 엑스포트 정책에 표시되는 순서대로 처리됩니다.

액세스 제어는 안전한 태세를 유지하는 데 있어 핵심입니다. 따라서 ONTAP은 엑스포트 정책 기능을 사용하여 특정 매개 변수와 일치하는 클라이언트에 대한 NFS 볼륨 액세스를 제한합니다. 엑스포트 정책에는 각 클라이언트 액세스 요청을 처리하는 엑스포트 규칙이 하나 이상 포함되어 있습니다. 엑스포트 정책은 각 볼륨과 연결되어 볼륨에 대한

클라이언트 액세스를 구성합니다. 이 프로세스의 결과는 클라이언트가 볼륨에 대한 액세스 권한을 부여 또는 거부(권한 거부 메시지 포함)할지 여부를 결정합니다. 이 프로세스는 볼륨에 제공되는 액세스 레벨도 결정합니다.

클라이언트가 데이터에 액세스하려면 SVM에 엑스포트 규칙이 있는 엑스포트 정책이 있어야 합니다. SVM은 여러 엑스포트 정책을 포함할 수 있습니다.

규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 사용 권한이 사용되고 더 이상 규칙이 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

내보내기 규칙은 다음 기준을 적용하여 클라이언트 액세스 권한을 결정합니다.

- 클라이언트에서 요청을 보내는 데 사용되는 파일 액세스 프로토콜(예: NFSv4 또는 SMB)
- 클라이언트 식별자(예: 호스트 이름 또는 IP 주소)
- 클라이언트가 인증하는 데 사용하는 보안 유형(예: Kerberos v5, NTLM 또는 AUTH_SYS)

규칙이 여러 조건을 지정하고 클라이언트가 하나 이상의 조건을 일치하지 않으면 규칙이 적용되지 않습니다.

엑스포트 정책의 예로는 다음과 같은 매개 변수를 가진 엑스포트 규칙이 있습니다.

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

보안 유형은 클라이언트가 받는 액세스 수준을 결정합니다. 세 가지 액세스 수준은 읽기 전용, 읽기/쓰기 및 수퍼유저입니다(사용자 ID가 있는 클라이언트의 경우 `0`). 보안 유형에 의해 결정되는 액세스 수준은 이 순서로 평가되므로 나열된 규칙을 준수해야 합니다.

내보내기 규칙의 액세스 수준 매개 변수에 대한 규칙입니다

클라이언트가 다음과 같은 액세스 수준을 얻을 수 있습니다	이러한 액세스 매개 변수는 클라이언트의 보안 유형과 일치해야 합니다
일반 사용자 읽기 전용	읽기 전용(`-rorule`)
일반 사용자 읽기-쓰기	읽기 전용(`-rorule`) 및 읽기-(`-rwrule`쓰기)
고급 사용자 읽기 전용	읽기 전용(`-rorule`) 및 `-superuser`
고급 사용자 읽기-쓰기	읽기 전용(`-rorule`) (`-rwrule`및 읽기/쓰기) 및 `-superuser`

다음은 이러한 세 가지 액세스 매개 변수 각각에 대해 유효한 보안 유형입니다.

- 모두
- 없음

- 안 함

다음 보안 형식은 매개 변수와 함께 사용할 수 `-superuser` 없습니다.

- krb5를 참조하십시오
- NTLM입니다
- 시스템

매개 변수 결과에 액세스하기 위한 규칙입니다

클라이언트의 보안 유형이 다음과 같은 경우	결과
access 매개 변수에 지정된 보안 유형과 일치합니다.	클라이언트는 자체 사용자 ID를 사용하여 해당 수준에 대한 액세스를 받습니다.
지정된 보안 유형과 일치하지 않지만 access 매개 변수에 옵션이 포함되어 `none`있습니다.	클라이언트는 해당 레벨에 대한 액세스 권한을 받고 매개 변수로 지정된 사용자 ID를 사용하여 익명 사용자를 `-anon` 받습니다.
지정된 보안 유형과 일치하지 않으며 access 매개 변수에 옵션이 포함되어 있지 `none`않습니다.	클라이언트는 해당 레벨에 대한 액세스 권한을 받지 않습니다. 이 매개 변수는 지정되지 않은 경우에도 항상 없음이 포함되므로 이 제한은 매개 변수에 적용되지 `-superuser` 않습니다.

Kerberos 5 및 **Krb5p**

ONTAP 9부터 개인 정보 보호 서비스(krb5p)를 통한 Kerberos 5 인증이 지원됩니다. krbp5 인증 모드는 안전하며 체크섬을 사용하여 클라이언트와 서버 간의 모든 트래픽을 암호화하여 데이터 무단 변경 및 스누핑으로부터 보호합니다. ONTAP 솔루션은 Kerberos 128비트/256비트 AES 암호화를 지원합니다. 개인정보보호 서비스에는 수신 데이터의 무결성 확인, 사용자 인증, 전송 전 데이터 암호화가 포함됩니다.

krb5p 옵션은 암호화 옵션으로 설정된 내보내기 정책 기능에 가장 많이 있습니다. 다음 예와 같이 krb5p 인증 방법을 인증 매개 변수로 사용할 수 있습니다.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Lightweight Directory Access Protocol 서명 및 봉인을 활성화합니다

서명과 봉인을 지원하여 LDAP 서버에 대한 쿼리에 대한 세션 보안을 활성화합니다. 이 접근 방식은 LDAP-over-TLS 세션 보안을 대체할 수 있습니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. SVM의 세션 보안 설정은 LDAP 서버에서 사용할 수 있는 설정과 일치합니다. 기본적으로 LDAP 서명 및 봉인은 사용되지 않습니다.

단계

1. 이 기능을 활성화하려면 `vserver cifs security modify` 매개 변수를 사용하여 명령을 `session-security-for-ad-ldap` 실행합니다.

   LDAP 보안 기능 옵션:

   - * 없음 *: 기본값, 서명 또는 봉인 없음
   - * 서명 *: LDAP 트래픽에 서명합니다
   - * Seal *: LDAP 트래픽을 서명 및 암호화합니다

   > 서명 및 봉인 매개변수는 누적되므로 서명 옵션을 사용할 경우 결과가 서명과 함께 LDAP 입니다. 단, 씰 옵션을 사용할 경우 결과는 표지와 씰입니다. 또한 이 명령에 매개 변수를 지정하지 않으면 기본값은 none입니다.

   다음은 구성의 예입니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

NetApp FPolicy를 생성하여 사용합니다

ONTAP 솔루션의 인프라 구성요소인 FPolicy를 생성하여 파트너 애플리케이션이 파일 액세스 권한을 모니터링하고 설정할 수 있도록 합니다. 더욱 강력한 애플리케이션 중 하나는 하이브리드 클라우드 환경 전반에서 모든 기업 데이터 액세스에 대한 중앙 집중식 가시성과 제어를 제공하여 보안 및 규정 준수 목표를 달성하는 NetApp SaaS 애플리케이션인 스토리지 워크로드 보안입니다.

액세스 제어는 중요한 보안 개념입니다. 가시성과 파일 액세스 및 파일 작업에 대응하는 기능은 보안 태세를 유지하는 데 있어 아주 중요합니다. 가시성과 파일 액세스 제어를 제공하기 위해 ONTAP 솔루션은 NetApp FPolicy 기능을 사용합니다.

파일 유형에 따라 파일 정책을 설정할 수 있습니다. FPolicy는 스토리지 시스템이 개별 클라이언트 시스템에서 요청한 생성, 열기, 이름 변경, 삭제 등의 작업을 처리하는 방식을 결정합니다. ONTAP 9부터 FPolicy 파일 액세스 알림 프레임워크가 개선되어 필터링 제어 및 단기적인 네트워크 중단에 대비한 복원력을 갖추게 되었습니다.

단계

1. FPolicy 기능을 활용하려면 먼저 명령으로 FPolicy 정책을 생성해야 `vserver fpolicy policy create` 합니다.

   > 또한 `-events` 가시성과 이벤트 수집에 FPolicy를 사용하는 경우 매개 변수를 사용하십시오. ONTAP에서 제공하는 추가 세분화 수준을 통해 필터링 및 사용자 이름 제어 수준까지 액세스할 수 있습니다. 사용자 이름으로 권한을 제어하고 액세스를 제어하려면 `-privilege-user-name` 매개 변수를 지정합니다.

   다음 텍스트는 FPolicy 생성의 예를 제공합니다.

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. FPolicy 정책을 생성한 후에는 명령으로 정책을 활성화해야 `vserver fpolicy enable` 합니다. 또한 이 명령은 FPolicy 항목의 우선순위 또는 순서를 설정합니다.

   FPolicy 시퀀스는 여러 정책이 동일한 파일 액세스 이벤트를 구독한 경우 액세스 허용 또는 거부 순서를 지시하기 때문에 중요합니다.

   다음 텍스트는 FPolicy 정책을 설정하고 명령을 통해 구성을 검증하기 위한 샘플 구성을 `vserver fpolicy show` 제공합니다.

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

FPolicy 개선 사항

ONTAP 9에는 다음 섹션에서 설명하는 FPolicy 개선 사항이 포함되어 있습니다.

필터링 컨트롤

디렉터리 활동에 대한 알림을 제거하거나 제거하는 데 새 필터를 사용할 수 `SetAttr` 있습니다.

비동기식 복원력

비동기 모드에서 작동하는 FPolicy 서버에서 네트워크 중단이 발생하는 경우, 정전 중에 생성된 FPolicy 알림은 스토리지 노드에 저장됩니다. FPolicy 서버가 온라인 상태로 돌아오면 저장된 알림에 대한 알림이 표시되고 스토리지 노드에서 가져올 수 있습니다. 정전 중에 알림을 저장할 수 있는 시간은 최대 10분까지 구성할 수 있습니다.

ONTAP에서 LIF 역할의 보안 특성입니다

LIF는 역할, 홈 포트, 홈 노드, 페일오버할 포트 목록 및 방화벽 정책과 같은 관련 특성이 있는 IP 주소 또는 WWPN(Worldwide Port Name)입니다. 클러스터가 네트워크를 통해 통신을

주고받는 포트에 LIF를 구성할 수 있습니다. 각 LIF 역할의 보안 특성을 이해하는 것이 중요합니다.

LIF 역할

LIF 역할은 다음과 같습니다.

- * 데이터 LIF *: SVM에 연결된 LIF로 클라이언트와의 통신에 사용됩니다.
- * 클러스터 LIF *: 클러스터 내 노드 간에 클러스터 간 트래픽을 전달하는 데 사용되는 LIF.
- * 노드 관리 LIF *: 클러스터의 특정 노드를 관리하기 위한 전용 IP 주소를 제공하는 LIF입니다.
- * 클러스터 관리 LIF *: 전체 클러스터에 대한 단일 관리 인터페이스를 제공하는 LIF입니다.
- * Intercluster LIF *: 클러스터 간 통신, 백업 및 복제에 사용되는 LIF.

각 **LIF** 역할의 보안 특성입니다

	Data LIF	클러스터 **LIF**입니다	노드 관리 **LIF**	클러스터 관리 **LIF**입니다	인터클러스터 **LIF**
프라이빗 IP 서브넷이 필요합니까?	아니요	예	아니요	아니요	아니요
보안 네트워크가 필요하십니까?	아니요	예	아니요	아니요	예
기본 방화벽 정책	매우 제한적입니다	완전히 열립니다	중간	중간	매우 제한적입니다
방화벽을 사용자 정의할 수 있습니까?	예	아니요	예	예	예

- 클러스터 LIF는 구성 가능한 방화벽 정책을 가지고 있지 않으며 완전히 열리기 때문에 격리된 보안 네트워크의 프라이빗 IP 서브넷에 있어야 합니다.
- LIF 역할은 인터넷에 공개되어서는 안 됩니다.

LIF 보안에 대해 자세히 알아보려면 다음을 참조하세요. "LIF의 방화벽 정책을 구성합니다". 이 페이지에서는 ONTAP 9.10.1부터 시작되는 LIF 서비스 정책에 대한 세부 정보도 제공합니다.

새 서비스 정책을 만드는 방법에 대해 자세히 알아보려면 다음을 참조하세요. `network interface service-policy create` 명령 "명령어 참조."

프로토콜 및 포트 보안

솔루션 강화에는 온박스 보안 작업 및 기능 외에도 오프 박스 보안 메커니즘도 포함되어야 합니다. 방화벽, IPs(침입 방지 시스템) 및 기타 보안 장치와 같은 추가 인프라 장치를 활용하여 ONTAP에 대한 액세스를 필터링하고 제한하는 것은 엄격한 보안 태세를 구축하고 유지하는 효과적인 방법입니다. 이 정보는 환경과 해당 리소스에 대한 액세스를 필터링하고 제한하기 위한 핵심 구성 요소입니다.

일반적으로 사용되는 프로토콜 및 포트

서비스	포트/프로토콜	설명
SSH	22/TCP입니다	SSH 로그인
telnet	23/TCP입니다	원격 로그인
Domain	53/TCP입니다	도메인 이름 서버
HTTP	80/TCP입니다 80/UDP입니다	HTTP
rpcbind	111/TCP 111/UDP	원격 프로시저 호출
NTP	123/UDP입니다	Network Time Protocol의 약어입니다
msrpc	135/TCP입니다	Microsoft 원격 프로시저 호출
Netbios-name	137/TCP 137/UDP	NetBIOS 이름 서비스입니다
netbios-ssn	139/TCP입니다	NetBIOS 서비스 세션입니다
SNMP	161/UDP입니다	SNMP를 선택합니다
HTTPS	443/TCP입니다	보안 링크: http
microsoft-ds	445/TCP입니다	Microsoft 디렉토리 서비스
IPsec	500/UDP입니다	인터넷 프로토콜 보안
mount	635/UDP입니다	NFS 마운트
named	953/UDP입니다	이름 데몬입니다
NFS	2049/UDP 2049/TCP	NFS 서버 데몬
nrv	2050/TCP입니다	NetApp 원격 볼륨 프로토콜
iscsi	3260/TCP입니다	iSCSI 타겟 포트입니다
Lockd	4045/TCP 4045/UDP	NFS 잠금 데몬
NFS	4046/TCP입니다	NFS 마운트 프로토콜
acp-proto	4046/UDP입니다	계정 프로토콜
rquotad	4049/UDP입니다	NFS rquotad 프로토콜
krb524	4444/UDP입니다	Kerberos 524
IPsec	4500/UDP입니다	인터넷 프로토콜 보안
acp	5125/UDP 5133/UDP 5144/TCP	디스크용 대체 제어 포트
Mdns	5353/UDP입니다	멀티캐스트 DNS

서비스	포트/프로토콜	설명
HTTPS	5986/UDP입니다	HTTPS 포트: 수신 이진 프로토콜
TELNET	8023/TCP입니다	노드 범위 텔넷
HTTPS	8443/TCP입니다	링크를 통한 7MTT GUI 툴: HTTPS
RSH	8514/TCP입니다	노드 범위 RSH
KMIP	9877/TCP입니다	KMIP 클라이언트 포트(내부 로컬 호스트만 해당)
ndmp	10000/TCP입니다	NDMP
cifs 증인 포트	40001/TCP입니다	CIFS 감시 포트입니다
TLS	50000/TCP입니다	전송 계층 보안
Iscsi	65200/TCP입니다	iSCSI 포트입니다
SSH	65502/TCP입니다	보안 셸
vsun	65503/TCP입니다	vsun

NetApp 내부 포트

포트/프로토콜	설명
900	NetApp 클러스터 RPC
902	NetApp 클러스터 RPC
904	NetApp 클러스터 RPC
905	NetApp 클러스터 RPC
910	NetApp 클러스터 RPC
911	NetApp 클러스터 RPC
913	NetApp 클러스터 RPC
914	NetApp 클러스터 RPC
915	NetApp 클러스터 RPC
918	NetApp 클러스터 RPC
920	NetApp 클러스터 RPC
921	NetApp 클러스터 RPC
924	NetApp 클러스터 RPC
925	NetApp 클러스터 RPC
927	NetApp 클러스터 RPC
928	NetApp 클러스터 RPC
929	NetApp 클러스터 RPC
931	NetApp 클러스터 RPC
932	NetApp 클러스터 RPC

포트/프로토콜	설명
933	NetApp 클러스터 RPC
934	NetApp 클러스터 RPC
935	NetApp 클러스터 RPC
936	NetApp 클러스터 RPC
937	NetApp 클러스터 RPC
939	NetApp 클러스터 RPC
940	NetApp 클러스터 RPC
951	NetApp 클러스터 RPC
954	NetApp 클러스터 RPC
955	NetApp 클러스터 RPC
956	NetApp 클러스터 RPC
958	NetApp 클러스터 RPC
961	NetApp 클러스터 RPC
963	NetApp 클러스터 RPC
964	NetApp 클러스터 RPC
966	NetApp 클러스터 RPC
967	NetApp 클러스터 RPC
7810	NetApp 클러스터 RPC
7811	NetApp 클러스터 RPC
7812	NetApp 클러스터 RPC
7813	NetApp 클러스터 RPC
7814	NetApp 클러스터 RPC
7815	NetApp 클러스터 RPC
7816	NetApp 클러스터 RPC
7817	NetApp 클러스터 RPC
7818	NetApp 클러스터 RPC
7819	NetApp 클러스터 RPC
7820	NetApp 클러스터 RPC
7821	NetApp 클러스터 RPC
7822	NetApp 클러스터 RPC
7823	NetApp 클러스터 RPC
7824	NetApp 클러스터 RPC

스토리지 시스템

AFX

NetApp AFX 개요: NetApp AFX에 대해 알아보세요

NetApp AFX는 여전히 ONTAP입니다. 단지 ONTAP의 이점을 활용하는 다른 방법일 뿐입니다. NetApp AFX는 NAS 및 객체 워크로드를 위한 분산 아키텍처를 제공하는 동시에, 여러분이 알고 사랑하는 풍부한 기능을 갖춘 ONTAP 소프트웨어를 그대로 제공합니다.

혁신의 진화: NetApp ONTAP

NetApp ONTAP는 1992년 여러 클라이언트에 NFS 워크로드를 제공하는 새로운 방식으로 개발되었으며, 성능, 데이터 복원력, 시점 복사 등 여러 측면에서 혁신을 가져왔습니다. 초기에는 NFSv2만 지원했지만, 최신 NFS 버전, 다른 데이터 프로토콜, 강화된 데이터 보호 기능에 대한 수요가 증가함에 따라 NetApp ONTAP는 발전해 왔습니다.

다음은 지난 30여 년 동안 ONTAP에서 발생한 주요 변화들을 간략하게 정리한 타임라인입니다.

NetApp ONTAP의 진화

10년	기능
1990s	NFSv2, NFSv3, CIFS, 스냅샷, WAFL 파일 시스템, AutoSupport, SnapMirror
2000s	SnapVault, SnapLock, NFSv4, 블록 프로토콜, FlexVols, FlexClone, GX/스케일 아웃, 중복 제거, 파일 클론
2010s	클러스터형 ONTAP, 인라인 스토리지 효율성, NFSv4.1/pNFS, NVMe, RAID-TEC, FlexGroup 볼륨, 볼륨 암호화, AFF, Cloud Volumes ONTAP, QoS, FabricPool, Azure NetApp Files (ANF), Google Cloud NetApp Volumes (GCNV), All SAN Array (ASA)
2020s	SnapMirror Business Continuity, FlexCache, ONTAP S3, IPsec, Autonomous Ransomware Protection, ANF 및 GCNV 내외부의 SnapMirror, Amazon FSxN, ASAr2, NetApp AFX가 여기에 있습니다

NetApp ONTAP 특성

수년간 ONTAP는 파일, 블록 및 객체를 단일 시스템으로 결합한 통합 플랫폼으로 운영되었습니다. 이로 인해 ONTAP는 데이터센터의 만능 도구, 즉 사용자가 요청하는 모든 작업을 수행할 수 있는 플랫폼으로 자리매김했습니다.

하지만 애플리케이션이 발전하고 IT 산업의 여러 변화에 따라 데이터센터 요구 사항이 바뀌면서 특정 기능을 수행할 수 있는 플랫폼에 대한 수요가 증가했습니다. 그 결과, 현재 ONTAP을 사용하는 몇 가지 다른 방법이 있습니다.

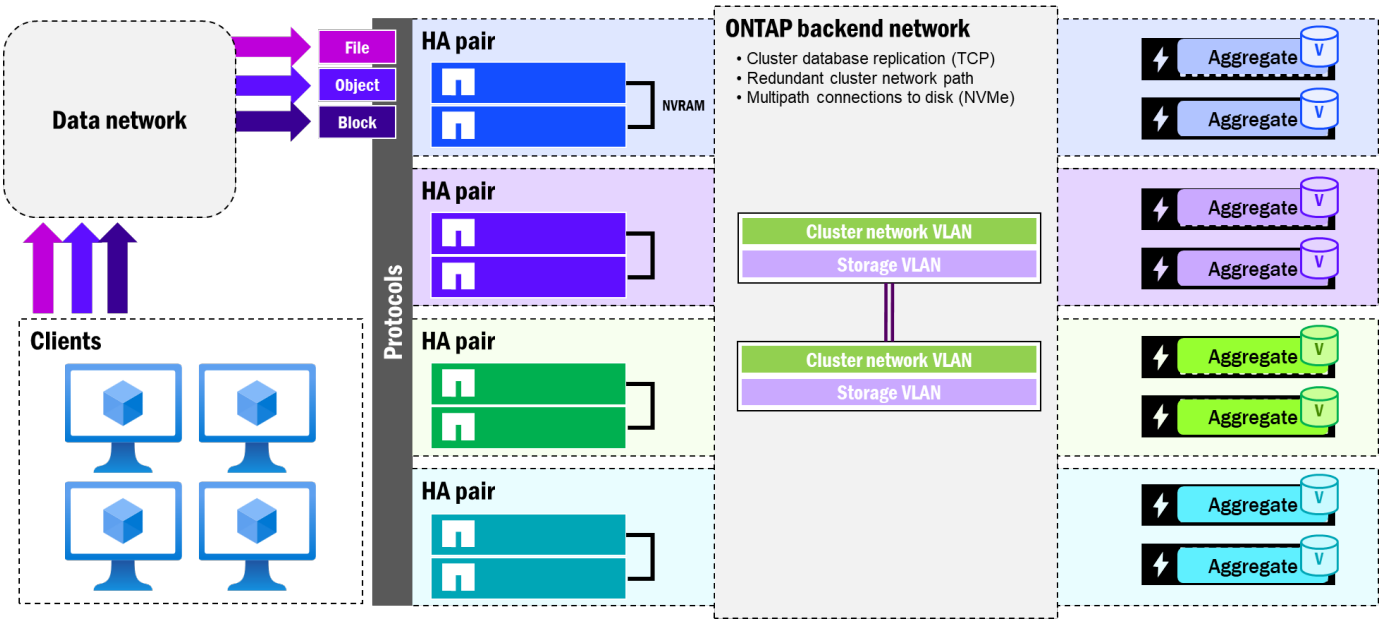
NetApp ONTAP 특성

ONTAP 퍼스낼리티	설명
통합 ONTAP	여러분이 항상 알고 있던 동일한 ONTAP이며, 여전히 활발하게 개발 및 개선되고 있습니다.
모든 SAN 어레이	ONTAP은 iSCSI, FCP 및 FC/TCP를 통한 NVMe만 지원하며 액티브/액티브 컨트롤러 기능과 ASAr2의 분산형 개념을 제공합니다.
클라우드 상주 ONTAP	클라우드에서 실행되는 ONTAP은 클라우드 데이터 센터에 있는 베어 메탈 시스템 또는 가상화된 ONTAP 인스턴스에서 실행됩니다.
분리형 ONTAP/AFX	ONTAP는 고성능 NAS 및 객체 워크로드를 위해 분산형 아키텍처를 사용합니다.

통합 **ONTAP** 아키텍처 개요

다음 다이어그램은 통합 ONTAP의 일반 아키텍처를 보여주며, 그 아래에는 모든 구성 요소가 어떻게 결합되는지에 대한 설명이 있습니다.

