ONTAP Technische Berichte

ONTAP Technical Reports

NetApp
August 07, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap-technical-reports/index.html on August 07, 2026. Always check docs.netapp.com for the latest.

Inhalt

ONTAP Technische Berichte . . . 1
Technische Berichte zu ONTAP und Applikationen und Datenbanken . . . 2
Microsoft SQL Server . . . 2
MySQL . . . 2
Oracle . . . 2
PostgreSQL . . . 4
SAP HANA . . . 4
Epic . . . 4
Technische Berichte zur Business Continuity . . . 5
SnapMirror Active Sync (ehemals SM-BC) . . . 5
MetroCluster . . . 5
Technische Berichte zur ONTAP Datensicherung und Disaster Recovery . . . 6
SnapMirror . . . 6
Applikationen und Infrastruktur mit SnapMirror . . . 6
Cyber-Vault: ONTAP . . . 6
Technische Berichte zu Volumes von ONTAP FlexCache und FlexGroup . . . 8
FlexCache . . . 8
FlexCache Write-Back . . . 8
FlexGroup Volumes . . . 8
Technische Berichte zum ONTAP Networking . . . 9
Routing . . . 9
Name Services . . . 9
NFS . . . 10
ONTAP NFS technische Berichte . . . 10
NFS . . . 10
Multi-Protokoll . . . 10
NFS über TLS . . . 10
NFS über TLS Übersicht . . . 10
Anwendungsfälle und Arbeitslasten . . . 11
Architektur . . . 12
NFS über TLS konfigurieren . . . 15
Sicherheit . . . 25
NFS über TLS überwachen . . . 27
Performance . . . 29
Interoperabilität und Grenzen . . . 30
Technische Berichte zum ONTAP SAN . . . 33
Sicherheit . . . 34
Technische Berichte zur Sicherheit von ONTAP . . . 34
Cyber-Vault: ONTAP . . . 34
Ransomware . . . 34
Zero Trust . . . 34
Multi-Faktor-Authentifizierung . . . 35
Mandantenfähigkeit . . . 35

Standards . . . 35
Attributbasierte Zugriffssteuerung . . . 35
NetApp Lösung für Ransomware . . . 35
Ransomware und das Datensicherungsportfolio von NetApp . . . 35
SnapLock und manipulationssichere Snapshots für den Schutz vor Ransomware . . . 38
FPolicy Dateisperrung . . . 39
Data Infrastructure Insights Speicher-Workload-Sicherheit . . . 40
In NetApp ONTAP integrierte, KI-basierte Erkennung und Reaktion . . . 41
Luftgewindelter WORM-Schutz mit Cyber-Vaulting in ONTAP . . . 42
Digital Advisor Ransomware-Schutz . . . 43
Umfassende Ausfallsicherheit mit NetApp Ransomware-Schutz . . . 44
NetApp und Zero Trust . . . 45
NetApp und Zero Trust . . . 45
Entwerfen eines datenorientierten Ansatzes für Zero Trust mit ONTAP . . . 47
Kontrollmechanismen für die Sicherheitsautomatisierung und Orchestrierung von NetApp außerhalb von ONTAP . . . 51
Zero-Trust- und Hybrid-Cloud-Implementierungen . . . 52
Attributbasierte Zugriffssteuerung . . . 53
Attributbasierte Zugriffssteuerung mit ONTAP . . . 53
Ansätze zur attributbasierten Zugriffssteuerung (ABAC) in ONTAP . . . 53
Verstärkte Sicherheit . . . 67
Leitfäden zur ONTAP-Erhöhung der Sicherheit . . . 67
Härteführungen . . . 67
Richtlinien zur Erhöhung der Sicherheit durch ONTAP . . . 67
Übersicht über die Erhöhung der Sicherheit durch ONTAP . . . 67
Validierung von ONTAP-Images . . . 68
Lokale Storage-Administratorkonten . . . 68
Methoden für die . . . 85
Autonomer Ransomware-Schutz von ONTAP . . . 91
Prüfung von Storage-Verwaltungssystemen . . . 91
Storage-Verschlüsselung in ONTAP . . . 93
Datenreplizierung Verschlüsselung . . . 96
IPsec-Verschlüsselung von aktiven Daten . . . 97
FIPS-Modus und TLS- und SSL-Management in ONTAP . . . 98
Erstellen Sie ein CA-signiertes digitales Zertifikat . . . 101
Online-Protokoll für den Zertifikatsstatus . . . 101
SSHv2-Management . . . 101
NetApp AutoSupport . . . 103
Network Time Protocol . . . 103
Lokale NAS-Dateisystemkonten (CIFS-Arbeitsgruppe) . . . 104
NAS-Filesystem-Auditing . . . 104
Konfigurieren und aktivieren Sie das CIFS-SMB-Signing and Sealing . . . 106
NFS-Sicherung . . . 107
Aktivieren Sie Lightweight Directory Access Protocol Signing and Sealing . . . 109
NetApp FPolicy erstellen und verwenden . . . 110

Sicherheitsmerkmale von LIF-Rollen in ONTAP . . . 112
Protokoll- und Portsicherheit . . . 113
Technische Berichte zu ONTAP NAS . . . 117
ONTAP S3 . . . 117
ONTAP SMB Technical Reports . . . 118
SMB . . . 118
Multi-Protokoll . . . 118
Speichersysteme . . . 119
AFX . . . 119
NetApp AFX-Übersicht: Erfahren Sie mehr über NetApp AFX . . . 119