일반 **ONTAP** 아키텍처



ONTAP 아키텍처의 주요 측면:

- 파일, 객체 및 블록 지원
- 프로토콜은 프런트엔드 클라이언트 데이터 네트워크를 통해 제공됩니다.
- 여러 개의 독립적인 노드를 함께 클러스터링할 수 있습니다.
- 각 노드는 데이터 및 관리 사용 사례에 대해 독립적인 플로팅 IP 주소를 제공할 수 있습니다
- 클러스터링된 노드는 클러스터 VLAN을 통해 NetApp에서 제공하는 백엔드 스위치에 연결됩니다.
- 노드들은 하드웨어 또는 전력 장애 발생 시 복원력을 제공하기 위해 고가용성(HA) 쌍으로 구성됩니다.
- HA 쌍은 쓰기를 보호하기 위해 복제하는 NVRAM 카드가 직접 연결되어 있습니다

- 각 노드에는 최소 하나 이상의 애그리게이트가 할당되며 전체 디스크 수의 일부를 소유합니다.
- 페일오버 시 노드의 디스크는 HA 파트너(HA 파트너에게만)에게 재할당됩니다.
- 디스크 셸프는 일반적으로 다중 경로 케이블을 통해 노드에 직접 연결되지만, 고급 시스템에서는 동일한 백엔드 클러스터 스위치에 스토리지 네트워크 개념이 도입되었습니다.
- 볼륨(FlexVols 및 FlexGroup 볼륨)은 데이터 액세스를 위한 스토리지의 진입점을 제공합니다

NetApp AFX란 무엇인가요**?**

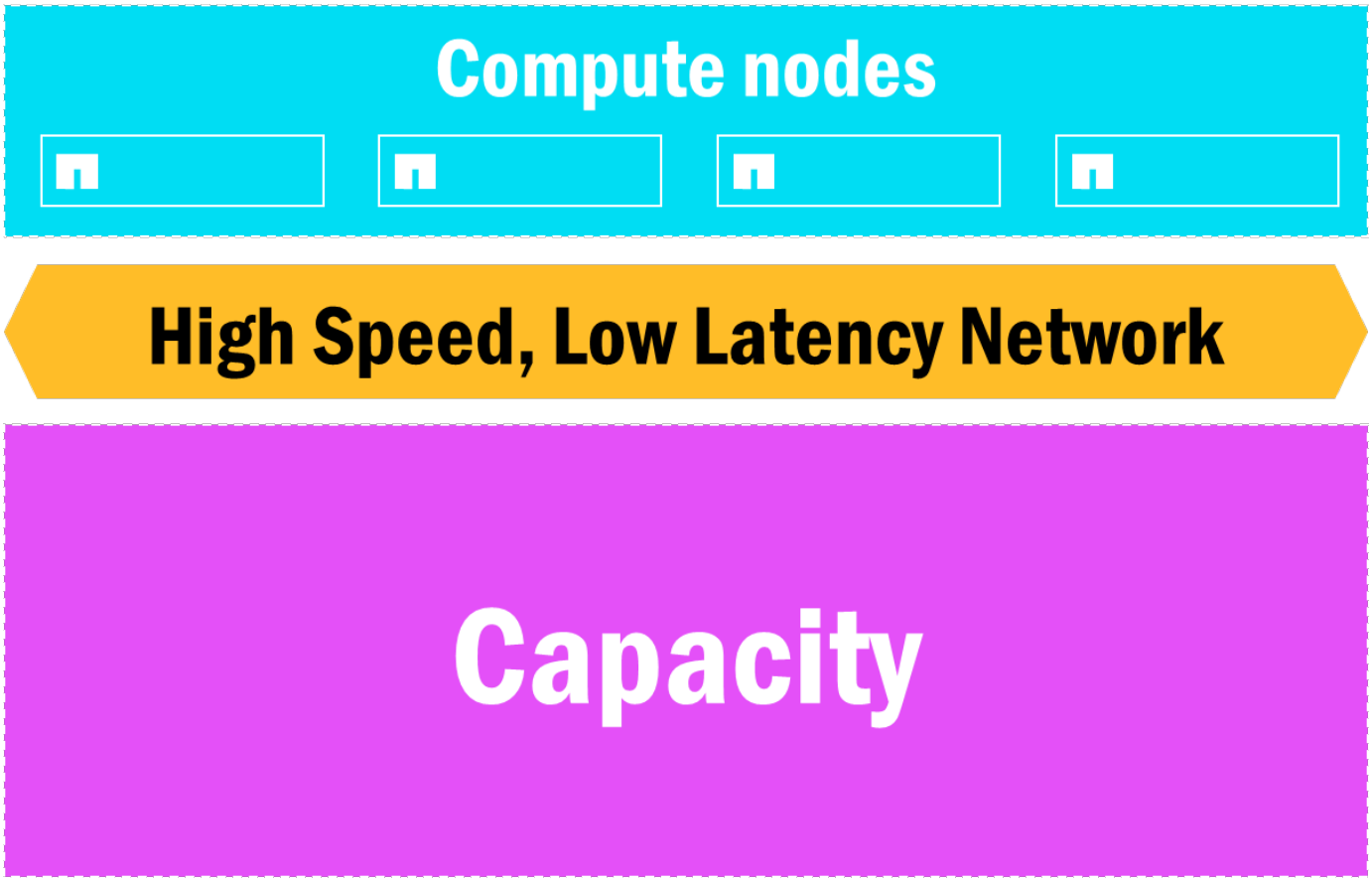
여기서 한 가지 명심해야 할 점은 NetApp AFX가 여전히 ONTAP라는 것입니다.

이는 ONTAP의 이점을 활용하는 또 다른 방법일 뿐입니다. Unified ONTAP 또는 All SAN Array 시스템에 설치하는 이미지와 동일한 이미지가 NetApp AFX에서도 사용됩니다. 코드베이스는 동일하지만, 시스템 부팅 방식에 따라 실행되는 코드 경로, 백엔드 스토리지의 표현 방식, 지원되는 기능 및 프로토콜이 결정됩니다.

NetApp AFX는 NAS 및 객체 워크로드를 위한 분산형 아키텍처를 제공하는 동시에, 익숙하고 사랑받는 풍부한 기능을 갖춘 ONTAP 소프트웨어를 그대로 제공합니다. 분산형 ONTAP는 모든 NetApp 컨트롤러 노드가 이중화된 네트워크 스위치와 고속 저지연 네트워크를 통해 동일한 용량을 사용하는 스토리지 아키텍처를 의미합니다. 이러한 접근 방식을 통해 컨트롤러 노드와 스토리지 용량이 서로 독립적으로 확장하여 다양한 고성능 워크로드의 요구 사항을 더욱 효과적으로 충족할 수 있습니다. 즉, 추가 성능이 필요하면 컨트롤러 노드를 추가하면 됩니다. 추가 용량이 필요하면 쉘프 인클로저를 추가하면 됩니다. 이를 통해 스토리지 관리자는 최종 사용자에게 더욱 비용 효율적인 스토리지 솔루션을 제공할 수 있는 유연성을 확보할 수 있습니다.

컨트롤러 노드가 디스크를 독립적으로 소유하지 않기 때문에 자체 용량 및 성능 제약 조건을 가진 물리적 애그리게이트도 존재하지 않습니다. 대신 용량은 모든 노드가 상호 작용할 수 있는 공유 모델로 제공되며 ONTAP가 자동으로 관리할 수 있습니다.

분리형 **ONTAP**



주요 용어 및 개념

아래는 AFX와 직접적으로 관련된 용어입니다. ONTAP 관련 용어는 제품 설명서를 참조하십시오.

"ONTAP 제품 설명서".

분산형 **ONTAP**

ONTAP를 기반으로 하는 새로운 아키텍처를 의미하며, 컴퓨팅과 용량을 서로 독립적으로 확장할 수 있는 기능을 제공합니다. "분리형 ONTAP"이라는 용어는 제품명이 아니라 통합 ONTAP와 NetApp AFX 아키텍처를 구분하기 위한 용어입니다.

NetApp AFX

NetApp AFX는 분산형 ONTAP 아키텍처의 공식 제품명이며 NetApp Insight 2025에서 발표되었습니다.

컴퓨팅 노드

NetApp AFX에서 컴퓨팅 노드는 스토리지 컨트롤러 노드를 의미하며, 문서에서는 종종 같은 의미로 사용됩니다. 이러한 노드에는 온보드 디스크가 없으며, 분산형 ONTAP 아키텍처가 제공하는 독립적인 확장성을 지원하기 위해 완전한 모듈형으로 설계되었습니다.

스토리지 가용 영역

스토리지 가용 영역(SAZ)은 NetApp AFX 클러스터에서 모든 디스크가 모든 노드에서 공유되는 단일 용량 풀입니다. SAZ를 통해 공유 용량, 향상된 성능, 전역 데이터 중복 제거 등의 기능을 활용할 수 있습니다.

NetApp AFX의 새로운 기능

이 섹션에서는 NetApp AFX의 최신 업데이트 정보를 제공하며, 새로운 릴리스가 출시될 때마다 업데이트될 예정입니다. 새로운 정보를 확인하려면 정기적으로 이 페이지를 방문해 주시고, 버전 릴리스 노트도 참조하시기 바랍니다.

NetApp ONTAP for AFX 최신 릴리스의 새로운 기능은 무엇입니까**?**

최신 릴리스:

ONTAP 9.19.1RC1(2026년 5월 기준)

NetApp AFX의 새로운 기능:

- 전역 중복 제거
- 동적 스토리지 효율성
- 고급 미리 읽기
- 32개 노드 지원
- 32PB 지원
- FlexGroup 볼륨당 512개의 구성 볼륨

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2026년 6월	초기 릴리스

NetApp AFX 아키텍처와 통합 ONTAP의 차이점

NetApp AFX는 스토리지 표현 방식, 노드가 디스크와 상호 작용하는 방식, 용량 관리 방식 등에서 통합 ONTAP과 상당한 아키텍처적 차이점을 보여줍니다.

앞서 우리는 통합 ONTAP 아키텍처가 자체 디스크 세트를 소유하고 디스크 집합을 통해 물리적 용량을 제공하는 직접 연결된 HA 쌍을 통해 파일, 객체 및 블록 데이터 스토리지를 제공하는 방식에 대한 일반적인 개요를 살펴보았습니다. 이 섹션에서는 통합 ONTAP과 NetApp AFX 아키텍처 간의 주요 차이점을 더 자세히 살펴보겠습니다.

시스템이 **NetApp AFX**를 실행 중인지 확인하는 방법

시스템에 NetApp AFX가 실행 중인지 확인하는 가장 일반적인 방법은 다음 명령을 실행하는 것입니다.

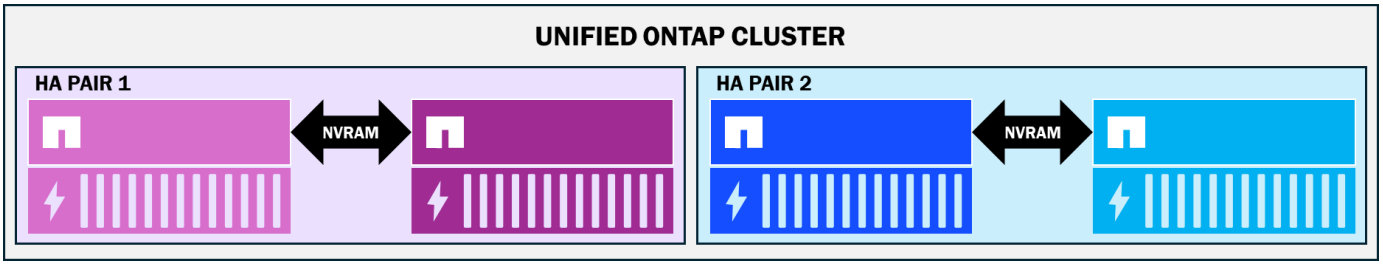
```
AFX::> node show -fields personality
node             personality
---------------- -----------
afx-01           AFX
afx-02           AFX
```

또 다른 단서는 새로운 Storage Availability Zone이지만, 이는 NetApp All-SAN Arrays(ASA)에서도 사용할 수 있는 개념입니다. 해당 명령을 통해 용량을 확인할 수 있습니다.

```
AFX::> storage availability-zone show
                     Availability Zone Name: storage_availability_zone_0
                     Availability Zone UUID: 545cb59f-32e9-11f1-a2f5-
d039eabdd925
                                 Total Size: 69.59TB
                              Physical Used: 837.1GB
                       Physical Used Percent: 1%
                                  Available: 68.77TB
                              Metadata Used: 837.1GB
                  Log and Recovery Metadata: 834.6GB
                              Delayed Frees: 2.50GB
 Physical User Data Without Snapshot Copies: 17.24MB
  Logical User Data Without Snapshot Copies: 17.24MB
   Efficiency Ratio Without Snapshot Copies: 1.00:1
               Space Full Threshold Percent: 98%
        Space Nearly Full Threshold Percent: 95%
```

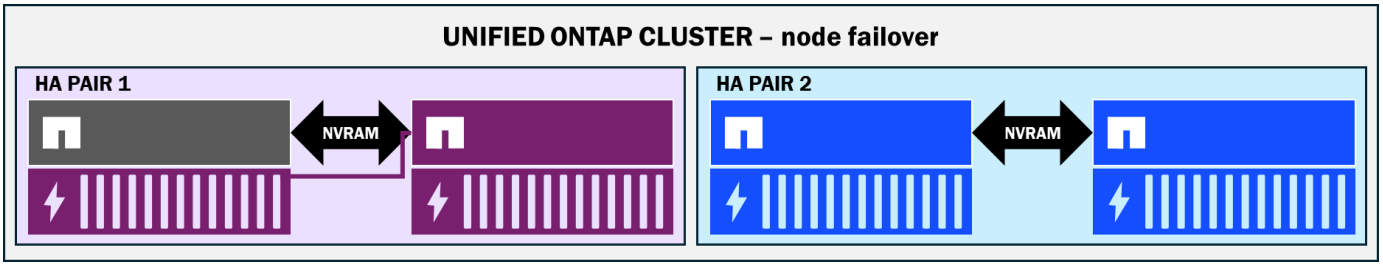
노드-디스크 관계

통합 ONTAP 아키텍처에서는 읽기 및 쓰기 작업이 특정 디스크 하위 집합으로 전달됩니다. 따라서 24개 노드로 구성된 클러스터에 24개의 디스크 셸프(노드당 하나의 셸프)가 있더라도, 각 노드는 특정 시점에 하나의 디스크 셸프에만 직접 액세스할 수 있으므로 클러스터에서 사용 가능한 용량과 성능이 제한됩니다.



또한 NVRAM이 HA 쌍 간에 직접 연결되어 있으므로 노드는 물리적으로 서로 인접해야 하며 장애 조치 대상으로서 더욱 긴밀하게 연결되어야 합니다. 예를 들어 한 노드가 파트너 노드로 장애 조치를 수행할 때 해당 노드가 물리적으로 접근할 수 있는 디스크는 HA 쌍 도메인에 있는 디스크뿐입니다.

HA 페일오버 중 통합 **ONTAP** 클러스터

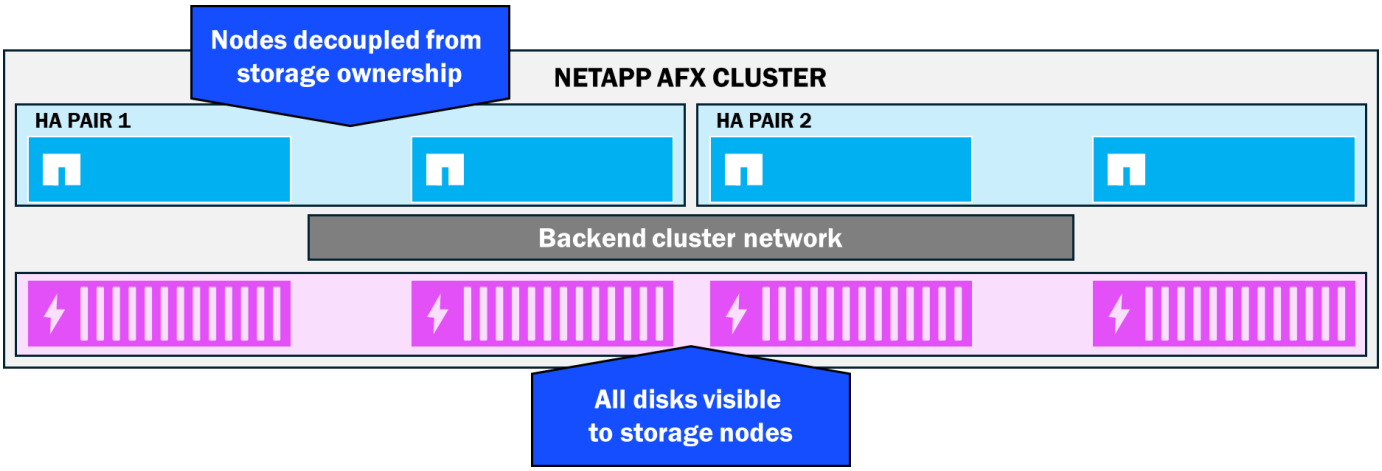


NetApp AFX에서는 컴퓨팅 노드에 디스크를 제공하는 방식에 몇 가지 주요 변경 사항이 있습니다.

모든 디스크는 모든 스토리지 노드에서 볼 수 있으며 디스크 소유권은 없습니다

NetApp AFX에서는 노드와 쉘프가 모두 동일한 백엔드 스위치에 연결되어 있어 ONTAP이 디스크에 대한 전체 가시성 도메인을 전체 스택으로 확장할 수 있습니다. 결과적으로 어떤 노드도 특정 디스크를 소유하지 않습니다. 대신 모든 디스크는 Storage Availability Zone이라는 단일 용량 풀에 참여하므로 용량 관리가 간소화되고 성능 잠재력이 향상됩니다(사용 가능한 디스크가 많을수록 사용 가능한 성능이 향상됨).

NetApp AFX 스토리지 가용 영역

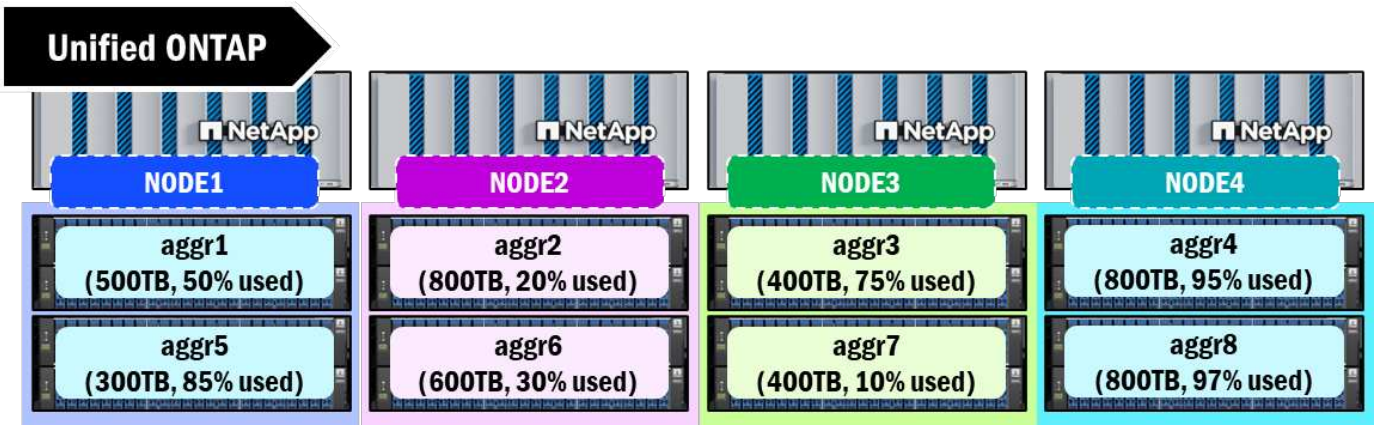


더 이상 물리적 애그리게이트가 없습니다

Unified ONTAP은 디스크를 RAID 그룹으로 모은 다음, 이를 애그리게이트라고 하는 용량 구조로 결합합니다. 이 애그리게이트는 스토리지에 물리적 용량을 제공하는 방식이며, 최종 사용자에게 데이터를 제공하기 위한 볼륨 생성에 사용 가능한 공간의 경계를 나타냅니다. 모든 노드에는 최소 하나 이상의 애그리게이트가 할당되어야 하며, 각 애그리게이트의 현재 용량 제한은 800TB입니다. 이 제한에 도달하면 더 이상 추가 쓰기 작업을 위한 공간이 없습니다.

물리적 애그리게이트는 용량 관리 어려움을 야기할 수 있습니다. 스토리지 관리자는 클러스터 노드 간 용량 균형을 유지하기 위해 볼륨을 수동으로 재배치해야 하는 경우가 있기 때문입니다. 이러한 어려움은 스케일아웃 볼륨 아키텍처(예: FlexGroup 볼륨)를 활용할 때 더욱 커질 수 있습니다. 또한 애그리게이트는 크기, 디스크 개수, 디스크 유형 등이 다양할 수 있으며, 이로 인해 노드 간 이동 시 성능 차이가 발생할 수 있습니다.

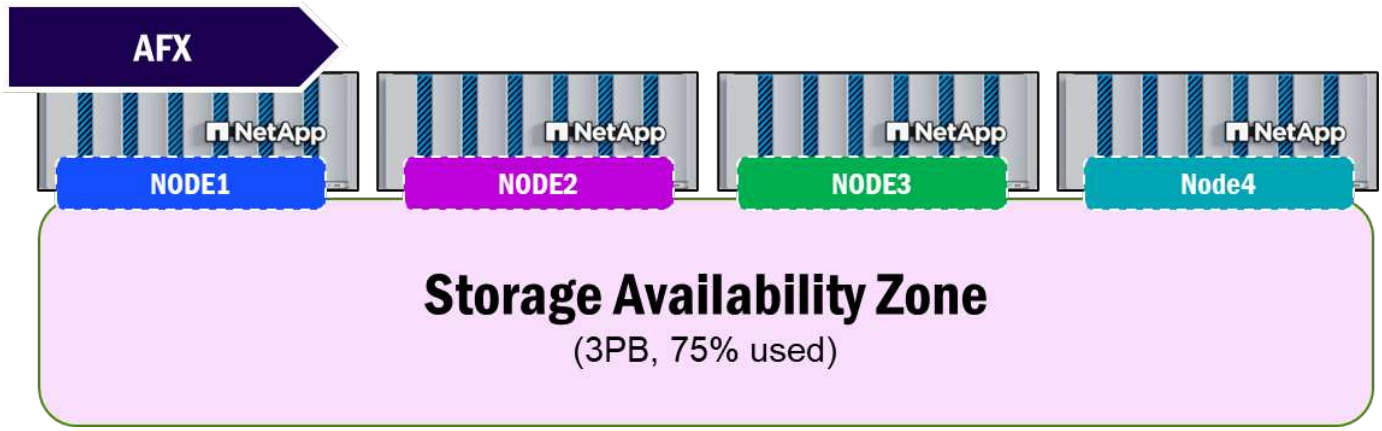
통합 **ONTAP**의 애그리게이트



NetApp AFX는 물리적 애그리게이트 개념을 가상화하고 ONTAP에서 관리하도록 하며, 새로운 스토리지 가용 영역을

통해 물리적 용량 관리를 노드 단위 방식에서 클러스터 단위로 전환합니다. 이 단일 용량 풀은 공간 관리에 대한 "보는 대로 얻는" 접근 방식을 제공합니다.

NetApp AFX 스토리지 가용 영역



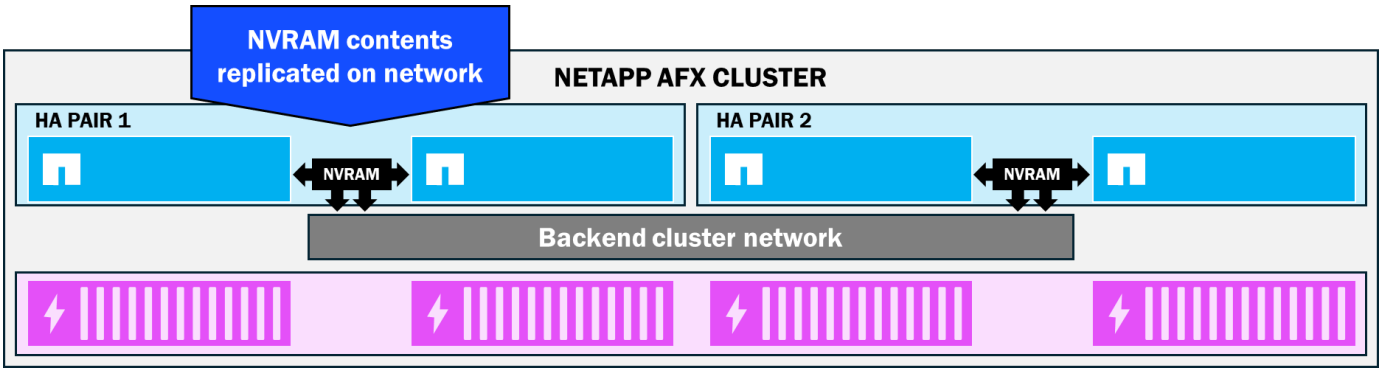
NVRAM이 직접 연결에서 스위치드 복제로 이동했습니다

ONTAP는 클러스터로 들어오는 쓰기 작업을 보호하기 위해 NVRAM을 임시 저장소로 사용합니다. ONTAP 클러스터의 각 노드에는 배터리로 백업되는 NVRAM 카드가 있습니다. 클라이언트에서 볼륨으로 쓰기 작업이 전송되면 먼저 NVRAM에 저장됩니다. NVRAM이 가득 차거나 10초 타이머가 만료되면(둘 중 먼저 발생하는 경우) NVRAM 내용이 디스크에 기록됩니다. 이를 정합성 보장 지점이라고 합니다.

NVRAM 콘텐츠는 HA 쌍 간에 지속적으로 복제되므로 데이터 정합성을 더욱 효과적으로 보호할 수 있습니다. 노드 장애가 발생하더라도 NVRAM 콘텐츠는 정상 노드에 보존되어 디스크에 커밋되기 때문입니다.

통합 ONTAP 클러스터에서 HA 쌍 간의 NVRAM 카드는 서로 직접 연결됩니다. NetApp AFX는 NVRAM 복제를 백엔드 클러스터 네트워크로 이동합니다. 결과적으로 HA 파트너 노드는 노드 간 엄격한 거리 제한을 받지 않습니다. 대신 HA 쌍은 이더넷 최대 거리까지 떨어져 있을 수 있습니다.

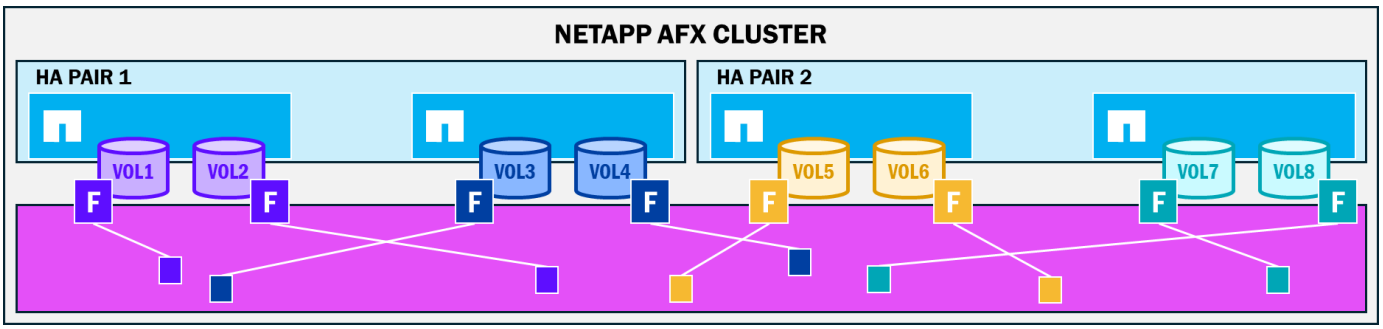
NetApp AFX NVRAM 복제



가용 영역 내의 모든 디스크에 기록된 데이터

NetApp AFX는 디스크 소유권 개념을 없애고 물리적 애그리게이트 구조를 ONTAP에서 관리하는 가상화된 접근 방식으로 전환하여, 클러스터에 구매한 용량을 클러스터에 연결된 모든 노드에서 사용할 수 있도록 합니다. AFX를 사용하면 노드:볼륨 소유권과 관계없이 모든 노드가 Storage Availability Zone의 모든 디스크에 쓰기 작업을 수행할 수 있습니다. 쓰기 작업은 여전히 NVRAM을 통한 경로를 거치므로 노드에는 여전히 볼륨 소유권 개념이 있지만, 해당 데이터는 사용 가능한 용량 내 어디에든 저장될 수 있습니다. 즉, 더 많은 디스크가 단일 워크로드에 참여할 수 있어 성능 향상 효과를 얻을 수 있습니다.

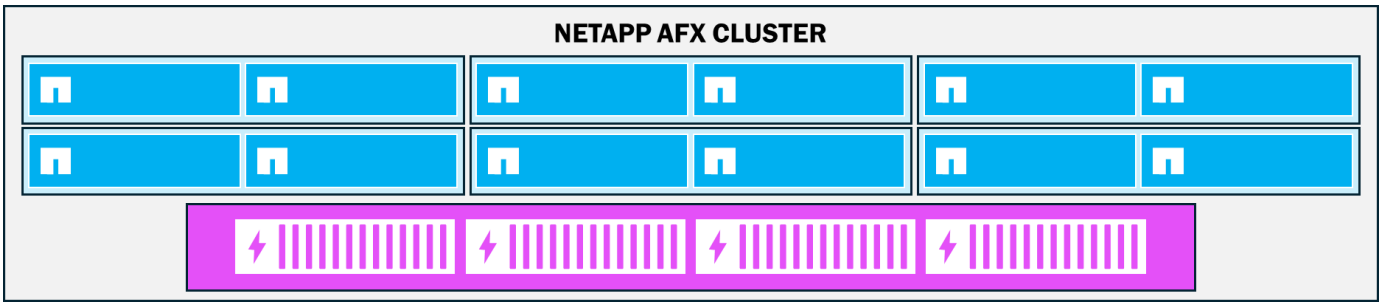
데이터가 **Storage Availability Zone**에 저장되는 방식



용량 및 컴퓨팅 노드의 독립적인 확장

NetApp AFX 아키텍처에서는 하드웨어 리소스가 분리되어 있어 노드를 추가할 때 더 이상 연결된 디스크를 함께 추가할 필요가 없습니다. 클러스터에서 RAM, CPU 또는 네트워크 처리량과 같은 성능 관련 리소스가 부족할 경우 스토리지 노드만 클러스터에 추가하면 기존 스토리지 가용 영역을 활용할 수 있습니다. 반대로 용량이 필요한 경우에는 쉘프만 추가하면 됩니다. 이러한 유연성을 통해 필요한 리소스만 구매하여 과잉 프로비저닝을 방지할 수 있습니다.

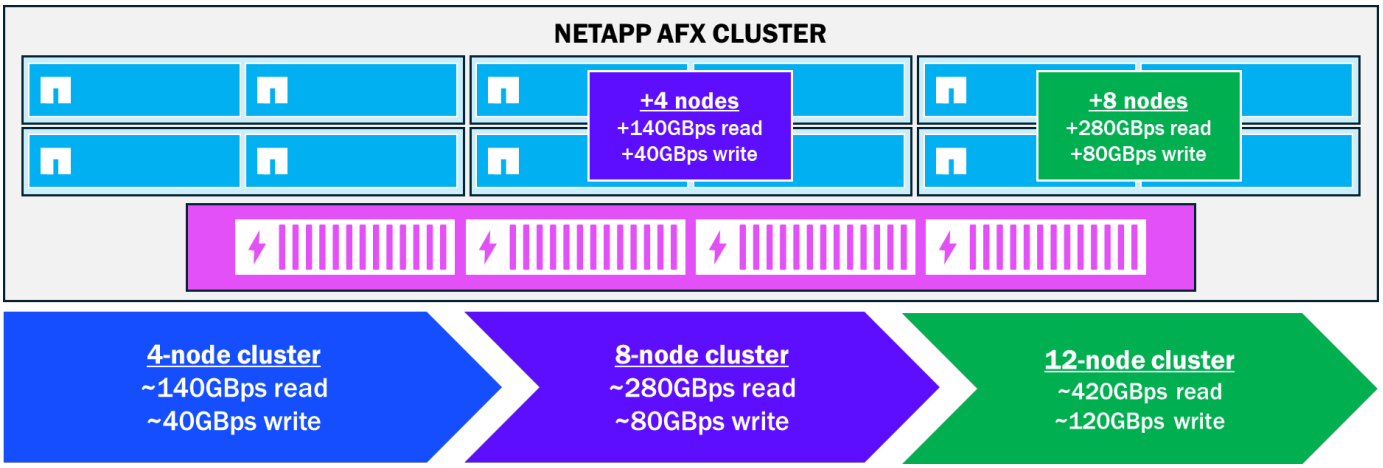
NetApp AFX – 독립적인 확장



노드 성능의 선형 확장

AFX 클러스터에 노드가 추가됨에 따라 워크로드에 더 많은 CPU, RAM 및 네트워크 리소스가 제공됩니다. 이러한 리소스가 환경에 통합됨에 따라 성능 향상은 선형적으로 나타납니다. 아래 그림은 노드가 추가됨에 따라 성능이 어떻게 향상되는지 보여줍니다.

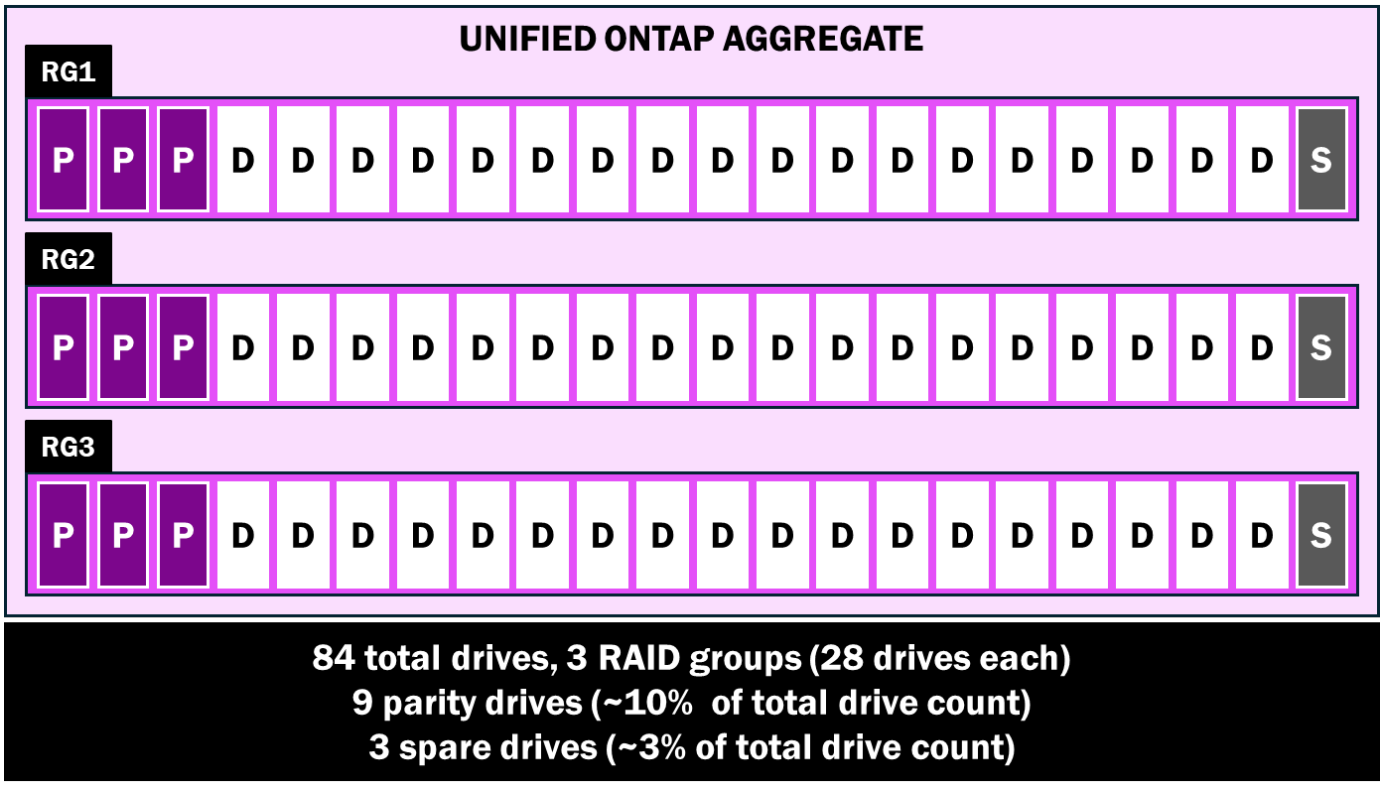
NetApp AFX 노드를 추가할수록 성능이 선형적으로 향상됩니다**.**



더 큰 **RAID** 그룹**,** 더 적은 패리티 드라이브

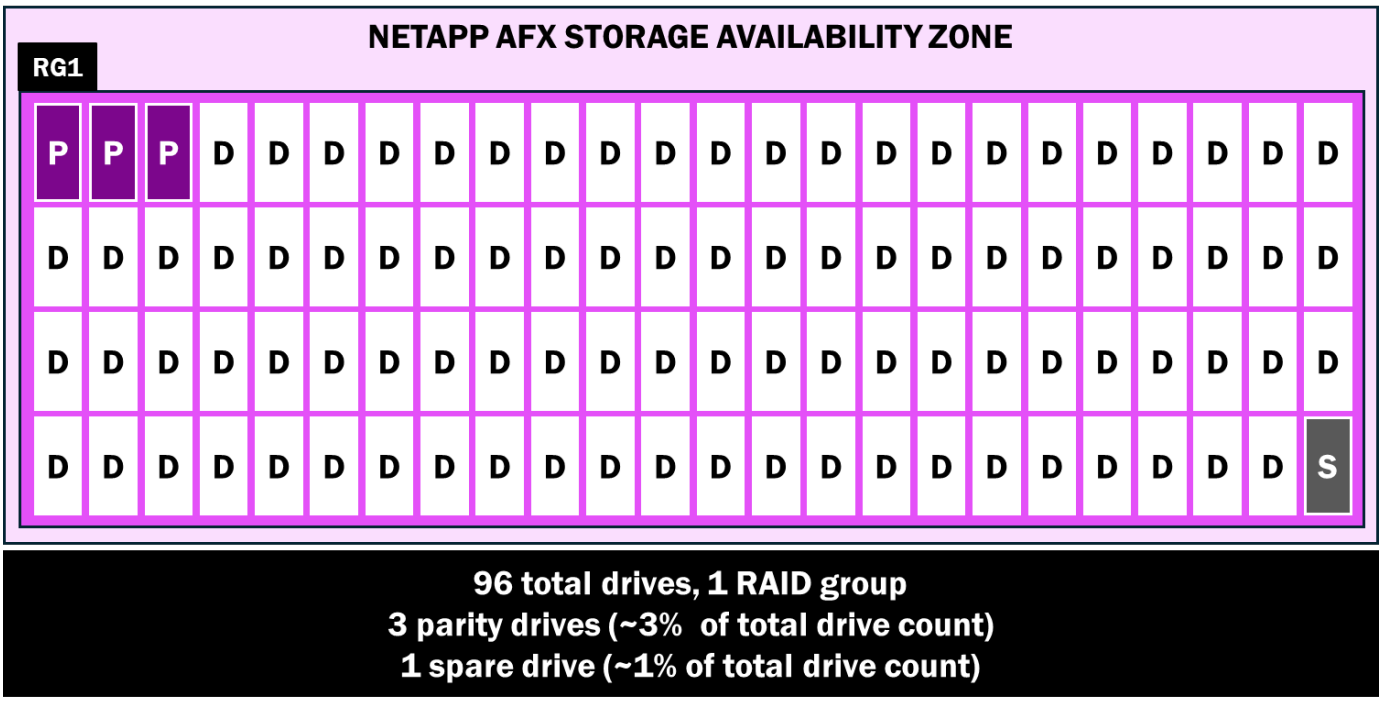
ONTAP는 RAID 그룹, 특히 디스크 장애 발생 시 3중 패리티 보호 기능을 제공하는 RAID-TEC을 통해 디스크의 데이터 보호와 성능을 결합한 솔루션을 제공합니다. RAID-TEC은 RAID 그룹에서 최대 3개의 동시 드라이브 장애를 견딜 수 있습니다. 통합 ONTAP에서 RAID 그룹은 최대 28개의 디스크를 지원하며, 이 중 3개는 패리티에 사용되고 1개는 예비 드라이브로 예약됩니다. 결과적으로 28개 드라이브 중 24개가 데이터 처리/RAID 스트라이프에 사용됩니다.

통합 **ONTAP RAID** 그룹



NetApp AFX는 여전히 RAID-TEC를 활용하지만, RAID 그룹 크기를 96개 드라이브로 늘리는 동시에 패리티 드라이브 3개와 예비 드라이브 1개만 필요로 합니다. 더 큰 RAID 그룹은 전반적인 성능을 향상시키며, SSD의 낮은 고장률, 더 많은 드라이브에 걸쳐 작업이 더욱 균등하게 분산되는 점, 그리고 NetApp AFX의 패리티에서 데이터 드라이브 재구축 기능 개선을 통해 드라이브 장애 노출을 최소화합니다.

NetApp AFX Storage Availability Zone RAID 그룹



다음 표는 드라이브 크기가 다양한 통합 ONTAP 및 NetApp AFX 시스템의 84개 디스크에 대해 사용 가능한 원시 용량을 대략적으로 나타낸 것입니다.

대략적인 원시 용량 비교, 드라이브 **84**개 기준 **– Unified ONTAP** 및 **NetApp AFX**

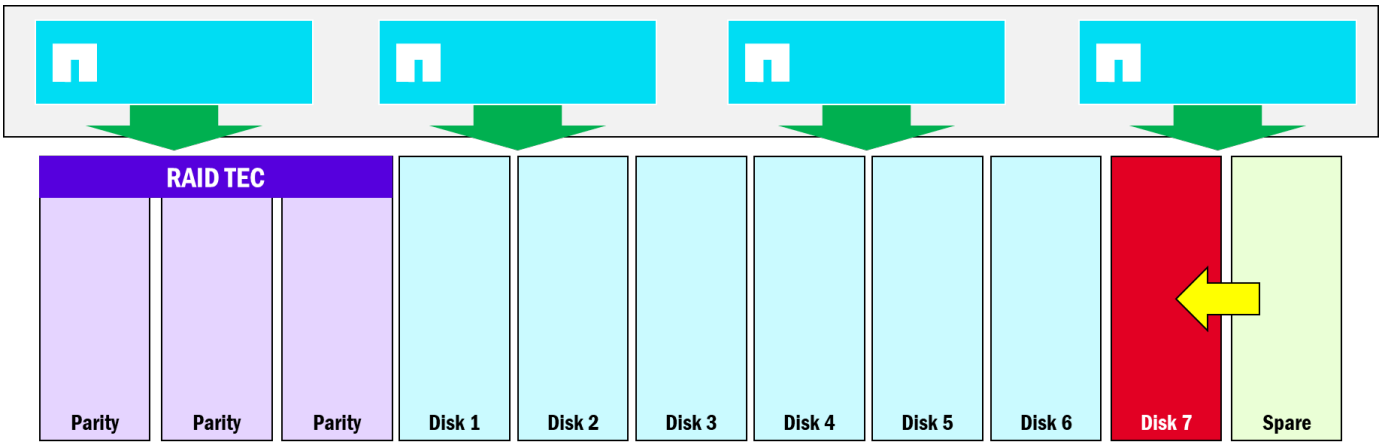
드라이브 크기	대략적인 원시 용량(통합)	대략적인 원시 용량**(AFX)**
7.6 TB	~547.2TB	~608TB (+60.8TB)
15.3 TB	~1101.6TB	~1224TB (+122.4TB)
30.6 TB	~2203.2TB	~2448TB (+244.7TB)
60.1 TB	~4327.2TB	~4808TB (+480.8TB)

디스크 장애 재구축 시간 단축

통합 ONTAP에서 각 노드는 스토리지 스택의 디스크 하위 집합을 소유합니다. 즉, 해당 노드는 소유한 디스크에만 쓰기 작업을 수행할 뿐만 아니라 디스크 장애 발생 시 디스크 재구축은 단일 노드에서만 처리됩니다.

NetApp AFX는 디스크 소유권이 필요하지 않습니다. 따라서 필요한 경우 단일 노드에서 모든 드라이브에 쓰기 작업을 수행할 수 있습니다. 또한 드라이브를 패리티 기반으로 재구축해야 할 경우 클러스터의 모든 노드가 참여하므로 단일 노드에서만 재구축해야 하는 경우보다 훨씬 빠르게 드라이브를 재구축할 수 있습니다.

NetApp AFX에서의 디스크 재구축

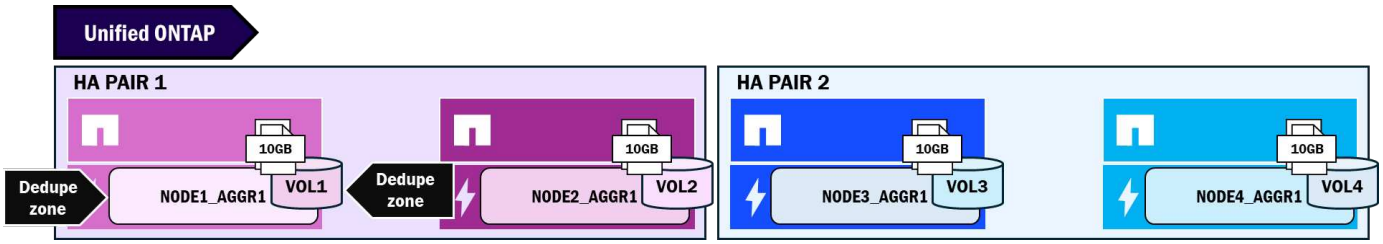


중복 제거 도메인

중복 제거는 스토리지 시스템이 파일 시스템에서 중복 블록을 찾아 단일 블록에 대한 포인터를 생성하여 사용된 총 용량을 줄일 수 있도록 합니다. 통합 ONTAP에서 중복 제거는 축소할 수 있는 블록에 대한 특정 경계를 따릅니다. 이러한 경계는 사용 중인 중복 제거 유형에 따라 달라집니다. 일반적으로:

- 볼륨 기반 중복 제거 → 볼륨 경계
- 볼륨 간 중복 제거 → 애그리게이트 경계

통합 **ONTAP** 중복 제거 도메인



아래 표는 통합 ONTAP의 다양한 시나리오에서 중복 데이터에 대한 용량 동작을 보여줍니다. 파일 복사본이 노드와 애그리게이트(따라서 중복 제거 도메인)에 걸쳐 있을 경우 공간 절약 효과가 감소합니다.

동일한 **10GB** 파일에 대한 다양한 시나리오에서의 중복제거 동작 **–** 통합 **ONTAP**

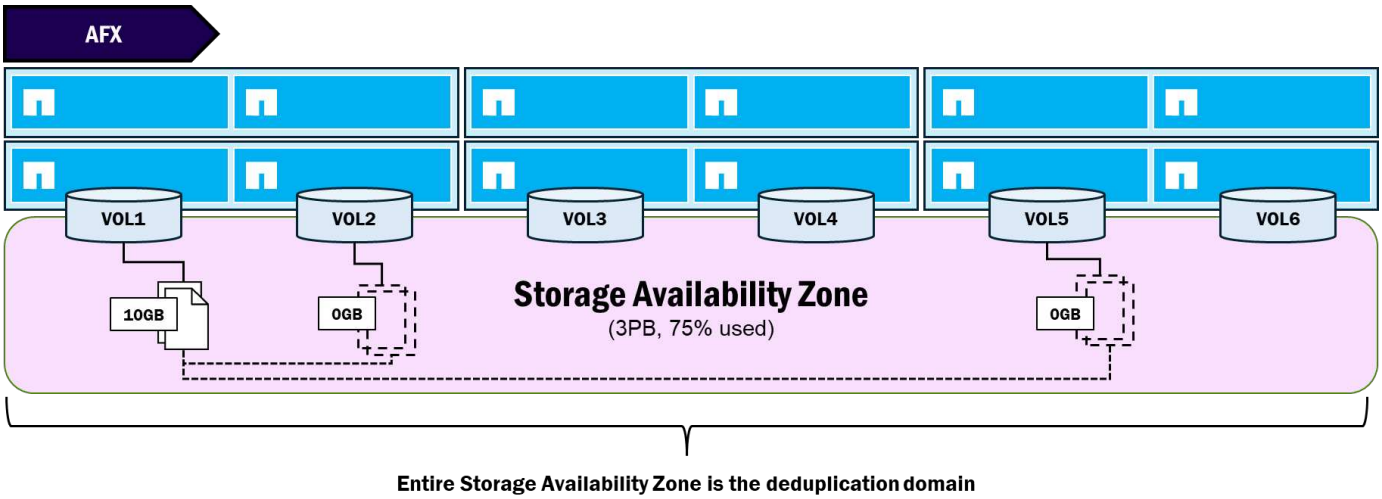
시나리오	사용된 공간
동일한 10GB 파일의 복사본 4개, 동일한 볼륨(볼륨 중복 제거)	10 GB
동일한 10GB 파일의 복사본 4개, 서로 다른 볼륨, 동일한 애그리게이트(볼륨 간 중복 제거 활성화됨)	10 GB
동일한 10GB 파일의 복사본 4개, 서로 다른 볼륨 4개, 서로 다른 애그리게이트 4개(볼륨 간 중복 제거 활성화됨)	40 GB

NetApp AFX는 물리적 애그리게이트를 제거하고 용량 관리를 새로운 스토리지 가용 영역으로 이동함에 따라 중복 제거 도메인 경계도 변경됩니다. AFX에서 중복 제거 도메인은 9.19.1 이전 버전에서는 볼륨 수준(unified ONTAP과 유사)이고 노드 수준(애그리게이트가 아닌)입니다.

ONTAP 9.19.1부터 AFX는 스토리지 가용 영역 수준에서 전역 중복 제거 도메인을 지원하므로 클러스터 스토리지 풀의

모든 중복 블록이 동일하게 처리됩니다.

NetApp AFX – 글로벌 중복제거 도메인**(ONTAP 9.19.1)**



아래 표는 NetApp AFX에서 다양한 시나리오에 따른 중복 데이터의 용량 동작을 보여줍니다.

동일한 **10GB** 파일에 대한 다양한 시나리오에서의 중복 제거 동작 **– NetApp AFX**

시나리오	사용된 공간
동일한 10GB 파일의 복사본 4개, 동일한 볼륨(볼륨 중복 제거)	10GB (9.18.1) 10GB (9.19.1)
동일한 10GB 파일의 복사본 4개, 서로 다른 볼륨, 동일한 노드(볼륨 간 중복 제거 활성화됨)	10GB (9.18.1) 10GB (9.19.1)
동일한 10GB 파일의 복사본 4개, 서로 다른 볼륨 4개, 서로 다른 노드 4개(볼륨 간 중복제거 활성화됨)	40GB (9.18.1) 10GB (9.19.1)

제거되었거나 더 이상 지원되지 않는 기능

NetApp AFX는 고성능 NAS 및 객체 워크로드, 특히 AI 학습 및 추론 분야에 최적화되어 있습니다(단, 이에 국한되지는 않습니다). NetApp AFX를 설계하면서 ONTAP의 일부 기능을 비활성화하기로 결정했습니다.

- 고성능 NAS 및 객체에 중점을 두기 때문에 블록 워크로드가 NetApp AFX 솔루션에서 제거되었습니다. FCP, iSCSI 또는 NVMe 데이터 프로토콜은 지원되지 않으며 블록 프로토콜을 추가할 계획도 없습니다.
- 분산(Disaggregated)은 분리(de-aggregated)와 동의어로, (적어도 물리적 스토리지 관리 개념으로서의) 애그리게이트가 제거되었음을 의미합니다. 물리적 애그리게이트를 제거하면 ONTAP에서 용량 관리가 간소화될 뿐만 아니라 단일 용량 풀을 구성할 수 있는 메커니즘이 제공됩니다.
- 애그리게이트가 제거됨에 따라 애그리게이트 관련 기능도 함께 제거됩니다. 예를 들어 Metrocluster는 사이트 장애 조치 기능을 위해 애그리게이트 수준 미러링을 활용합니다. 따라서 Metrocluster도 NetApp AFX에서 제거됩니다. 사이트 장애 조치 기능은 ONTAP 9.19.1GA에 포함된 새로운 SnapMirror Active-Sync for NAS 기능을 통해 제공됩니다.
- FabricPool이라는 콜드 데이터 계층화 기능은 애그리게이트별로 제공되므로 현재 NetApp AFX에서는 사용할 수 없습니다.
- NetApp AFX에서는 새로운 용량 아키텍처 덕분에 복사 기반 볼륨 이동이 더 이상 필요하지 않습니다. 자세한 내용은 제로 카피 볼륨 이동를 참조하십시오.

- 기능 제거는 CLI/GUI/REST API 변경을 의미하기도 하므로, 더 이상 지원되지 않는 기능에 대한 모든 명령이나 API 호출도 제거됩니다.
- ZAPI는 현재 NetApp AFX에서 사용할 수 없습니다.
- 가상화를 위한 NFS 복사 오프로드(FlexGroup 볼륨의 세분화된 데이터 분산 기능만 해당)

ONTAP 관리 변경 사항

일반적으로 NetApp AFX 관리는 클러스터 관리에 사용되는 메커니즘을 변경하지 않습니다. 관리자는 여전히 CLI, GUI 및 REST API를 활용하여 클러스터에 로그인하고 구성할 수 있습니다. 하지만 NetApp AFX는 스토리지 관리 작업 방식을 개선할 수 있는 기회를 제공했습니다.

더욱 간편해진 용량 관리

NetApp AFX 스토리지 가용 영역은 노드 및 애그리게이트 기반 접근 방식에서 클러스터 전체에서 사용할 수 있는 단일 용량 풀로 관리 엔드포인트를 줄여줍니다. 볼륨 크기가 증가하거나 감소함에 따라 ONTAP는 스토리지 가용 영역에서 용량을 자동으로 빌리고 반환합니다.

이러한 이유로 스토리지 관리자는 더 이상 최대 24개 노드와 수백 개의 애그리게이트에 걸쳐 사용 가능한 여유 공간을 찾고 관리하는 데 신경 쓸 필요가 없습니다. 이제 용량을 관리하고 확인하는 곳은 단 한 곳뿐입니다.

예를 들어, 통합 ONTAP의 CLI에서 클러스터의 전체 물리적 용량 정보를 보려면 "`aggregate show-space`"를 사용하면 모든 애그리게이트 항목이 출력됩니다. NetApp AFX에서는 "`cluster space show`"를 사용하면 단일 스토리지 가용 영역만 표시됩니다.

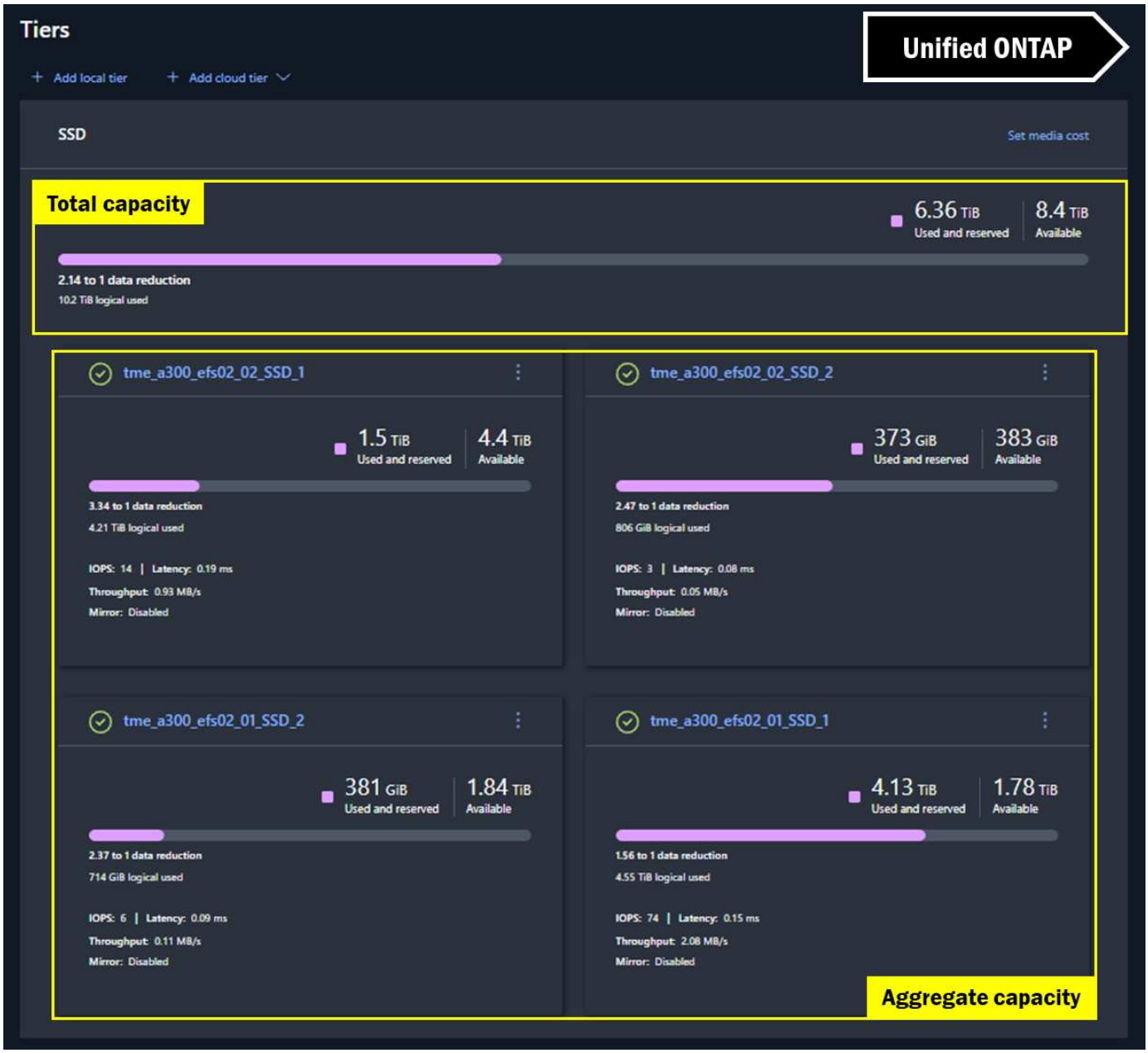
통합 **ONTAP**과 **NetApp AFX**에서 용량 관련 **CLI** 명령어를 나란히 비교

```
unified::> aggr show-space                    Unified ONTAP

Aggregate : aggr1

Feature                          Used        Used%
-------------------------------- ----------  ------
Volume Footprints                250.2TB        50%
Aggregate Metadata               31.06MB         0%
Snapshot Reserve                 8.41GB          5%
Total Used                       1.2TB          95%

Total Physical Used              225.2TB        50%

Total Provisioned Space          450.2TB        90%

.....

8 entries were displayed.
```

```
AFX::> cluster space show                     AFX

 Availability Zone Name: storage

                                  Total Size: 3PB
                               Physical Used: 2PB
                        Physical Used Percent: 75%
                                    Available: 1PB
                                Metadata Used: 1.71TB
                    Log and Recovery Metadata: 1.71TB
                                Delayed Frees: 1.22GB
  Physical User Data Without Snapshot Copies: 3.33MB
   Logical User Data Without Snapshot Copies: 3.33MB
    Efficiency Ratio Without Snapshot Copies: 1.00:1
                  Space Full Threshold Percent: 98%
         Space Nearly Full Threshold Percent: 95%

1 entry was displayed.
```

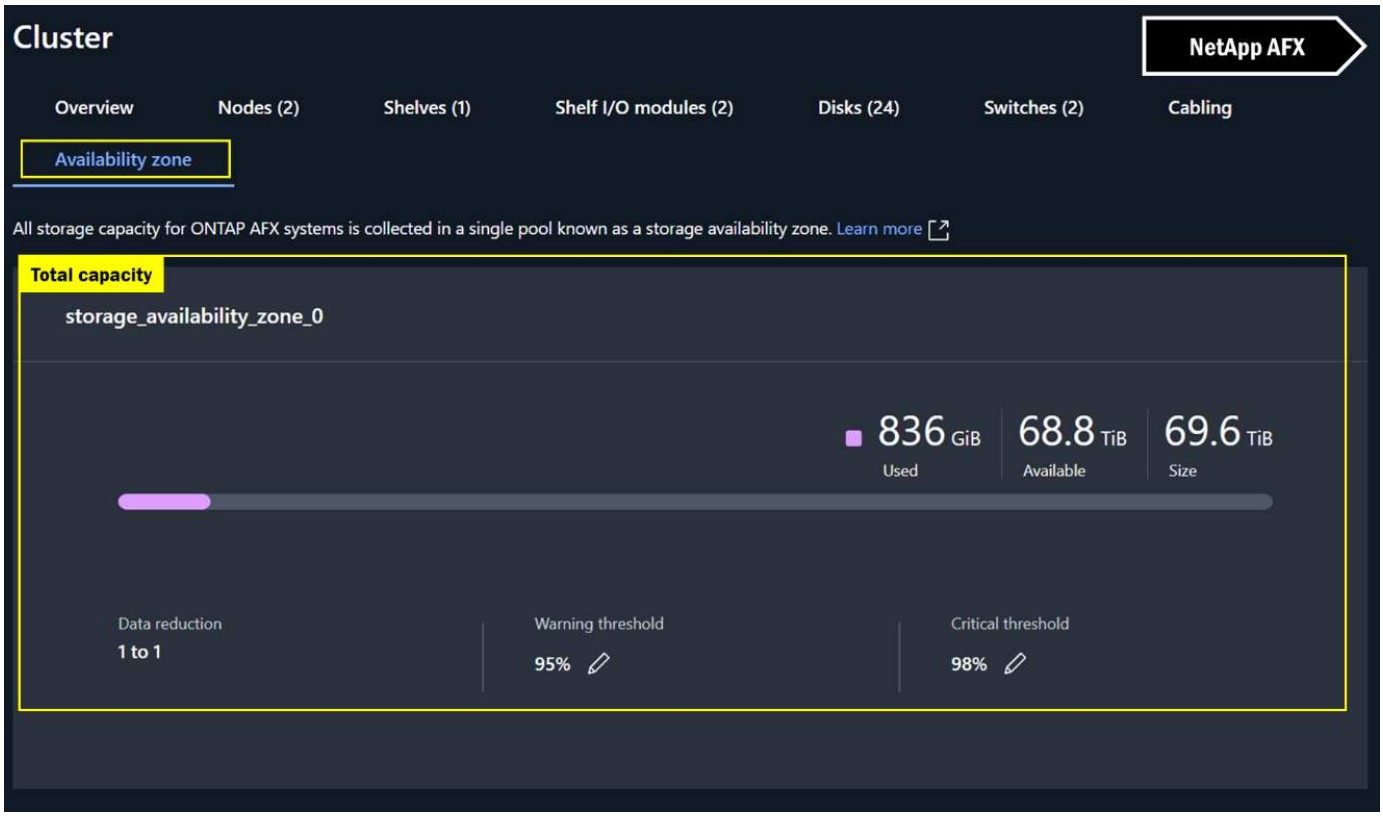
Unified ONTAP System Manager GUI에서는 티어를 사용하여 용량을 표시합니다. 실제로 GUI는 총계를 합산하여 클러스터의 전체 용량을 보여주려고 하지만, 전체 사용량은 여전히 애그리게이트 단위로 표시됩니다.

System Manager 용량 보기 **– Unified ONTAP**



NetApp AFX System Manager에서 클러스터 공간에 대한 보기 방식은 거의 동일하지만, 애그리게이트가 없으므로 추가 계산이 필요하지 않습니다. 표시되는 용량이 실제로 사용할 수 있는 용량입니다.

System Manager 용량 보기 **– NetApp AFX**

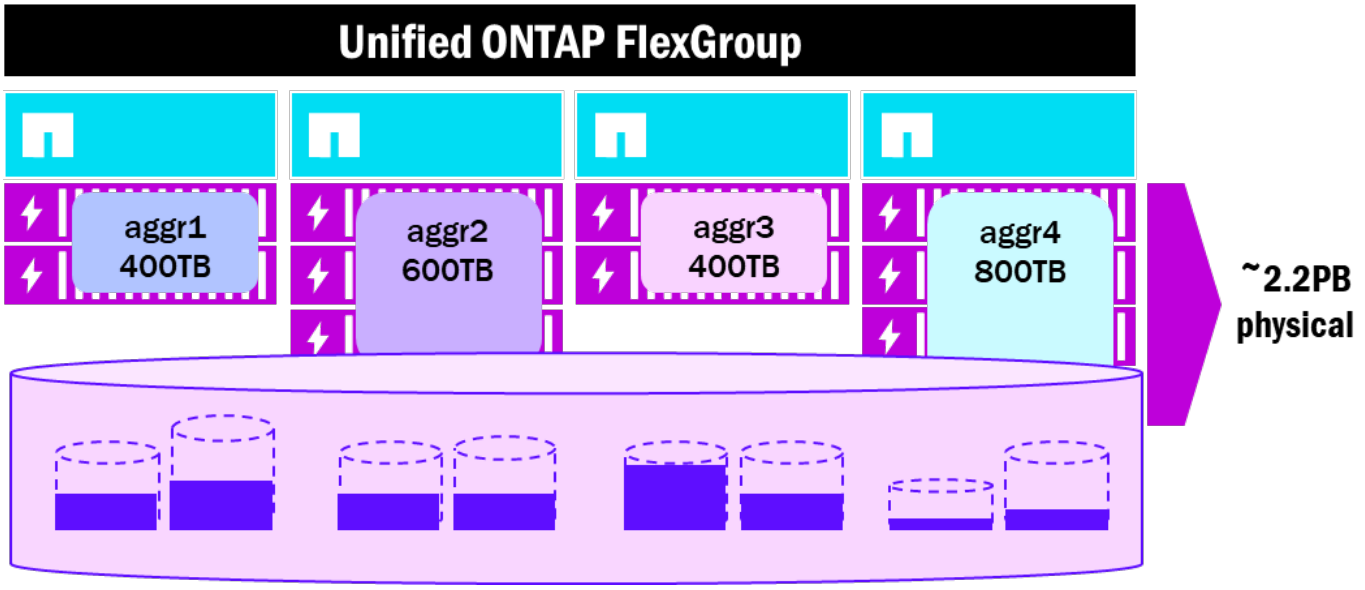


FlexGroup 볼륨 관리 개선 사항

FlexGroup 볼륨은 클러스터의 여러 노드와 애그리게이트에 걸쳐 생성된 여러 개의 기본 FlexVol 구성 볼륨으로 구성되며 NAS 클라이언트에 단일 대형 네임스페이스로 제공됩니다. FlexGroup 볼륨은 고성능 워크로드에 성능, 확장성, 로드 밸런싱 및 파일 수 이점을 제공합니다. 그러나 노드와 애그리게이트 간에 조정되기 때문에 용량이 차기 시작하면 물리적 한계에 직면할 수 있습니다. 애그리게이트에서 제공하는 독립적인 파일 시스템에도 독립적인 용량 사용량 및 제한이 있기 때문입니다. 예를 들어, FlexGroup 볼륨 구성 요소를 포함하는 애그리게이트가 클러스터의 다른 애그리게이트보다 먼저 용량이 차기 시작하면 전체 FlexGroup 자체에 용량 또는 성능 문제가 발생할 수 있습니다.

결과적으로 스토리지 관리자는 기본 FlexGroup 인프라에 대해 지나치게 걱정하게 되어 환경의 다른 측면을 유지 관리하는 데 소홀해질 수 있습니다.

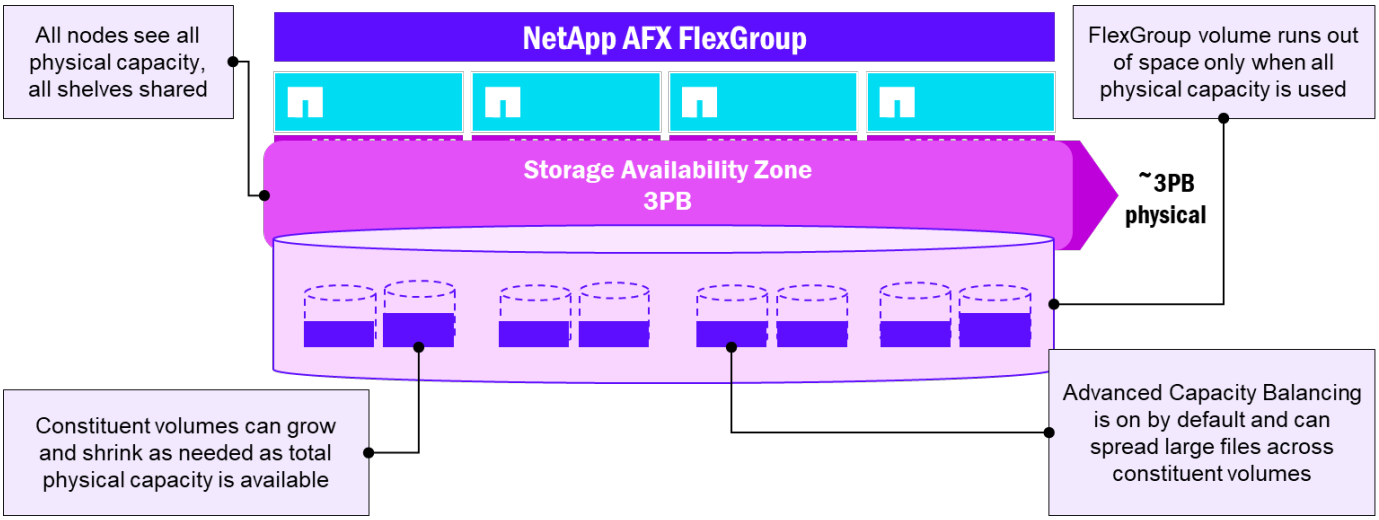
FlexGroup 볼륨 레이아웃 **-** 통합 **ONTAP** 애그리게이트



NetApp AFX는 단일 스토리지 가용 영역에 용량을 제공하며, 이는 FlexGroup 볼륨의 작동 방식과 더욱 유사합니다. 크기가 서로 다른 여러 애그리게이트에 걸쳐 여러 개의 구성 볼륨이 존재하는 대신, 모든 볼륨이 동일한 용량 풀에 상주하므로 FlexGroup 볼륨 사용 시 전반적인 관리 오버헤드가 크게 단순화됩니다.

또한 AFX는 FlexGroup 볼륨에 대해 Advanced Capacity Balancing을 기본적으로 활성화하여 볼륨 내 대용량 파일의 분산을 최적화합니다. 이제 FlexGroup 볼륨 구성 요소는 관리 개념이 아닌 백그라운드에서 조용히 작업을 수행하는 방식으로 전환됩니다.

FlexGroup 볼륨 레이아웃 **- NetApp AFX**



자동화된 스토리지 관리 작업

NetApp AFX의 스토리지 가용 영역을 사용하면 모든 용량이 모든 노드에서 공유됩니다. 노드는 여전히 볼륨을 소유하지만, ONTAP는 각 노드의 필요에 따라 용량을 빌리고 해제하여 각 노드의 용량 사용량을 자동으로 관리합니다. 즉, 스토리지 관리자는 더 이상 사용 가능한 공간의 균형을 최적으로 맞추는 방법에 대해 고민할 필요가 없습니다.

또한 RAID 그룹 관리는 ONTAP에 의해 자동화되어 있으며, 새로 추가된 디스크는 관리자 개입 없이 기존 또는 새로운 RAID 그룹에 추가됩니다. ONTAP는 데이터 복사 없이 노드 간 볼륨 이동도 관리합니다.

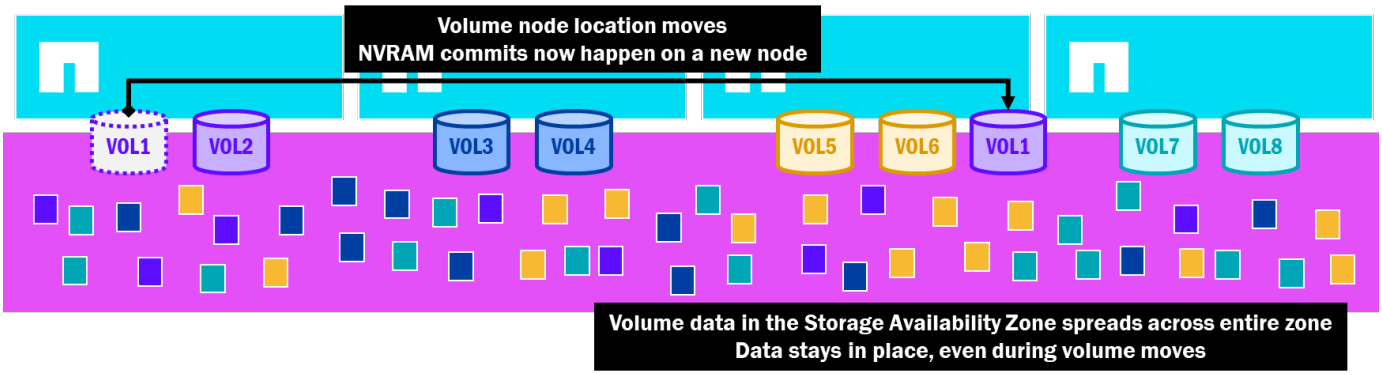
Unified ONTAP는 클러스터 전체의 성능 및 용량 사용량을 관리하는 방법으로 노드 또는 애그리게이트 간에 볼륨을 중단 없이 이동할 수 있는 방법을 제공합니다.

볼륨 이동이 시작되면 다음과 같은 일이 발생합니다.

- 지정된 대상 애그리게이트에 새로운 빈 볼륨이 생성됩니다
- 볼륨 메타데이터(스토리지 효율성 정보, 파일 핸들 등)는 새 대상 볼륨으로 복제됩니다
- 볼륨 데이터는 SnapMirror 기술을 통해 백엔드 클러스터 네트워크를 거쳐 대상 볼륨으로 복제됩니다. 대상 애그리게이트에 이동을 위한 여유 공간이 있어야 하며, 그렇지 않으면 이동 작업이 실패합니다.
- 두 볼륨이 데이터 변경 사항과 일관성을 유지하도록 볼륨 복제가 다시 수행됩니다
- 컷오버 프로세스가 시작되어 원본 볼륨을 오프라인으로 전환하고 대상 볼륨을 클라이언트의 새로운 원본 볼륨으로 승격합니다
- 클라이언트 IO는 전환 중에 잠시 일시 중지되지만 재마운트는 필요하지 않습니다

NetApp AFX에서 스토리지 가용 영역은 모든 노드에 모든 용량을 제공하며, 모든 노드는 해당 풀의 모든 디스크에 쓰기 작업을 수행할 수 있습니다. 데이터가 한 번 배치되면 볼륨이 이동되더라도 원래 위치에 그대로 유지됩니다. 즉, 데이터 복사가 필요하지 않습니다. 볼륨 이동 프로세스는 통합 ONTAP와 동일하지만, SnapMirror를 통한 데이터 복제가 필요하지 않습니다. 추가 용량도 필요하지 않습니다.

NetApp AFX에서 제로 복사 볼륨 이동



경량 볼륨 이동 기능을 통해 AFX는 성능이나 용량 제약 없이 많은 관리 작업을 자동화할 수 있으며, 이러한 볼륨 이동은 아래 항목에서 설명하는 NetApp AFX의 몇 가지 새로운 기능에 사용됩니다.

HA 페일오버 동작

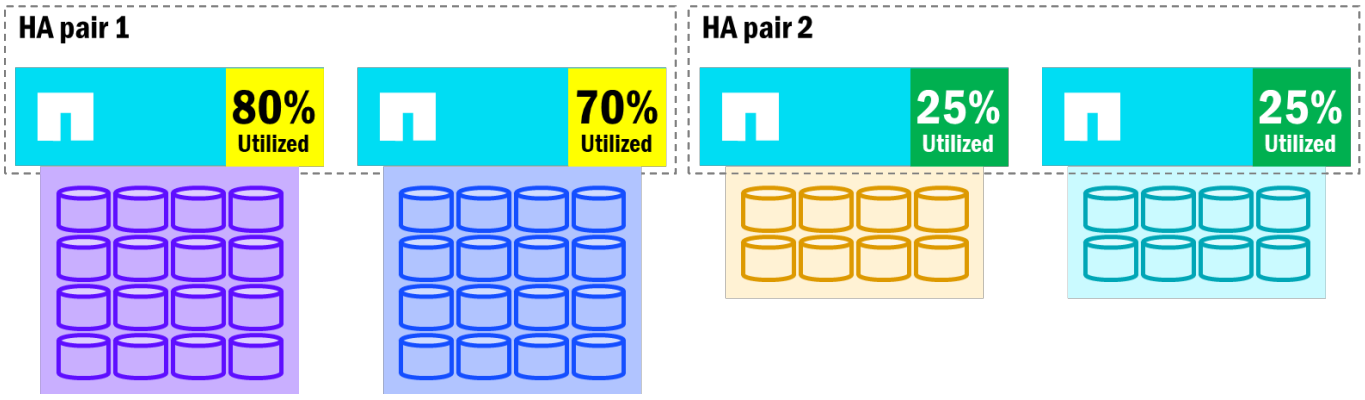
통합 ONTAP에서 노드는 디스크와 애그리게이트를 소유하며, 데이터는 볼륨을 통해 제공됩니다. 쓰기 작업은 로컬 노드의 NVRAM을 사용하여 해당 노드가 소유한 디스크에 플러시됩니다. 노드가 재부팅되거나 장애가 발생하면 ONTAP는 장애가 발생한 노드의 리소스에 대한 테이크오버를 트리거하여 디스크 및 애그리게이트 소유권을 파트너 노드로 이전합니다. 네트워크 인터페이스 또한 IP 공간의 포트로 페일오버되며, NVRAM 내용은 HA 쌍 전체에 지속적으로 복제되므로, 해당 노드는 NVRAM 내용을 플러시하여 장애가 발생한 노드의 쓰기 작업을 디스크에 커밋합니다. 이후, 생존한 노드는 노드 반환이 발생할 때까지 장애가 발생한 노드의 애그리게이트와 볼륨을 소유하게 됩니다. 즉, 페일오버 문제가 해결될 때까지 해당 볼륨과 이미 생존한 노드가 소유한 볼륨에 대한 모든 트래픽은 단일 노드에서 처리됩니다.

초기 통합 ONTAP 클러스터 구축 시에는 단일 노드가 파트너 노드에 과부하를 일으키는 것을 방지하기 위해 장애 조치 계획을 미리 세우는 것이 좋습니다. 어떤 볼륨이 성능 저하의 주요 원인이 될지 예측하기 어렵기 때문에 이는 그 자체로

어려운 과제이지만, 무중단 볼륨 이동 및 볼륨 QoS(서비스 품질) 정책과 같은 기능을 통해 문제를 완화할 수 있습니다.

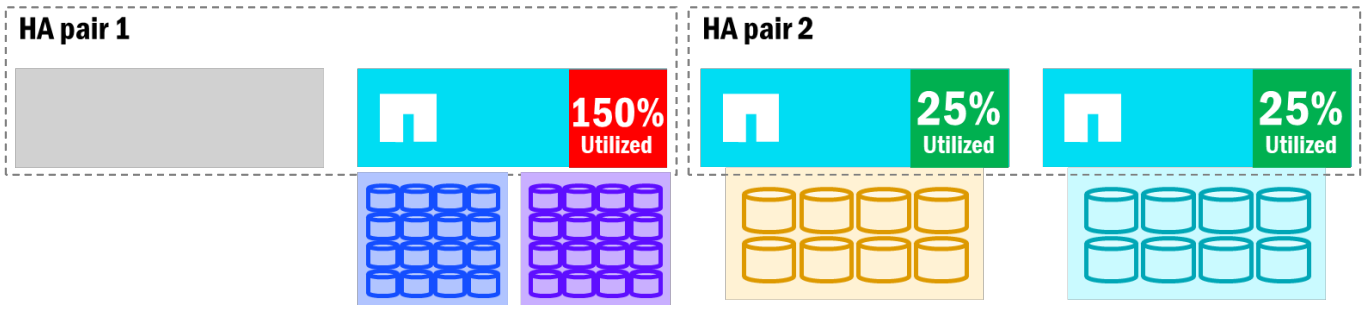
아래 이미지는 통합 ONTAP 클러스터에서 노드 간 성능 불균형이 발생할 수 있는 방식과 장애 조치로 인해 경우에 따라 성능 저하가 발생할 수 있는 방식을 보여줍니다.

Unified ONTAP – 노드 활용률의 잠재적 불균형



HA 쌍의 노드에 볼륨 수 및 성능 사용률 불균형이 발생하면 노드 페일오버가 전체 성능에 영향을 미칩니다. 정상 노드가 장애가 발생한 노드의 모든 볼륨을 소유하게 되기 때문입니다. 한편, 클러스터의 다른 노드에는 추가 작업을 처리할 여유가 있을 수 있습니다.

통합 **ONTAP –** 장애 조치가 노드 활용률에 미치는 영향



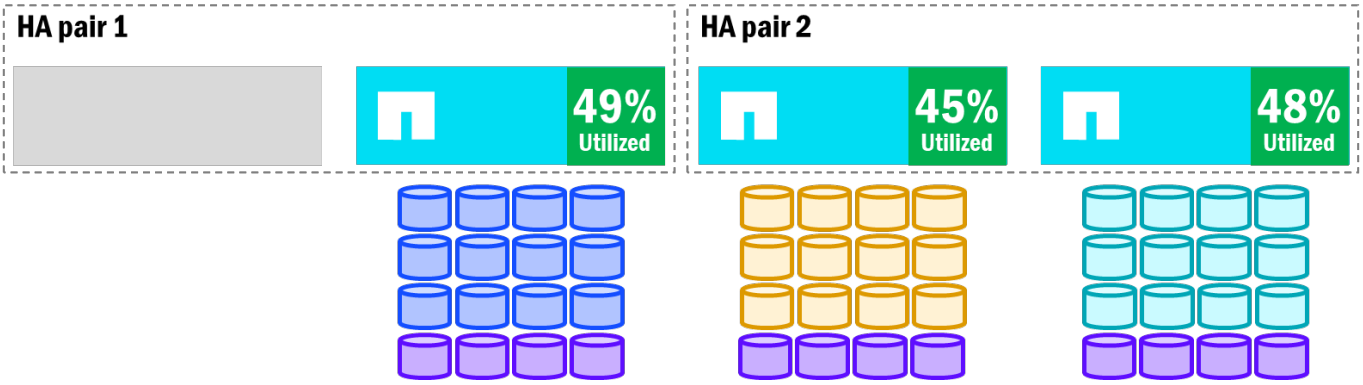
위 예시에서 HA 파트너 노드가 추가 작업을 처리해야 할 경우 과부하가 발생하여 해당 노드의 모든 볼륨 성능에 영향을 미칠 수 있습니다. 볼륨 이동은 이러한 상황을 완화하는 데 도움이 될 수 있지만, 노드 간 복사(사용 가능한 여유 공간 필요)가 필요하며, 이 작업에 소요되는 시간이 노드 장애 복구 시간보다 길어질 수 있습니다. 또한, 볼륨을 이동하면 원래 노드로 장애 복구되지 않습니다. 대신 이동한 노드에 그대로 유지됩니다.

NetApp AFX를 사용하면 노드 장애 조치가 몇 가지 다른 동작을 보입니다.

- 노드는 디스크를 소유하지 않고 물리적 애그리게이트도 없으므로 노드 페일오버 시 이러한 리소스를 전송할 필요가 없습니다. 대신 네트워크 인터페이스와 볼륨 소유권만 다른 노드로 이전됩니다.
- NVRAM 커밋은 여전히 발생하지만, 직접 연결 대신 HA 네트워크를 통해 이루어집니다.
- 볼륨이 파트너 노드로 초기 페일오버를 수행하면 AFX는 클러스터 내의 다른 생존 노드에 볼륨을 재분배합니다. 이는 제로 카피 볼륨 이동을 통해 가능합니다.
- 노드가 복구되면 볼륨은 원래 노드로 다시 이동합니다.

NetApp AFX는 클러스터의 노드 간 성능 균형을 유지하여 비교적 균등한 사용률을 유지하므로, 장애 조치가 발생하고 볼륨이 재분배될 때 클러스터 전체의 노드 사용률은 거의 동일해야 합니다.

NetApp AFX - 장애 조치 후 볼륨 재조정



노드 추가 및 제거

통합 ONTAP과 NetApp AFX 모두 클러스터에 노드를 추가하고 제거할 수 있습니다. 하지만 아키텍처 차이로 인해 노드 추가 및 제거 프로세스가 약간 다릅니다.

통합 **ONTAP**에서 노드 추가/제거

우리는 통합 ONTAP가 노드와 디스크 간의 직접적인 소유권 관계를 가지며, 모든 노드에는 디스크와 하나 이상의 애그리게이트가 연결되어 있어야 한다는 것을 이미 배웠습니다. 이러한 점을 염두에 두고, 추가 및 제거 시 다음 사항이 적용됩니다.

- 통합 ONTAP에서 노드를 추가할 때는 별도의 단계가 필요하지 않지만, 모든 노드(새 노드 포함)에서 균형 잡힌 성능을 제공하려면 볼륨을 새 노드로 이동해야 합니다. 이를 위해서는 기존 볼륨과 워크로드를 사전에 분석하고, 이동할 볼륨을 결정한 다음, 실제 볼륨 이동을 수행해야 합니다. 이 과정에서도 백엔드 클러스터 네트워크를 통해 데이터를 복사해야 합니다.
- 통합 ONTAP에서 노드를 제거하려면 해당 노드에 있는 기존 볼륨을 수동으로 옮겨야 합니다. 즉, 성능 균형을 유지하기 위해 어떤 노드에 어떤 볼륨을 저장할 수 있는지 파악해야 하며, 해당 볼륨을 이동할 수 있는 충분한 여유 공간이 있어야 합니다. 여유 공간이 부족한 경우, 클러스터 내에서 워크로드를 재배치하기 위해 추가적인 볼륨 이동이 필요할 수 있습니다. 노드 제거는 HA 페어 제거도 포함하므로 작업량이 두 배로 늘어납니다. 또한 각 노드는 디스크를 소유하고 있으므로 해당 노드의 전체 디스크를 다시 초기화해야 합니다. 이러한 모든 요소는 비교적 간단해야 할 작업에 시간과 노력을 추가합니다.

NetApp AFX에서 노드 추가/제거

또한 NetApp AFX는 표준 노드-디스크 소유권 방식을 활용하지 않고 물리적 애그리게이트를 사용하여 클러스터에 용량을 제공하지 않는다는 사실을 알게 되었습니다. 이 때문에 노드 추가 및 제거 동작 방식이 다소 다릅니다.

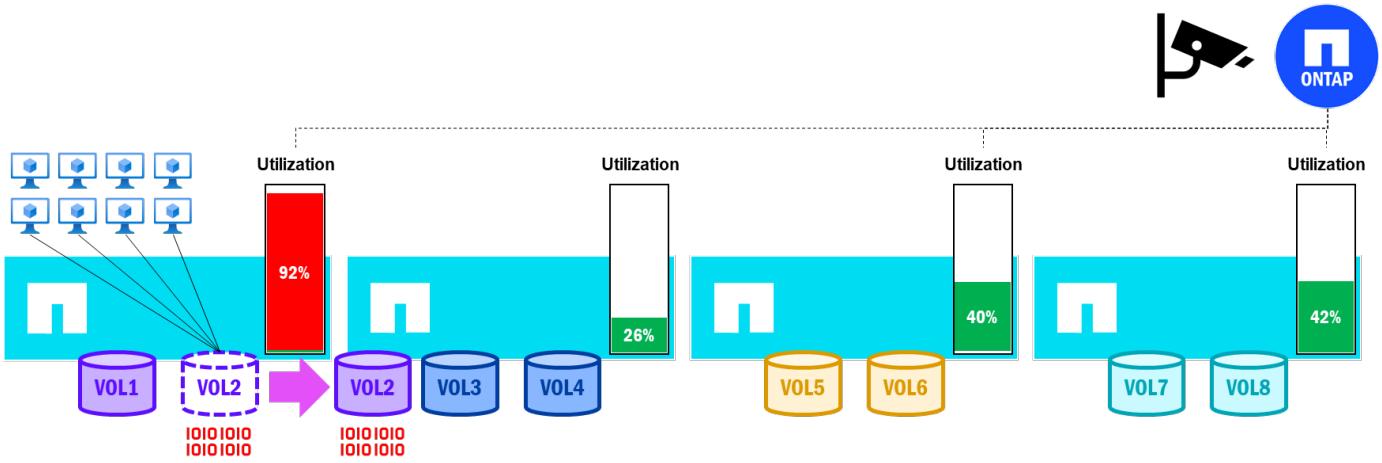
- NetApp AFX에 노드를 추가할 때 더 이상 사전 볼륨 분석이나 관리자 개입을 통해 각 노드의 볼륨 균형을 맞출 필요가 없습니다. 대신 ONTAP는 새로 추가된 노드 간에 볼륨 수를 자동으로 균형 있게 분산하여 비교적 균일한 성능 프로필을 유지합니다. ONTAP는 데이터 복사 없이 자동으로 볼륨을 노드 간에 이동하므로 클러스터에 노드를 추가하는 데 필요한 시간, 용량 및 노력을 줄여줍니다.
- NetApp AFX에서 노드를 제거하는 데에는 수동 작업이 거의 또는 전혀 필요하지 않습니다. 노드 제거 태그가 지정되면 ONTAP는 자동으로 볼륨을 다른 노드로 이동하여(복사 없이) 제거되는 노드의 데이터를 비웁니다. 또한 노드에 디스크가 할당되지 않으므로 노드 제거 후 디스크를 다시 초기화할 필요가 없습니다. 이러한 특징 덕분에 AFX의 노드는 모듈식 구조를 가지며 확장 및 축소가 용이합니다.

성능 중심 볼륨 이동

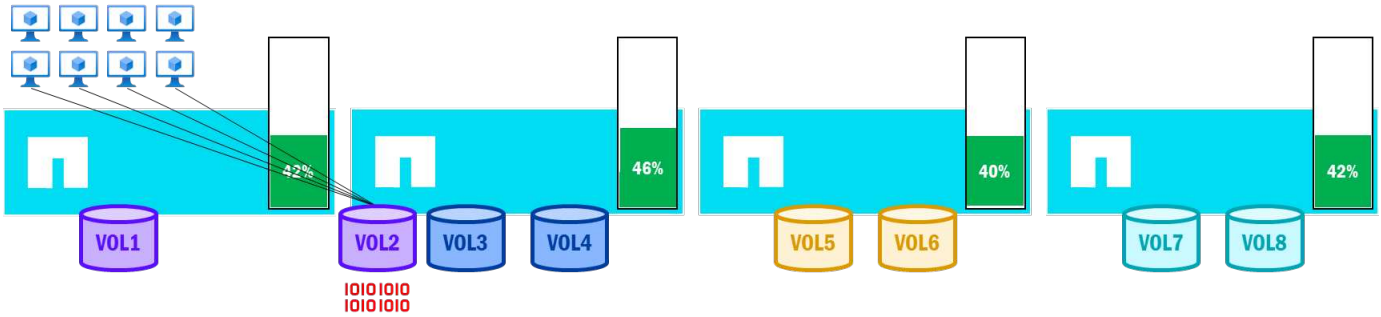
NetApp AFX의 제로 카피 볼륨 이동 기능은 데이터를 복사하지 않고 필요에 따라 볼륨의 균형을 재조정할 수 있으므로 추가 용량 없이도 빠르게 수행할 수 있습니다. 즉, 볼륨 이동이 ONTAP 클러스터에서 사용할 수 있는 자동 로드 밸런싱의 주요 부분이 될 수 있습니다. 이제 볼륨 이동 비용이 거의 들지 않으므로 ONTAP는 이 유용한 도구를 활용하여 성능 중심의 볼륨 로드 밸런싱과 같은 기능을 통합할 수 있습니다.

NetApp AFX의 ONTAP 9.18.1 이상 버전에서는 노드, HA 쌍 및 볼륨 사용률이 지속적으로 모니터링되는 동시에 성능 데이터가 수집 및 분석됩니다. 노드 사용률이 정의된 임계값을 벗어나면 ONTAP는 클러스터 전체의 균형 잡힌 성능을 유지하기 위해 사용률이 낮은 노드로 이동할 볼륨을 자동으로 선택합니다.

NetApp AFX에서 성능 기반 볼륨 이동 **-** 높은 사용률 시 볼륨 이동이 트리거됩니다



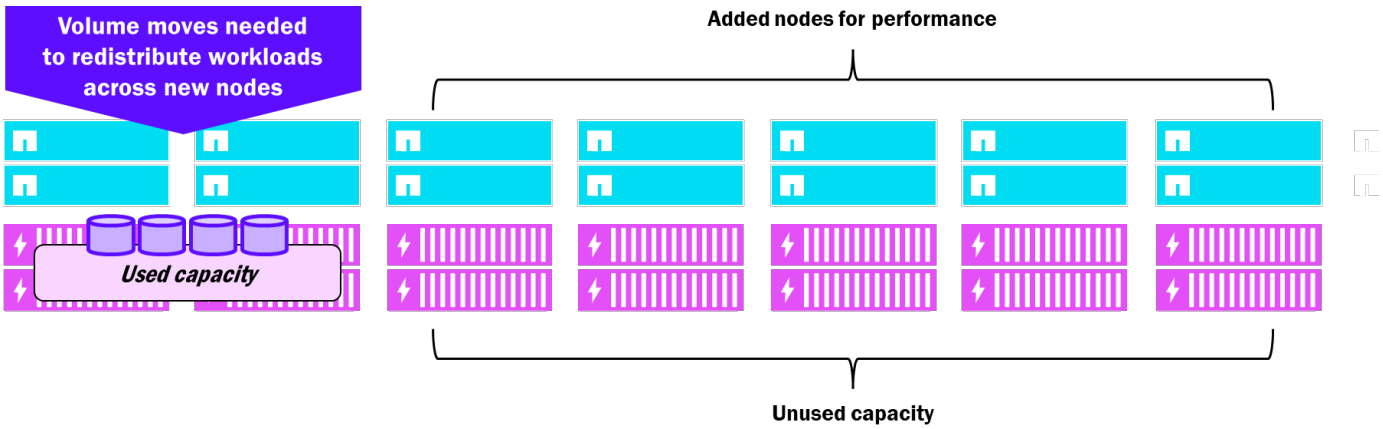
NetApp AFX에서 성능 기반 볼륨 이동 **-** 볼륨 이동 후 노드 활용률 균형 유지



클러스터 규모 및 확장

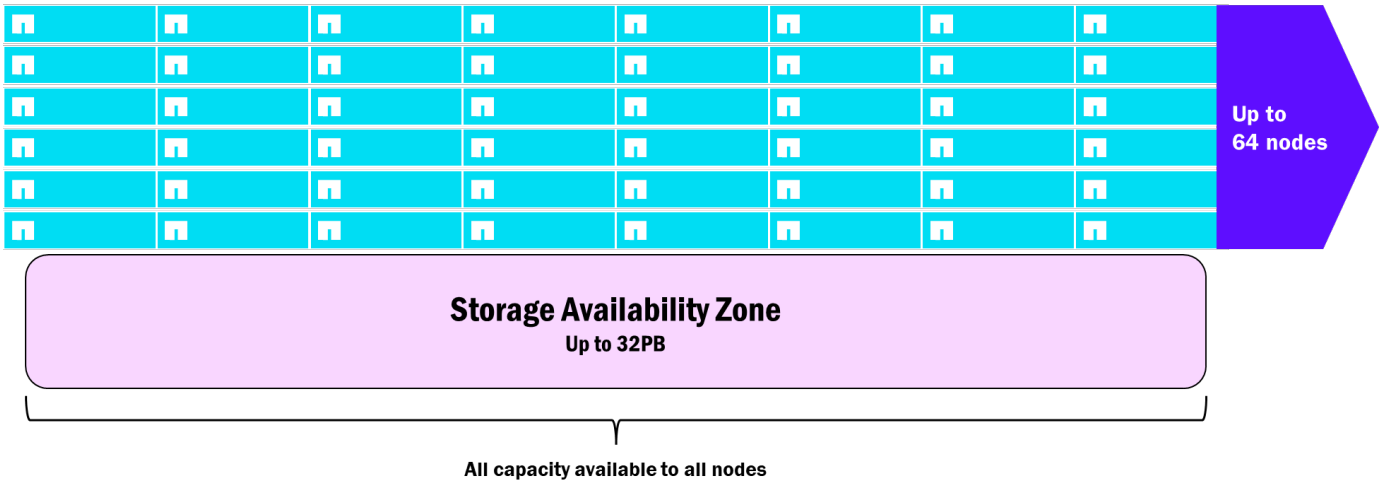
Unified ONTAP 클러스터는 최대 24개의 노드를 지원하며, 추가되는 각 노드에는 시스템 기능 및 데이터 서비스를 위한 디스크가 반드시 포함되어야 합니다. 디스크 쉘프는 클러스터에 추가할 수 있지만, 클러스터 크기가 24개 노드이든 관계없이 항상 단일 HA 쌍에 연결되고 단일 노드에서만 소유됩니다. 즉, 성능만 필요한 경우에도 클러스터에 용량이 추가되며, 이러한 성능 증가는 대부분 새 노드가 소유하는 특정 디스크 세트로 제한됩니다. 결과적으로 반드시 필요하지 않은 추가 용량이 발생할 수 있습니다.

Unified ONTAP – 추가된 확장 고려 사항



NetApp AFX는 클러스터에 대해 더 큰 규모를 지원합니다. 9.19.1부터 AFX 클러스터는 단일 클러스터에서 최대 32개의 노드에 도달할 수 있습니다. 그리고 모든 노드가 모든 디스크를 보고 액세스할 수 있으므로, 모든 노드는 해당 드라이브의 성능과 용량(ONTAP 9.19.1 기준 최대 32PB)을 공유할 수 있어 리소스가 고립되는 일이 없습니다. 볼륨 이동에는 복사가 필요하지 않으므로, ONTAP은 새로 추가된 노드로 볼륨을 자동으로 이동시켜 노드 활용도를 고르게 분산시키고, 용량은 Storage Availability Zone을 통해 고르게 분배됩니다.

NetApp AFX – 확장 고려 사항 추가



루트 볼륨 변경

NetApp ONTAP에서 각 노드에는 루트 볼륨이 할당되며, 이 볼륨은 로그 파일, 부팅 이미지, 코어 파일, 클러스터 데이터베이스 등과 같은 시스템별 파일 및 기능에 사용됩니다.

통합 ONTAP에서 이러한 루트 볼륨은 물리적 루트 애그리게이트에 저장되었습니다. 루트 애그리게이트가 사용하는 용량을 줄이기 위해 ADP(Advanced Disk Partitioning)를 통해 데이터 드라이브 파티션에 걸쳐 생성되었습니다.

NetApp AFX는 물리적 애그리게이트를 방정식에서 제거하므로 루트 애그리게이트와 ADP를 사용할 필요가 없습니다. 루트 볼륨은 여전히 개념으로 존재하지만 이제 용량 풀의 가상화된 영역에 존재하며 추가 구성이 필요하지 않습니다. 또한 루트 볼륨 기능이 변경됩니다. 부팅 이미지와 복제된 클러스터 데이터베이스는 스토리지 스택에서 각 AFX 노드에 있는 온보드 부팅 미디어로 이동됩니다. 이제 스토리지 스택에 대한 액세스가 손실되더라도 노드는 계속 부팅하고 클러스터 자격을 유지할 수 있으므로 문제 해결의 복잡성이 완화됩니다.

온보드 부팅 미디어

NetApp AFX 노드는 약 3.8TB 크기의 NVMe 연결 M.2 장치인 온보드 부트 미디어를 활용합니다. 이러한 부트 장치에는 스토리지 인클로저와 별도로 부트 이미지 파일과 복제된 데이터베이스가 포함되어 있어 디스크 액세스 문제 발생 시 추가적인 이중화를 제공합니다. 부트 미디어에 장애가 발생하면 해당 노드는 HA 파트너에 의해 인계되고 부트 미디어를 교체할 수 있습니다. 교체가 완료되면 스토리지 관리자가 새로운 ONTAP 이미지를 장치에 로드하고 ONTAP는 자동으로 클러스터 데이터베이스를 재구축하여 전체 기능을 복원합니다.

성능

NetApp AFX는 성능과 확장성을 염두에 두고 설계되었으며, 특히 높은 읽기 및 쓰기 처리량이 필요하고 간단하고 선형적인 확장이 가능한 워크로드에 적합합니다.

노드별 성능

각 NetApp AFX 스토리지 노드는 읽기 및 쓰기에 대해 특정 처리량을 제공합니다. 클러스터에 노드가 추가됨에 따라 성능이 선형적으로 증가하며, 이는 이 문서의 "노드 성능의 선형 확장" 섹션에서 설명합니다.

현재 노드 유형은 "AFX 1K"이며 아래와 같이 읽기 및 쓰기 처리량을 제공합니다. NetApp AFX에 새로운 하드웨어가 추가되면 이러한 제한 사항이 변경될 수 있습니다. 참고: 최대 성능은 아래 "벤치마크 결과" 섹션에 표시된 것처럼 여러 클라이언트가 여러 파일을 읽고 쓰는 환경에서 달성되었습니다.

노드당 성능 예상치

노드 유형	최대 읽기 성능	최대 쓰기 성능
AFX 1K	~35GB/s	~10GB/s

최신 성능 예상치는 NetApp 영업팀에 문의하십시오.

쉘프별 성능

각 셸프에는 16개의 100GB 이더넷 포트를 갖춘 고성능 셸프 모듈이 포함되어 있으며, 클러스터의 컴퓨팅 노드와 고대역폭 스토리지 상호 작용을 위해 RoCEv2 통신을 활용합니다. 모든 물리적 리소스와 마찬가지로 이러한 셸프에도 달성할 수 있는 최대 성능이 있으며, 특히 NetApp AFX는 동일한 디스크 세트를 가리키는 여러 노드를 구성할 수 있기 때문에 더욱 그렇습니다. 다음 표는 TLC 및 QLC 드라이브에 대한 단일 셸프의 예상 최대 읽기 및 쓰기 성능을 보여줍니다. TLC와 QLC의 차이점에 대한 자세한 내용은 "TLC와 QLC"를 참조하십시오.

셸프당 성능 예상치

쉘프 모듈 유형	최대 읽기 성능	최대 쓰기 성능
NSM 140	140GB/s (TLC 및 QLC)	70GB/s TLC 35GB/s QLC

최신 성능 예상치는 NetApp 영업팀에 문의하십시오.

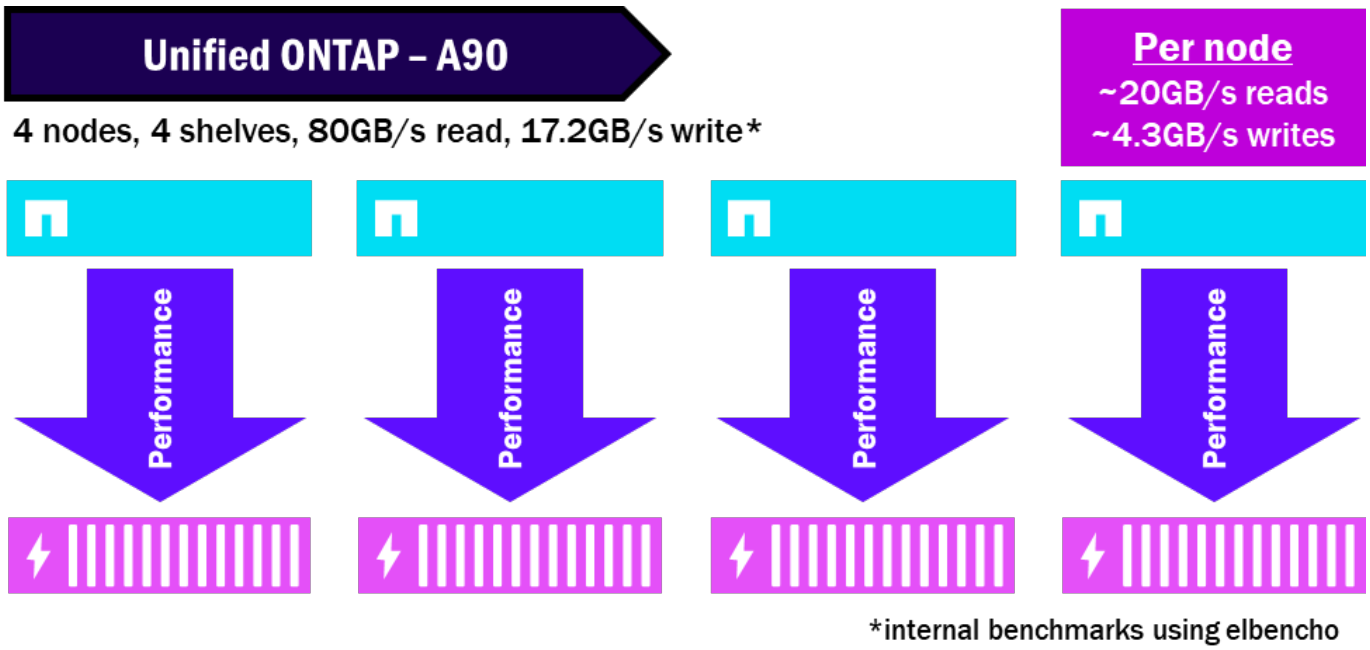
성능 밀도

분산형 ONTAP 아키텍처에서 스토리지 노드와 셸프를 분리하면 더 많은 노드가 더 적은 셸프로 트래픽을 전송할 수 있으므로 필요한 용량만으로 최대 성능을 얻는 데 필요한 전체 데이터 센터 공간을 줄일 수 있습니다.

이러한 "성능 밀도" 개념을 통해 스토리지 관리자는 스토리지 환경을 과도하게 프로비저닝할 필요 없이 보유한 하드웨어를 최대한 활용할 수 있습니다.

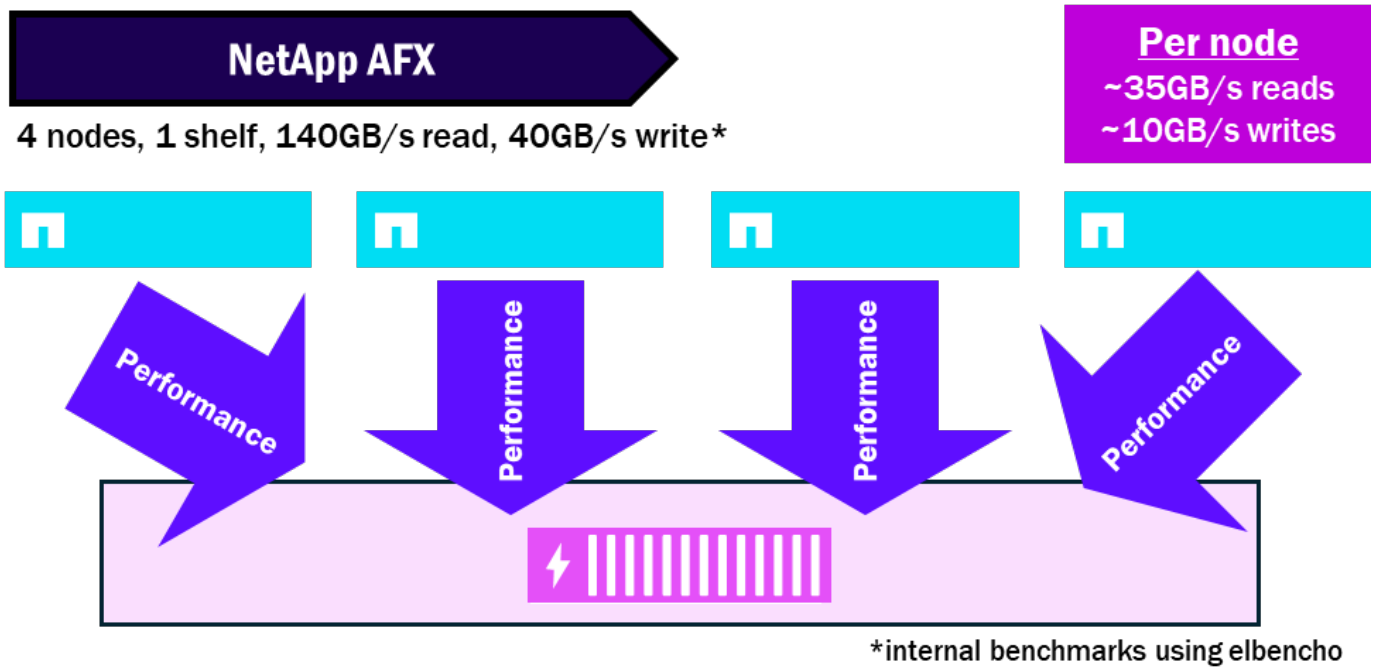
예를 들어, 통합 ONTAP 클러스터에서는 각 노드가 자체 디스크 세트를 가지므로 성능은 해당 노드가 소유한 디스크에만 집중됩니다. 또한 하나의 노드만 하나의 디스크 세트에 접근할 수 있기 때문에 사용 가능한 디스크를 완전히 활용하여 최대 성능을 달성하지 못할 수도 있습니다.

Unified ONTAP – 성능 분배 방식



NetApp AFX는 모든 디스크를 단일 스토리지 가용 영역으로 통합하여 모든 노드가 모든 디스크를 활용할 수 있도록 합니다. 또한 디스크와 노드가 분리되어 있으므로 동일한 성능을 얻기 위해 필요한 쉘프 수가 줄어듭니다. 이를 통해 성능이 집중되고 쉘프의 최대 성능 잠재력을 극대화할 수 있습니다.

NetApp AFX – 성능 밀도



노드 대 쉘프 비율

Unified ONTAP 노드는 노드당 최소 한 세트의 디스크가 필요하며, 단일 노드에 여러 개의 셸프를 연결할 수 있습니다. 따라서 자체 디스크 용량을 충분히 활용하지 못하는 단일 노드에서 성능 병목 현상이 발생할 수 있습니다.

NetApp AFX는 모든 디스크 셸프를 모든 노드에 제공합니다. 각 셸프에는 16개의 100GB RoCE 지원 인터페이스가 있는 모듈이 포함되어 있어 셸프당 허용되는 총 성능을 향상시킵니다. 따라서 여러 노드가 동일한 디스크 세트에 읽기/쓰기 작업을 수행하여 단일 셸프의 성능을 최대한 활용할 수 있습니다.

ONTAP 9.19.1 버전 기준으로 노드 대 쉘프 포화 비율은 약 4:1입니다.

벤치마크 결과

다음 섹션에서는 아래 구성 매개변수를 사용하는 NetApp AFX 클러스터의 벤치마크 결과를 다룹니다.

- 4개 노드, 4개 데이터 인터페이스
- 2개의 쉘프(7.6TB 드라이브)
- ONTAP 9.19.1
- NFSv4.2(pNFS, 세션 트렁킹)
- FlexGroup 볼륨
- "ElBencho" 벤치마크
- 쓰기: elbencho --hosts=x.x.x.[y-z] -d -w -b 1M -t 80 --iodepth 1 --direct -s 600g /fio_vol1/
- 읽기: elbencho --hosts=x.x.x.[y-z] -r -b 256k -t 80 --lat --iodepth 2 --direct -s 600g --infloop /fio_vol1/
- Cisco C240 M8 서버 4대, 2포트 * 200GbE CX-7 카드, 80개 스레드
- NFS 마운트 옵션: rw,vers=4.2,rsize=1048576,wsize=1048576,trunkdiscovery,proto=tcp

위 구성은 4노드 클러스터에서 사용 가능한 최대 읽기 속도(~134GB/s)에 매우 근접했으며, 노드당 허용된 최대 쓰기 속도(40GB/s)에 정확히 도달했습니다.

NetApp AFX – ElBencho 읽기 성능, 4개 노드

NetApp AFX – ElBencho 쓰기 성능, 4개 노드

적극적인 사전 읽기

미디어 스트리밍 워크로드에서 4K 영화는 종종 수만 개의 파일로 분할되며, 각 파일의 크기는 일반적으로 50MB에서 250MB 사이입니다. 각 파일은 프레임을 나타내며, 애플리케이션은 단일 요청으로 전체 프레임을 읽습니다. 버퍼링 없이 매끄럽고 끊김 없는 스트림을 유지하려면 이러한 프레임 읽기가 끊김 없이 완료되어야 합니다.

ONTAP는 (`-aggressive-readahead-mode`이러한 워크로드를 최적화하기 위한 볼륨 수준 옵션을 제공합니다. ONTAP 9.19.1부터 유사한 파일 유형(예: 미디어 렌더링 및 스트리밍)에서 예측 가능한 I/O 패턴을 가진 워크로드를 가속화하기 위해 적극적인 미리 읽기를 위한 새로운 `cross_file_sequential_read`모드가 AFX에 도입되었습니다.

cross_file_sequential_read는 파일 이름을 기반으로 다음에 읽을 파일을 예측하고 클라이언트가 읽기 호출을 하기 전에 해당 파일들을 미리 읽어옵니다. 이 예측 로직은 디렉터리 내의 모든 파일이 단조롭게 증가하는 숫자 접미사(예: file1, file2, file3)를 사용하는 명명 패턴을 따른다고 가정합니다. 디렉터리 내의 모든 파일은 십진수 또는 16진수 번호를 사용하여 이 패턴을 따라야 합니다. 파일 이름은 최대 255자까지 가능합니다. 이 로직은 파일 확장자에 관계없이 현재 파일 이름만을 기반으로 현재 디렉터리에서 다음에 읽을 파일 이름 세트를 생성합니다. 이전에 10진수 번호로 생성된 파일 이름이 디렉터리에 존재하지 않으면 16진수 번호로 다시 생성됩니다. 생성된 파일 이름 중 어느 것도 존재하지 않으면 해당 세트에 대한 프리페칭은 수행되지 않습니다. 프리페칭은 다음 클라이언트 읽기 호출이 발생하면 재개됩니다.

이러한 옵션을 활성화하면 "frametest" 성능 벤치마크에서 30개 클라이언트(NFSv3 및 SMB3)와 34개 클라이언트(NFSv4.1)를 사용하여 초당 30프레임으로 30,000개의 4K 프레임을 읽을 수 있었으며, 프레임 손실은 단 한 건도 발생하지 않았습니다.

파일 간 순차 읽기는 주로 미디어 워크로드를 위해 설계되었지만, AI 학습 및 추론과 같이 액세스 패턴과 파일 이름이 예측 가능한 다른 읽기 중심 워크로드에서도 이점을 얻을 수 있습니다.

고려 사항 및 주의 사항

- 공유 버퍼 캐시 - 적극적인 읽기 미리 읽기 기능은 노드의 다른 볼륨과 동일한 버퍼 캐시를 사용합니다. 이 기능을 활성화하면 해당 노드의 다른 볼륨에 대한 읽기 성능에 영향을 줄 수 있습니다.
- 기본 스토리지 성능 – 파일 읽기 속도가 충분히 빠르지 않으면(예: HDD 기반 FAS 시스템) 클라이언트 읽기가 발생하기 전에 캐시된 데이터가 제거되어 미리 읽기의 이점이 상쇄될 수 있습니다.
- 액세스 패턴 요구 사항 – 워크로드의 읽기 패턴이 순차적이지 않거나 디렉터리의 파일 이름이 순차적으로 증가하는 순서로 지정되지 않은 경우 cross_file_sequential_read의 적극적인 미리 읽기 모드는 의미 있는 이점을 제공하지 않습니다.

NFSv4.x 성능 향상

NFS 버전 3은 1995년 공식 출시 이후 수십 년 동안 NFS 애플리케이션의 표준으로 자리 잡았습니다. 뛰어난 성능과 안정성 덕분에 최신 NFS 버전으로의 전환이 어려운 이유도 충분합니다.

하지만 NFSv3에도 한계가 있습니다. 프로토콜의 무상태성은 성능 향상과 스토리지 장애 조치 시 중단 최소화에는 좋지만, 데이터 일관성 및 잠금 관리에는 적합하지 않습니다. NFS 서버는 잠금 상태를 추적하지 않기 때문에 장애 발생 시 NFS 서버가 잠금을 해제할 수도 있고 해제하지 않을 수도 있으며, NFS 클라이언트는 파일이 잠겨 있는지 여부를 알 수 없을 수 있습니다.

Security for NFSv3 is also a bit lacking. The protocol requires multiple open firewall ports to function properly and numeric IDs are sent in plaintext over the wire. Furthermore, NFS does not have robust ACL support, and does not include native file and folder auditing. As a result of these limitations, NFSv4 was created in 2003 via link:https://datatracker.ietf.org/doc/html/rfc3530[RFC-3530^] (obsoleted in 2015 by link:https://datatracker.ietf.org/doc/html/rfc7530[RFC-7530^]). NFSv4.x는 20년 이상 존재해 왔지만, 몇 가지 이유로 아직 널리 채택되지 못했습니다.

- ID 관리의 복잡성: 많은 환경에서 NFSv4.x의 이름 문자열 및 Kerberos 보안 요구 사항을 제대로 활용하기 위한 네임 서비스 인프라가 구축되어 있지 않습니다.
- 최신 NFS 클라이언트의 필요성: NFSv4가 처음 출시된 시점으로부터 시간이 흐른 지금과 같이 현대적인 NFS 환경에서는 이 문제가 덜 중요해졌습니다. 현재 사용되는 거의 모든 운영 체제에는 NFSv4를 완벽하게 지원하는 NFS 클라이언트가 포함되어 있지만, 필요한 NFSv4.x 패키지가 없는 레거시 시스템도 여전히 존재합니다. 실제로 일부 애플리케이션은 여전히 이전 버전의 NFS를 사용해야 합니다.
- "고장 나지 않았으면 고치지 마라"는 사고방식: 기업 IT 조직은 새로운 기술, 심지어 20년 이상 된 기술조차 도입하는 데 있어 매우 보수적인 것으로 악명이 높습니다. 현재 NFS 버전이 잘 작동하고 있다면 왜 바꿔야 할까요?
- 성능 문제: NFSv4.x와 같은 상태 저장 프로토콜의 성능은 지난 20년 동안 대부분 상태 비저장 NFSv3에 비해 뒤처져 왔습니다. 과거에는 성능 영향이 NFSv4.x의 장점을 상쇄하는 경우가 많았습니다.

AFX를 사용한 ONTAP 9.18.1의 NFSv4.x 개선 사항

ONTAP의 일부 아키텍처 변경으로 NFS의 전반적인 성능이 크게 향상되었으며, NFSv4.x의 성능 개선에도 상당한 진전이 있었습니다.

다음은 이러한 변경 사항 중 일부를 간략하게 요약한 것입니다.

순차 읽기 향상**: NFSv4.1**이 **NFSv3**보다 **30%** 우수

ONTAP 9.18.1은 NFSv4.1을 사용한 다중 경로 IO 지원을 도입했습니다. MPIO는 WAFL 파일 시스템에서 읽기 작업을 처리하는 대신, 읽기 작업을 네트워크 도메인으로 이동시켜 다중 경로 안전 방식으로 처리합니다. 이 접근 방식은 컨텍스트 스위치를 줄여 순차 읽기 트래픽에서 전반적인 병렬성을 향상시키고, WAFL을 우회하여 버퍼 관리의 오버헤드를 줄입니다.

FlexGroup 볼륨의 임의 읽기 향상**: NFSv4.1**이 **NFSv3**의 **7%** 이내

FlexGroup 볼륨은 여러 개의 하위 구성 볼륨을 하나의 통합 네임스페이스로 제공하는 볼륨입니다. AFX에서 FlexGroup 볼륨은 기본적으로 고급 용량 균형 조정(Advanced Capacity Balancing)이 활성화되어 있어 10GB보다 큰 파일은 여러 구성 볼륨에 멀티파트 파일로 분산하여 기록됩니다. 이러한 파일 파트가 원격 위치에 저장되기 때문에, 기존 NFSv4.x 환경에서는 임의 읽기 성능이 다소 떨어지는 문제가 있었습니다(NFSv3보다 약 18% 낮음). ONTAP 9.18.1 버전에서는 이러한 문제를 해결하기 위해 NFSv4.x 환경에서 멀티파트 읽기에 대한 캐시된 IO 지원을 도입했습니다. 참고: 이 변경 사항은 FlexVol 볼륨에는 적용되지 않습니다.

순차 쓰기**:** 이전 릴리스 대비 **+10%** 향상

HA 페일오버 기능에 사용되는 NVLOG 데이터 복제 방식이 개선되어 NetApp AFX 시스템의 전반적인 순차 쓰기 성능이 향상되었습니다.

메타데이터 작업**: EDA** 벤치마크에서 **NFSv3** 대비 **15%** 이내의 성능

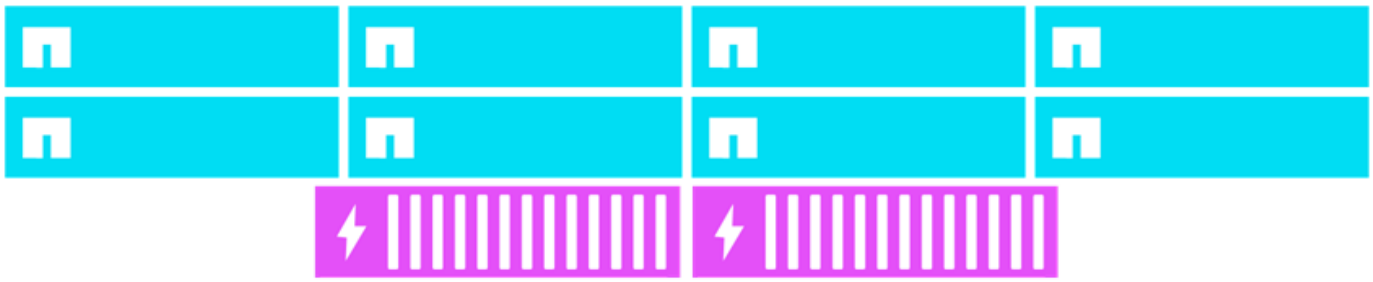
NFSv4.1은 전통적으로 모든 OPEN 및 CLOSE 작업을 직렬화하여 클러스터 노드가 네트워크에서 WAFL로 전송되기 전에 한 번에 하나씩 처리합니다. ONTAP 9.18.1에서는 동시 열림/닫힘(COC) 기능을 도입하여 경쟁 조건 해결 방식을 변경함으로써 네트워크 직렬화를 없애고 이전 릴리스에서 발생했던 OPEN/CLOSE 병목 현상을 해결합니다.

이러한 모든 변경 사항은 AFX에서 이루어진 아키텍처 변경 사항과 함께 ONTAP 9.18.1에서 전반적인 NFSv4.1 성능을 향상시킬 수 있게 했습니다.

순차 **IO** 결과

성능이 다소 향상된 부분 중 하나는 순차 I/O(즉, 예측 가능하고 순차적으로 발행되는 I/O)였습니다. fio를 사용한 표준 성능 테스트에서 ONTAP 9.18.1을 실행하는 AFX는 순차 읽기 성능을 거의 30%, 순차 쓰기 성능을 10% 향상시켰습니다.

NetApp AFX – ONTAP 9.18.1에서의 **NFSv4.1** 순차 **IO** 성능



	AFX 9.17.1	AFX 9.18.1
Seq. reads	220GB/s	**283GB/s**
Seq. writes	70.6GB/s	**77.7GB/s**

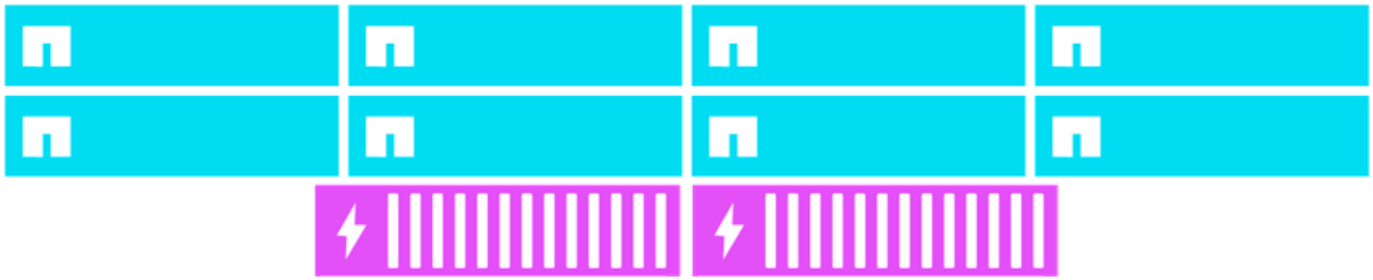
메타데이터 비중이 높은 워크로드 결과

NFSv4.x의 주요 성능 저하 요인 중 하나인 메타데이터 처리 성능이 더욱 인상적으로 개선되었습니다. 메타데이터는 파일 소유자 및 속성 관리, 파일 생성 및 목록 조회 등에 사용되는 일반적으로 4K 범위의 랜덤 IO입니다. NFSv4.x의 상태 유지 특성으로 인해 이러한 유형의 작업은 CPU 및 지연 시간 측면에서 더 많은 비용이 소요되며, 이는 결과적으로 전반적인 성능을 저하시킵니다.

AFX ONTAP 9.18.1의 변경 사항으로 이러한 유형의 워크로드에 대한 NFSv4.x 성능이 크게 향상되어 NFSv3 성능과의 격차를 15% 이내로 좁혔습니다.

저희 성능 엔지니어링 팀은 표준 AI 이미지, EDA 및 소프트웨어 빌드 벤치마크의 성능을 비교한 결과 이전 ONTAP 릴리스 대비 상당한 성능 향상을 발견했습니다.

NetApp AFX – ONTAP 9.18.1에서의 **NFSv4.1** 메타데이터 **IO** 성능



	9.17.1	9.18.1	Delta
AI Image processing	209 KIOPS	**239 KIOPS**	**+16%**
Software dev	600 KIOPS	**950 KIOPS**	**+58%**
EDA	480 KIOPS	**881 KIOPS**	**+84%**

관리 툴

NetApp AFX에서 스토리지를 표현하는 방식에는 아키텍처적으로 상당한 차이가 있지만, 기능 세트와 ONTAP 관리 방식은 사실상 변경되지 않았습니다. 이는 전적으로 의도적인 설계입니다. ONTAP은 ONTAP이므로 가능한 한 학습 곡선이 거의 없거나 전혀 없어야 합니다. 그리고 이 경우 NetApp AFX는 여전히 ONTAP을 실행하고 있습니다.

관리 – CLI

NetApp AFX의 CLI는 통합 ONTAP의 CLI가 제공하는 것과 거의 동일합니다. 대부분의 명령은 클러스터 수준에서 실행되지만 노드 수준 명령도 실행할 수 있습니다. 최상위 명령 디렉터리와 하위 명령, 그리고 명령의 탭 자동 완성 기능도 그대로 제공됩니다. 또한 모든 CLI 바로 가기도 동일하게 작동합니다(예: `-fields`를 사용한 콘텐츠 필터링).

NetApp AFX CLI의 유일한 실질적인 차이점은 추가된 기능과 제거된 기능(이 문서의 "" 섹션 참조)에 있습니다. 애그리게이트 또는 MetroCluster와 같은 기능이 제거된 경우 해당 CLI 명령은 더 이상 사용할 수 없습니다.

또한 NetApp AFX에 새로운 기능과 성능이 추가됨에 따라 새로운 명령어도 사용할 수 있게 됩니다. 예를 들어, 새로운 "NetApp AI Data Engine(AIDE)" 추가 기능은 백엔드 클러스터 네트워크를 통해 NetApp AFX 클러스터와 직접 상호 작용합니다. 따라서 `dcn` 및 `data-engine` 명령어 디렉터리가 NetApp AFX CLI에 추가됩니다.

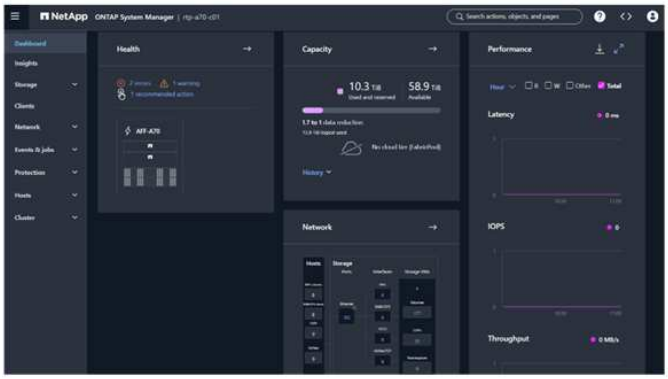
다음은 NetApp AFX 클러스터에서 관리자 권한으로 사용할 수 있는 최상위 명령 디렉터리를 보여줍니다. 새로 추가된 명령은 굵게 표시되어 있습니다.

```
AFX::>
    cluster         data-engine    dcn            event          exit
    history         job            man            metrocluster   network
    qos             redo           rows           run            security
    set             snaplock       snapmirror     statistics     statistics-v1
    storage         system         top            up             volume
    vserver
```

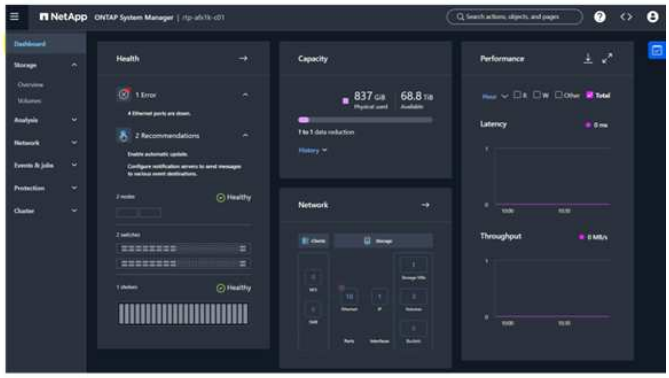
관리 – GUI

System Manager는 여전히 리소스 관리를 위해 NetApp AFX 클러스터와 상호 작용하는 GUI 인터페이스이며, 처음 로그인할 때 통합 ONTAP 시스템에 로그인하지 않았다는 것을 한눈에 알아차리기 어려울 것입니다.

통합 **ONTAP** 및 **NetApp AFX System Manager** 랜딩 페이지 비교



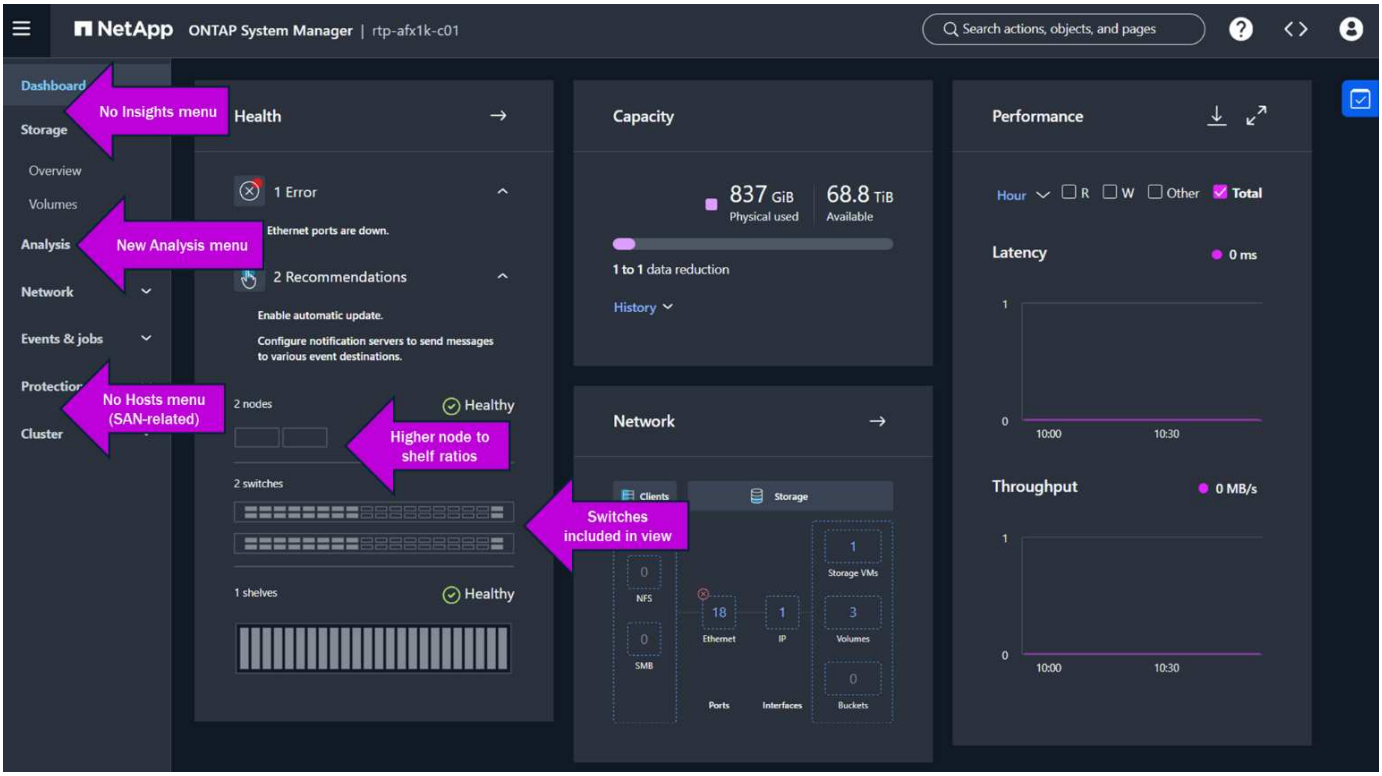
System Manager Dashboard view
Unified ONTAP



System Manager Dashboard view
NetApp AFX

위에서 보시는 바와 같이, 통합 ONTAP과 NetApp AFX의 System Manager에는 뚜렷한 차이점이 많지 않습니다. 하지만 몇 가지 알아챌 만한 단서가 있습니다.

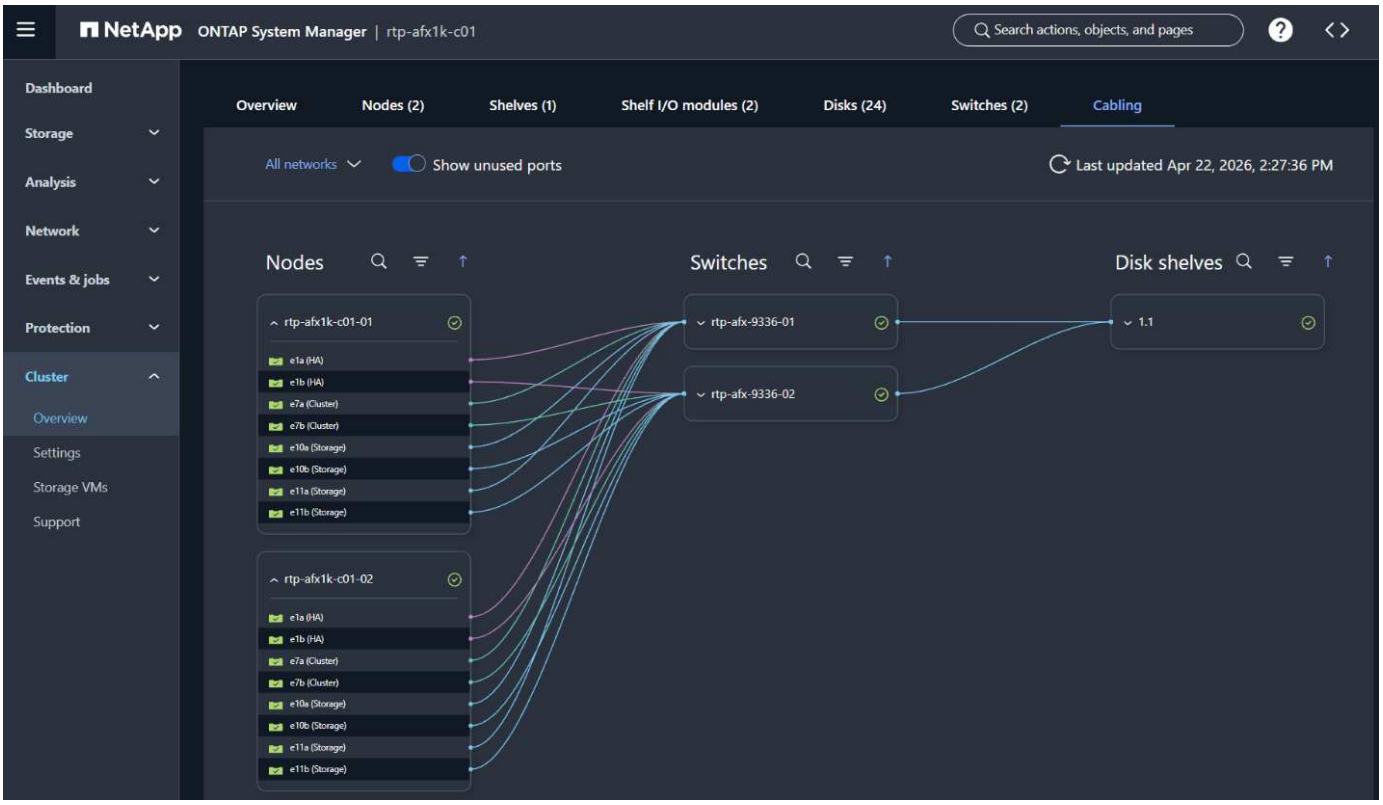
System Manager에서 **NetApp AFX**가 다른 점



메뉴와 대시보드를 자세히 살펴보면 대부분의 내용은 이전과 동일합니다. 볼륨에는 사용량과 총 용량이 표시됩니다. 네트워크 인터페이스에는 포트와 IP 주소가 표시됩니다. SnapMirror에 대한 보호 정책을 구성할 수 있습니다. 하드웨어 보기도 계속 사용할 수 있습니다. 하지만 NetApp AFX는 새로운 케이블링 보기를 제공하여 스토리지 스택 전체에 걸쳐

모든 케이블이 어디에 연결되어 있는지 자세히 확인할 수 있도록 보기 기능을 향상시켰습니다.

NetApp AFX 케이블 연결 보기



REST API

NetApp AFX는 ONTAP REST API 호출의 대부분을 유지하기 위해 상당한 노력을 기울이고 있습니다. 따라서 REST API를 기반으로 자동화 도구를 개발한 경우 대부분의 경우 해당 도구를 계속 사용할 수 있습니다. 주요 예외 사항으로는 애그리게이트, Metrocluster, SAN 및 일부 성능 카운터가 있습니다. 전체 REST API 문서는 NetApp AFX 클러스터의 System Manager에서 https://clus_mgmt_ip/docs/api 경로로 이동하여 확인할 수 있습니다.

오프박스 **ONTAP** 관리 툴

NetApp AFX는 다음과 같은 외부 ONTAP 관리 도구를 일부 지원합니다.

- NetApp System Manager
- NetApp Console
- Grafana Harvest(25.11.0 이상)
- NetApp Trident(25.10 이상)

NetApp AFX는 현재 다음을 지원하지 않습니다.

- NetApp ActiveIQ Unified Manager

네트워킹, 보안 및 운영

NetApp AFX는 일부 분리형 아키텍처에만 적용되는 조정 사항을 제외하고, 통합 ONTAP와

동일한 네트워킹 스택, 보안 기능, 데이터 보호 기술, 무중단 운영, 볼륨 유형을 지원합니다.

네트워킹

NetApp AFX의 네트워킹 스택은 통합 ONTAP와 동일합니다.

- 데이터 LIF는 여전히 내부 및 외부 서비스에 네트워크 주소를 제공하는 데 사용됩니다.
- 각 노드에는 고유한 물리적 포트 및 가상 포트 세트가 있습니다.
- VLAN, ifgroup 및 BGP는 모두 여전히 지원됩니다.
- LIF는 클러스터의 물리적 노드와 포트 간에 페일오버를 수행할 수 있습니다.
- IPspace/브로드캐스트 도메인은 이전과 동일하게 구성되어 있습니다.
- 각 SVM은 자체적인 전용 데이터 네트워크를 가질 수 있습니다.
- 관리 네트워크는 데이터 네트워크와 분리될 수 있습니다.
- 클라이언트 데이터 네트워크는 400GB 네트워킹 지원이 새로 추가된 것 외에는 변경 사항이 없습니다.
- 백엔드 클러스터 스위치는 여전히 NetApp에서 제공하는 "골든 구성" 파일을 통해 구성됩니다.

주요 네트워크 차이점은 다음과 같습니다.

- 백엔드 클러스터 네트워크 포트는 이제 클러스터 스위치에 대한 100GB 연결만 지원합니다.
- 클러스터 스위치는 400GB를 지원하므로 백엔드 노드 연결에는 스위치에서 사용하는 포트 수를 줄이기 위해 4 x 100GB 브레이크아웃 케이블이 사용됩니다.
- 이제 스위치의 새로운 HA VLAN 구성을 통해 백엔드 클러스터 네트워크 전체의 HA 쌍 간에 NVRAM이 미러링됩니다.
- AI Data Engine에 대해 새 DCN 네트워크가 기본적으로 추가됩니다. 이러한 IP 주소는 자동으로 생성되며 필요에 따라 변경할 수 있습니다.

보안

NetApp AFX는 ONTAP를 실행하므로 ONTAP와 동일한 보안을 사용합니다. 모든 암호화 모듈이 동일하므로 인증 프로세스가 완료되면 보안 인증도 동일합니다. NetApp AFX는 통합 ONTAP와 동일한 보안 암호를 지원합니다.

또한 NetApp AFX는 다음을 포함하되 이에 국한되지 않는 통합 ONTAP에서 제공하는 많은 보안 기능을 지원합니다.

- 자율 랜섬웨어 보호
- 안전한 다중 테넌시
- 저장 데이터 암호화(볼륨 암호화) 및 전송 데이터 암호화(TLS 1.3)
- 자체 암호화 드라이브(SED)
- NFS 및 SMB Kerberos 인증 및 암호화
- 다중 관리 검증
- SnapLock

통합 ONTAP이 획득한 인증(및 기타 보안 강화 정보)에 대한 자세한 내용은 다음을 참조하십시오.

- "NetApp 제품 보안"
- "ONTAP 보안 강화 개요"

스냅샷 및 데이터 보호

NetApp AFX는 통합 ONTAP와 동일한 스냅샷 및 복제 기술을 활용하며, 이러한 기능의 작동 방식에 큰 변화는 없습니다. 실제로 AFX는 기존에 익숙한 "규칙 및 구성"를 사용하여 통합 ONTAP 시스템과의 복제를 수행할 수 있습니다.

AFX에서 복제와 관련하여 유일한 예외는 FlexGroup 볼륨을 통합 ONTAP 시스템으로 복제하는 경우입니다. 이 경우 대상 통합 ONTAP 시스템은 고급 용량 균형 조정(Advanced Capacity Balancing)을 지원하기 위해 ONTAP 9.16.1 이상 버전을 실행해야 합니다.

무중단 운영

ONTAP는 볼륨 이동, 업그레이드, 클러스터 유지 관리, 스토리지 페일오버 등과 같은 무중단 운영을 제공합니다. NetApp AFX는 일부 조정을 통해 동일한 무중단 운영을 제공합니다.

- 볼륨 이동은 여전히 중단 없이 진행되지만 더 이상 복사가 필요하지 않습니다.
- 스토리지 페일오버는 여전히 무중단 방식이지만, 초기 페일오버 후에는 클러스터의 모든 남아 있는 노드에 걸쳐 볼륨이 재조정됩니다.
- LIF 마이그레이션은 동일합니다.
- 하드웨어 유지 보수 및 업그레이드는 동일합니다.

볼륨 유형

Unified ONTAP는 다음과 같은 다양한 볼륨 유형을 지원합니다.

- FlexVols
- FlexGroup 볼륨
- FlexCache
- FlexClone
- 객체 버킷

NetApp AFX는 이러한 각 볼륨 유형을 완벽하게 지원할 뿐만 아니라 통합 ONTAP 시스템과 FlexCache 볼륨 간의 완벽한 상호 운용성도 제공합니다.

FlexGroup 볼륨이 AFX 아키텍처를 통해 얻는 이점에 대한 자세한 내용은 "FlexGroup 볼륨 관리 개선 사항"을 참조하십시오.

하드웨어 세부 정보

다음 섹션에서는 NetApp AFX 클러스터 하드웨어에 대한 세부 정보를 다룹니다. NetApp AFX 하드웨어에 대한 최신 정보는 "https://hwu.netapp.com"을 참조하십시오.

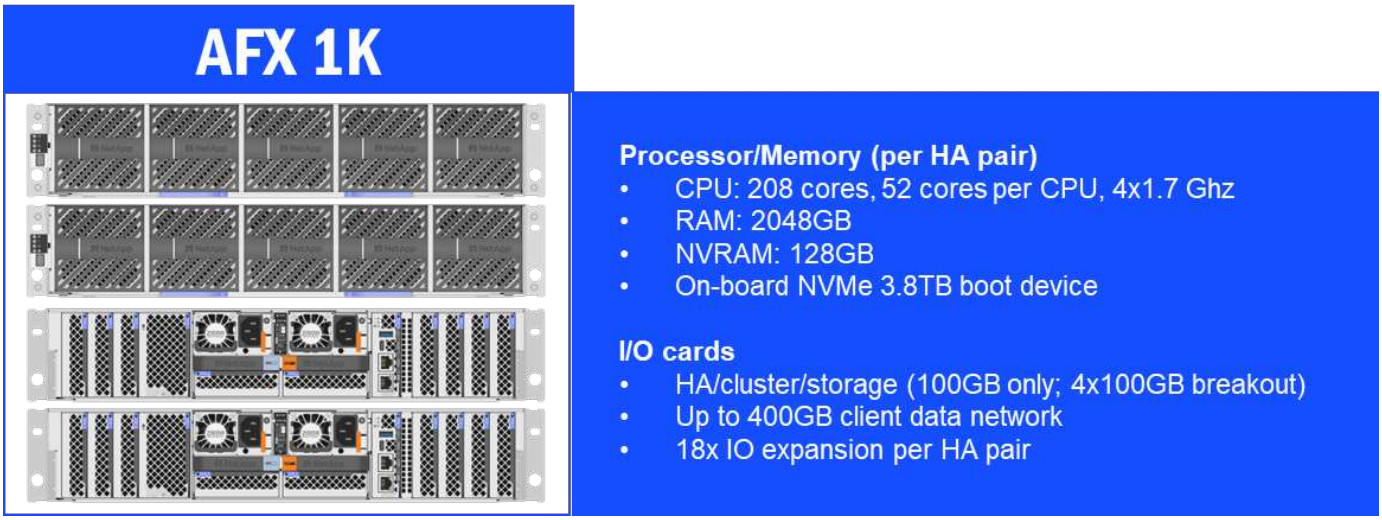
지원되는 **hardware**

NetApp AFX에서 지원하는 하드웨어에 대한 최신 정보는 "https://hwu.netapp.com"을(를) 참조하십시오.

노드

NetApp AFX 노드는 통합 ONTAP 클러스터용으로 제공되는 AFF A1K 모델 노드를 기반으로 합니다. 이 노드에는 스토리지용 온보드 디스크가 없으며, 성능 요구 사항에 따라 노드를 쉽게 추가 및 제거할 수 있도록 모듈식으로 설계되었습니다. 각 노드는 2U의 랙 공간을 차지하며, AFX 클러스터에 추가될수록 성능이 선형적으로 향상됩니다.

NetApp AFX 1K 노드 세부 정보



하드웨어 슬롯

NetApp AFX 1K 노드는 다음과 같은 슬롯 할당을 사용합니다.

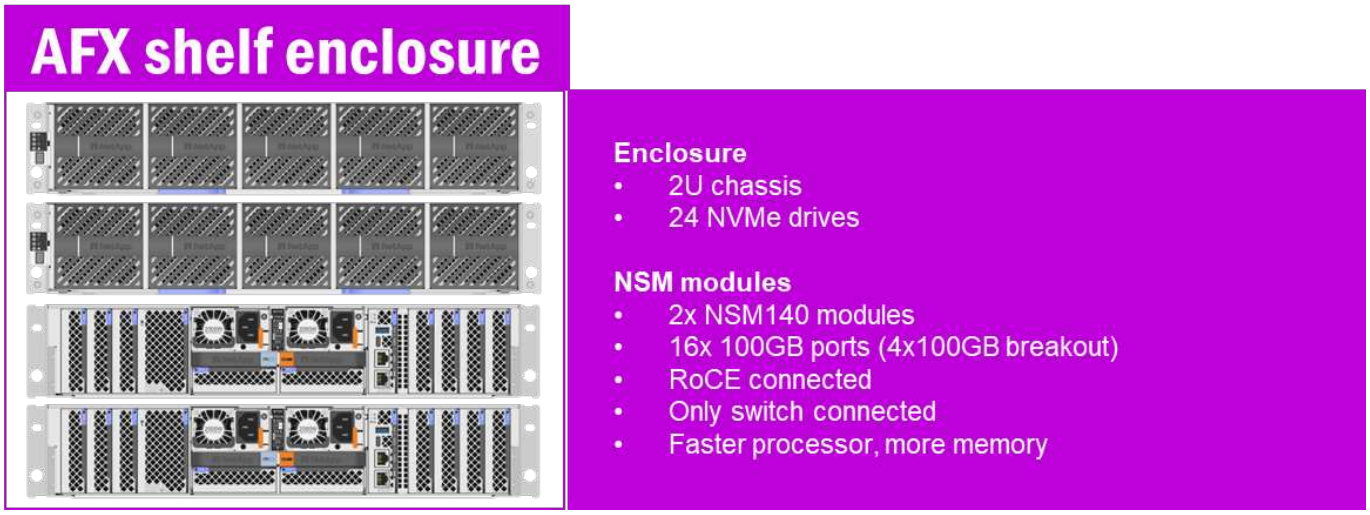
- 슬롯 1은 HA 복제 전용입니다.
- 슬롯 7은 클러스터 복제 전용입니다.
- 슬롯 10과 11은 스토리지 쉘프 통신 전용입니다.

쉘프

NetApp AFX 셸프는 AFF 시스템에서 사용하는 것과 동일한 엔클로저를 사용합니다. AFX 셸프의 주요 차이점은 사용되는 모듈에 있습니다. NSM140 모듈은 향상된 성능 기능을 제공하며 분산형 ONTAP을 가능하게 합니다. 몇 가지 주요 고려 사항은 다음과 같습니다.

- 완전히 채워진 쉘프만 지원됩니다.
- NetApp AFX는 연결 시 쉘프를 자동으로 감지합니다.
- 현재 셸프 제거는 지원되지 않습니다.

NetApp AFX 쉘프 엔클로저 세부 정보

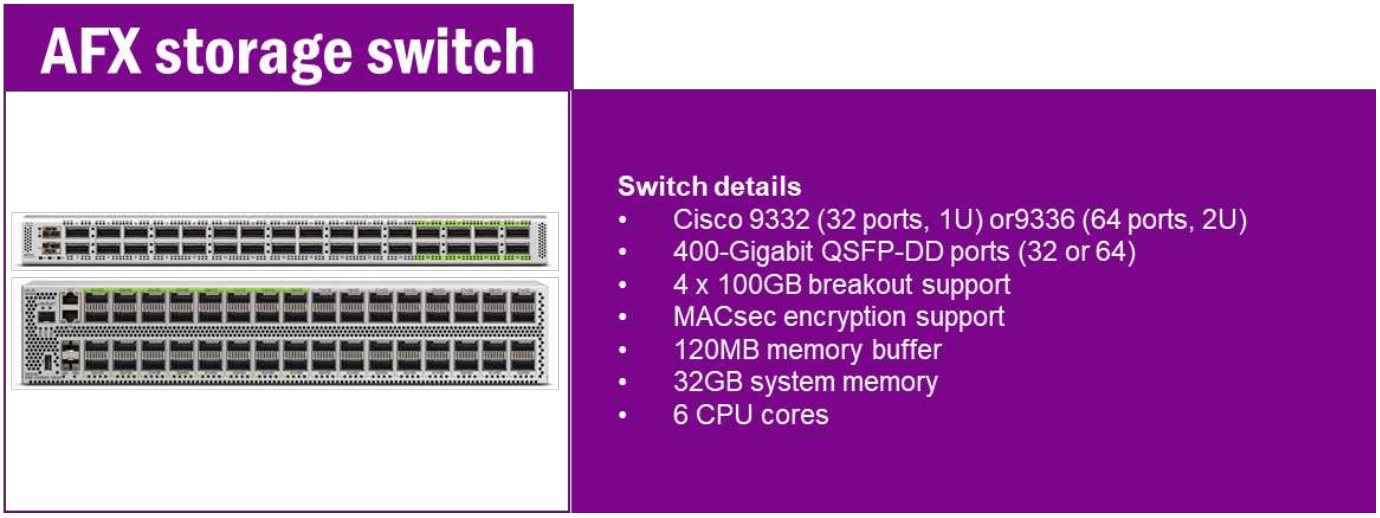


스위치

NetApp AFX는 클러스터 데이터베이스 복제, 원격 데이터 작업, 스토리지 작업 및 NVRAM 미러링과 같은 클러스터 내 통신을 위해 여전히 백엔드 클러스터 스위치를 사용합니다. 기능적으로 통합 ONTAP과 NetApp AFX 클러스터 스위치 간의 유일한 차이점은 다음과 같습니다.

- 400GbE 지원
- 새 HA VLAN
- 자세한 내용은 "Cisco 스위치 데이터 시트"를 참조하십시오.

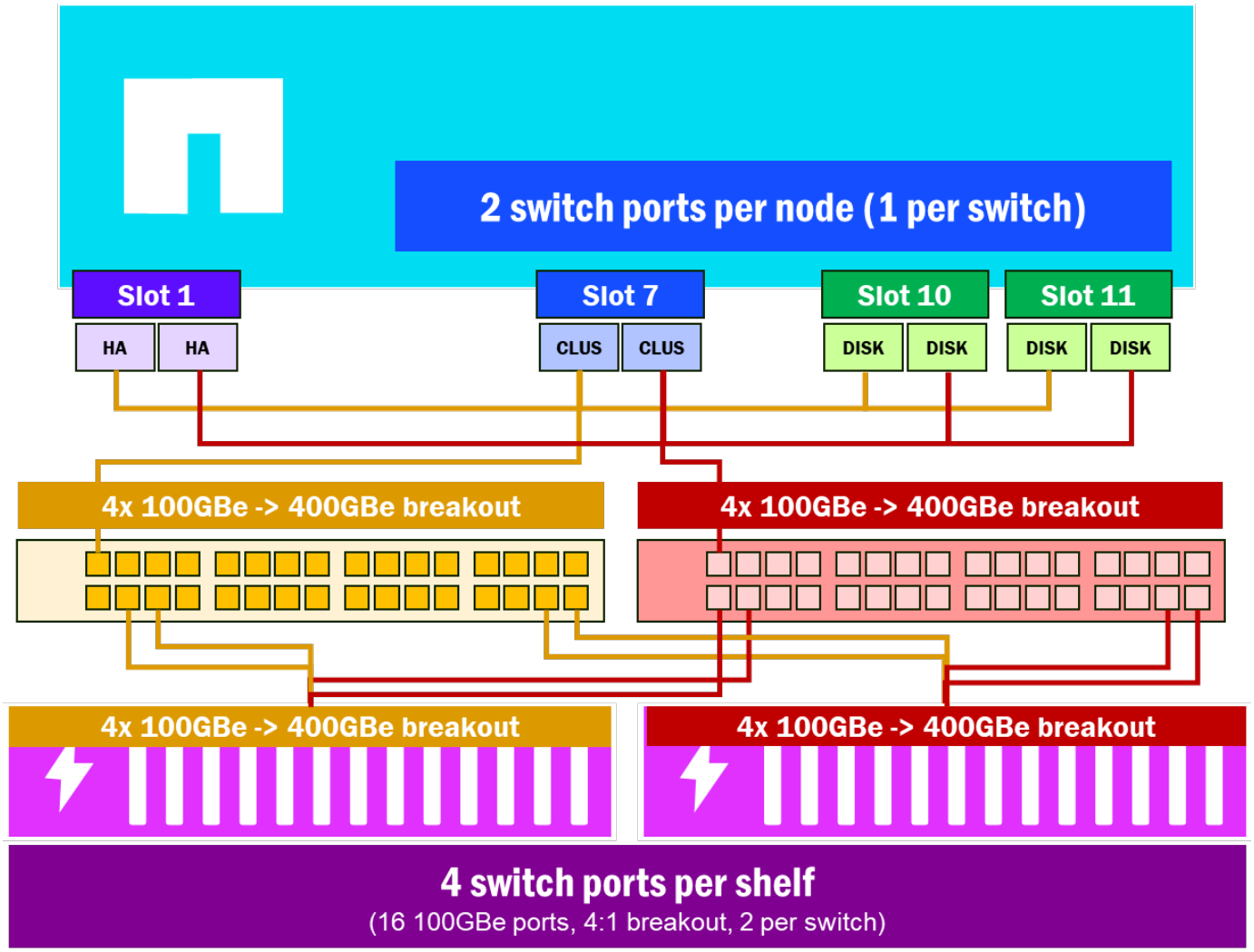
NetApp AFX 클러스터 스위치



클러스터 스위치 연결

NetApp AFX는 주요 아키텍처 개념의 상당 부분을 백엔드 클러스터 스위치에 의존하여 구현합니다. 예를 들어, 클러스터 인터페이스, 스토리지 어댑터, 스토리지 셸프, NVRAM 카드 등은 모두 클러스터 스위치에 연결됩니다. 현재 이러한 인터페이스는 모두 100GB 통신만 지원하는 반면, 스위치는 400GB를 지원합니다. 따라서 100GB 인터페이스는 4 x 100GB 브레이크아웃 케이블을 통해 스위치의 400GB 인터페이스에 연결됩니다. 이러한 방식을 통해 스위치에서 사용하는 포트 수를 줄일 수 있습니다. 예를 들어, 16 x 100GB 스토리지 셸프 모듈 포트는 스위치에서 4개의 포트만 사용하고, 노드의 총 8개 포트는 스위치 포트 2개를 사용합니다.

NetApp AFX 스위치 케이블링



디스크 유형 및 크기

NetApp AFX는 현재 다음과 같은 크기의 NVMe 연결 SSD만 지원합니다.

- 7.6 TB
- 15.3 TB
- 30.1 TB
- 60.6 TB

TLC와 QLC

NetApp AFX는 TLC와 QLC 플래시 유형을 모두 활용할 수 있습니다. 7.6TB 및 15.3TB 드라이브는 TLC 모델이며, 30.1TB 이상의 드라이브는 QLC입니다. 미디어 유형에 관계없이 NVIDIA SuperPod 인증 성능 표준을 충족할 수 있습니다.

NetApp AFX에 사용되는 모든 드라이브는 성능 등급이 지정된 드라이브이며, QLC와 TLC는 읽기 트래픽에서 거의 동일한 성능을 제공합니다. QLC는 쓰기 성능이 TLC에 비해 약간 떨어지며, 쓰기 작업이 많은 워크로드에서는 마모 평준화 현상이 약간 더 많이 발생할 수 있습니다.

성능 수치는 "쉘프별 성능"을 참조하십시오.

사용할 드라이브 유형을 선택할 때는 스토리지가 호스팅할 워크로드와 관련된 성능/용량 밀도 트레이드오프를 고려해야 합니다.

최대값 및 제한값

다음 섹션에서는 NetApp AFX 클러스터의 최대값과 최소값을 통합 ONTAP와 비교하여 설명합니다.

최신 제한 사항은 "Hardware Universe"을 참조하십시오.

NetApp AFX 최대값 및 최소값

제한	통합 **ONTAP**	**NetApp AFX**
볼륨 수(클러스터)	• 30,000(플랫폼에 따라 다름)	• 30,000
애그리게이트 크기	• 800 TB	• 해당 없음
노드 수	• 24	• 8 (9.17.1) • 32 (9.19.1RC1)
총 용량	• 노드 및 드라이브에 따라 다릅니다. 자세한 내용은 "hwu.netapp.com"을 참조하십시오.	• 2PB (9.17.1) • 3PB (9.18.1RC1) • 16PB(9.18.1GA 릴리스) • 20PB (9.19.1RC0) • 32PB (9.19.1RC1)
지원되는 쉘프 수	• HA 쌍당 8개 • 클러스터당 192개	• 클러스터당 12개(9.18.1GA) • 클러스터당 17개(9.19.1RC0) • 클러스터당 25개(9.19.1RC1)(HA 쌍 제한 없음)
지원되는 총 드라이브 수	• HA 쌍당 240 • 2880(노드 24개)	• 클러스터당 288개(쉘프 수 제한 기준, HA 쌍 제한 없음) • 클러스터당 408개(9.19.1RC0) • 클러스터당 600개(9.19.1RC1)
볼륨 크기	• 300TB(FlexVol) • 60PB(FlexGroup)	• 300TB(FlexVol) • 60PB (FlexGroup)*

제한	통합 **ONTAP**	**NetApp AFX**
볼륨당 최대 파일 수	• 20억(FlexVol) • 4천억(FlexGroup)	• 20억(FlexVol) • 4천억(FlexGroup)
디렉터리당 최대 파일 수(기본 320MB maxdirsize 값)	• 약 4백만(FlexVol) • 약 2백만(FlexGroup)	• 약 4백만(FlexVol) • 약 2백만(FlexGroup)
SnapMirror 동시 전송	• 250	• 250
qtree 수	• 4096	• 4096
노드당 최대 TCP 연결 수	• 100,000	• 100,000
노드당 최대 잠금 수	• 300만	• 300만
최대 데이터 인터페이스 수(클러스터)	• 4096	• 4096
최대 구성요소 수 – FlexGroup	• 200	• 200 • 9.19.1 RC1의 512
클러스터 간 LIF의 최대 개수	• 8	• 8
최대 IP 공간 수	• 512	• 512
오리진당 최대 FlexCache 수	• 100	• 100
최대 FlexCache 수(노드)	• 400	• 400

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- Hardware Universe"https://hwu.netapp.com/"
- NetApp AFX 제품 페이지 https://www.netapp.com/afx/
- NetApp AFX: 확장 가능하고 안전한 AI 데이터 인프라 "https://www.netapp.com/blog/afx-scalable-secure-ai-data-infrastructure/"
- NFSv3와 NFSv4.x 중 어떤 것을 선택해야 할까요? 이제 선택이 점점 명확해지고 있습니다… "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Deciding-between-NFSv3-or-NFSv4-x-The-choice-is-getting-clearer"
- NetApp AFX 데이터 시트 "https://www.netapp.com/media/142853-ds-3466-netapp-afx-datasheet.pdf"

ONTAP SnapCenter 기술 보고서

SnapCenter은 애플리케이션 정합성이 보장되는 데이터 보호 및 클론 관리를 위한 유니파이드 플랫폼을 제공합니다. SnapCenter는 애플리케이션 통합 워크플로우를 활용해 백업, 복원, 클론 라이프사이클 관리를 단순화합니다. SnapCenter는 스토리지 기반 데이터 관리를 활용하여 성능과 가용성을 향상하고 테스트 및 개발 시간을 단축합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "SnapCenter"설명합니다.

Oracle용 SnapCenter

"TR-4700: Oracle 데이터베이스 모범 사례를 위한 SnapCenter 플러그인"
NetApp SnapCenter는 Oracle의 일관된 데이터 보호를 위한 확장 가능한 통합 플랫폼으로, 중앙 집중식 제어 및 감독을 통해 복잡한 작업을 자동화합니다. SnapCenter를 사용하여 Oracle 데이터베이스를 구축하는 데 권장되는 방법에 대해 알아보십시오.

"TR-4964: SnapCenter 서비스를 사용하여 Oracle 데이터베이스 백업, 복원 및 클론 복제" Amazon FSx for ONTAP 스토리지 및 EC2 컴퓨팅 인스턴스에 구축된 Oracle 데이터베이스를 백업, 복원 및 클론 복제하도록 SnapCenter 서비스를 설정하는 방법에 대해 알아보십시오. SnapCenter 서비스는 설정 및 사용이 훨씬 간편하지만 SnapCenter 인터페이스를 통해 사용할 수 있는 주요 기능을 제공합니다.

Microsoft SQL Server용 SnapCenter

"TR-4714: NetApp SnapCenter를 사용하는 Microsoft SQL Server의 모범 사례"
SnapCenter를 사용하여 NetApp 스토리지에 Microsoft SQL Server를 성공적으로 구축하여 데이터를 보호하는 방법에 대해 알아보십시오.

Microsoft Exchange Server용 SnapCenter

"TR-4681: NetApp SnapCenter를 사용하는 Microsoft Exchange Server에 대한 모범 사례"
데이터 보호를 위해 SnapCenter를 사용하여 NetApp 스토리지에 Microsoft Exchange Server를 성공적으로 구축하는 방법에 대해 알아보십시오.

SAP HANA용 SnapCenter

"TR-4614: SnapCenter를 통한 SAP HANA 백업 및 복구" SnapCenter는 SAP HANA 및 기타 데이터베이스의 애플리케이션 정합성이 보장되는 데이터 보호를 위한 확장 가능한 통합 플랫폼입니다. SnapCenter는 중앙 집중식 제어 및 감독을 지원하면서 사용자가 애플리케이션별 백업, 복원 및 클론 작업을 관리할 수 있는 기능을 위임합니다. 데이터베이스 및 스토리지 관리자는 SnapCenter를 사용하여 다양한 애플리케이션과 데이터베이스의 백업, 복원, 클론 복제 작업을 관리하는 단일 툴에 대해 알아보십시오.

"TR-4926: NetApp ONTAP용 Amazon FSx 기반 SAP HANA - SnapCenter를 통한 백업 및 복구" Amazon FSx for NetApp ONTAP 및 SnapCenter에서 SAP HANA 데이터 보호를 위한 권장 사례에 대해 알아보십시오. 이 플레이북에서는 SnapCenter 개념, 구성 권장사항, 구성, 백업 작업, 복원 및 복구 작업을 수행할 수 있습니다.

"TR-4667: SnapCenter를 사용하여 SAP HANA 시스템 복사 및 클론 작업 자동화" SnapCenter 스토리지 클론 생성과 사전 클론 생성 및 클론 생성 후 작업을 유연하게 정의하는 옵션을 통해 SAP 기반 관리자는 SAP 시스템 복사, 클론 복제 또는 업데이트 작업을 가속화하고 자동화할 수 있습니다. 지금 알아보기 운영 스토리지 또는 2차 스토리지에서

SnapCenter 스냅샷 백업을 선택하면 논리적 손상, 재해 복구 테스트 또는 SAP QA 시스템 업데이트 등 가장 중요한 사용 사례를 해결할 수 있습니다.

"TR-4719: SnapCenter를 통해 SAP HANA 시스템 복제 백업 및 복구"
SAP HANA 시스템 복제 환경에서 SnapCenter 기술과 SAP HANA 플러그인을 사용하여 백업 및 복구를 수행하는 방법에 대해 알아보십시오.

"TR-4667: SnapCenter를 사용하여 SAP HANA 시스템 복사 및 클론 작업 자동화" 스토리지 계층에서 애플리케이션 정합성이 보장된 NetApp Snapshot 백업을 생성하는 기능은 시스템 복사본 및 시스템 클론 작업의 기초입니다. 스토리지 기반 스냅샷 백업은 SAP HANA용 NetApp SnapCenter 플러그인과 SAP HANA 데이터베이스에서 제공하는 인터페이스를 사용하여 생성됩니다. SnapCenter는 SAP HANA 백업 카탈로그에 Snapshot 백업을 등록하여 복원 및 복구뿐만 아니라 클론 복제 작업에 백업을 사용할 수 있습니다.

SnapCenter 강화 가이드

"TR-4957: NetApp SnapCenter 보안 강화 가이드"
조직에서 정보 시스템 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 SnapCenter를 구성하는 방법을 알아보십시오.

ONTAP 계층화 기술 보고서

FabricPool 데이터 계층화 솔루션을 사용하면 스토리지 효율성을 위해 애플리케이션을 재설계하는 부담은 줄이면서 플래시 시스템의 전반적인 사용자 환경을 개선할 수 있습니다. FabricPool는 스토리지 설치 공간과 시스템 환경의 관련 비용을 줄여 줍니다. 활성 데이터는 고성능 SSD에 유지됩니다. 비활성 데이터는 스토리지 효율성을 유지하면서 저비용 오브젝트 스토리지로 계층화되어 있습니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "ONTAP FabricPool"설명합니다.

"TR-4598: FabricPool 모범 사례"
FabricPool의 기능, 요구사항, 구축 및 권장 사례에 대해 알아보십시오.

"TR-4826: NetApp FabricPool with StorageGRID 권장 가이드"
StorageGRID를 ONTAP 구성 요소 FabricPool의 용량 계층으로 구축 및 사이징하는 데 권장되는 Best Practice에 대해 알아보십시오. 또한 StorageGRID를 사용할 때의 핵심 기능, 요구사항, 구축 및 권장 사항도 다룹니다.

"TR-4695: NetApp FabricPool를 통한 데이터베이스 스토리지 계층화"
Oracle RDBMS(관계형 데이터베이스 관리 시스템)를 비롯한 다양한 데이터베이스를 사용하는 FabricPool의 이점과 구성 옵션에 대해 알아봅니다.

ONTAP 가상화 기술 보고서

NetApp 가상화 솔루션은 서버에서 최대의 가치를 제공하는 데 도움이 됩니다. 혁신적인 고성능 ONTAP 플래시 시스템을 기반으로 하는 응답 속도가 빠른 가상 서버 인프라를 통해 데이터에 훨씬 더 빠르게 액세스할 수 있습니다. 가상 인프라가 수 페타바이트의 데이터까지 중단 없이 확장됨에 따라 여러 워크로드에 대한 공유 액세스에 필요한 성능을 제공할 수 있습니다. ONTAP은 주요 파트너십, 구축 지침, 애플리케이션 통합, 우수한 설계를 통해 가상 서버 인프라 구축을 간소화하고 복잡성을 줄이도록 지원합니다. ONTAP는 온프레미스와 클라우드 모두에서 강력한 가상화 환경을 위한 권장 모범 사례와 솔루션을 제공합니다.

이러한 기술 보고서는 제품 설명서에 대해 자세히 "VMware vSphere용 ONTAP 툴"설명합니다.

"TR-4597: ONTAP용 VMware vSphere" ONTAP은 거의 20년 동안 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션으로 자리매김해 왔으며, 관리를 단순화하는 동시에 비용을 절감할 수 있는 혁신적인 기능을 계속해서 추가하고 있습니다. 이 문서에서는 구축을 간소화하고 위험을 줄이며 관리를 단순화하는 최신 제품 정보 및 권장 사례를 비롯하여 vSphere용 ONTAP 솔루션에 대해 소개합니다.

"TR-4400: NetApp ONTAP를 통해 VVOL(VMware vSphere 가상 볼륨)을 이동합니다" ONTAP은 20년 이상 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션으로 자리매김했으며, 비용을 절감하면서 관리를 간소화하는 혁신적인 기능을 지속적으로 추가하고 있습니다. 본 문서에서는 최신 제품 정보 및 사용 사례와 권장 사례 및 기타 정보를 비롯하여 VMware VVOL(vSphere 가상 볼륨)을 위한 ONTAP 기능을 다루며 구축 간소화 및 오류 감소를 위한 방법에 대해 설명합니다.

"TR-4900: NetApp ONTAP를 사용하는 VMware 사이트 복구 관리자" ONTAP은 2002년에 현대적인 데이터 센터에 선보인 이후 VMware vSphere 환경을 위한 업계 최고의 스토리지 솔루션으로, 관리 작업을 간소화하는 동시에 비용을 절감할 수 있는 혁신적인 기능을 지속적으로 추가하고 있습니다. 이 문서에서는 VMware의 업계 최고 수준의 DR(재해 복구) 소프트웨어인 VMware SRM(Site Recovery Manager)을 위한 ONTAP 솔루션을 소개합니다. 최신 제품 정보와 권장 사례를 통해 배포를 간소화하고 위험을 줄이며 지속적인 관리를 단순화합니다.

"ONTAP 및 vSphere 자동화 소개" VMware ESX를 처음 접하는 날부터 자동화는 VMware 환경을 관리하는 데 있어 핵심적인 역할을 했습니다. 코드로 인프라를 구축하고 프라이빗 클라우드 운영으로 사례를 확장하는 기능은 확장, 유연성, 셀프 프로비저닝 및 효율성에 관한 문제를 해결하는 데 도움이 됩니다. 이 문서에서는 ONTAP 및 VMware vSphere 환경의 자동화를 위한 ONTAP 솔루션을 소개합니다.

"WP-7353: VMware vSphere용 ONTAP 툴 - 제품 보안" 이 문서에서는 VMware vSphere 9.X용 ONTAP 툴을 제품 환경의 기존 위협과 새로운 위협으로부터 보호하는 데 사용되는 기술과 기술에 대해 설명합니다.

"WP-7355: SnapCenter 플러그인 VMware vSphere - 제품 보안" 이 문서에서는 VMware vSphere 4.X용 NetApp SnapCenter 플러그인을 제품 환경의 기존 위협과 새로운 위협으로부터 보호하는 데 사용되는 기술과 기술에 대해 설명합니다.

"TR-4568: Windows Server에 대한 NetApp 배포 지침 및 스토리지 모범 사례" Microsoft Windows Server는 네트워킹, 보안, 가상화, 클라우드, 가상 데스크톱 인프라, 액세스 보호, 정보 보호, 웹 서비스, 응용 프로그램 플랫폼 인프라 등을 포함하는 엔터프라이즈급 운영 체제입니다. 이 문서에서는 Microsoft Windows를 중심으로 배포를 간소화하고 위험을 줄이며 관리를 단순화하는 최신 제품 정보와 권장 사례를 비롯하여 Hyper-V 가상화 기술에 특히 중점을 두고 있습니다.

법적 고지

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.

ONTAP

"ONTAP 9.16.1 참고 사항" "ONTAP 9.16.0 참고 사항" "ONTAP 9.15.1 참고 사항" "ONTAP 9.15.0 참고 사항" "ONTAP 9.14.1에 대한 고지 사항" "ONTAP 9.14.0에 대한 고지 사항" "ONTAP 9.13.1 참고 사항" "ONTAP 9.12.1에 대한 고지 사항" "ONTAP 9.12.0 참고 사항" "ONTAP 9.11.1에 대한 고지 사항" "ONTAP 9.10.1에 대한 고지 사항" "ONTAP 9.10.0에 대한 고지 사항" "ONTAP 9.9.1에 대한 참고 사항" "ONTAP 9.8에 대한 고지 사항" "ONTAP 9.7의 알림 사항" "ONTAP 9.6 고지 사항" "ONTAP 9.5 알림" "ONTAP 9.4 고지 사항" "ONTAP 9.3 공지 사항" "ONTAP 9.2 관련 고지 사항" "ONTAP 9.1에 대한 참고 사항"

MetroCluster IP 구성을 위한 ONTAP 중재자

"9.9.1 MetroCluster IP 구성을 위한 ONTAP mediator에 대한 알림" "9.8 MetroCluster IP 구성에 대한 ONTAP 중재자에 대한 알림" "9.7 MetroCluster IP 구성에 대한 ONTAP 중재자에 대한 알림"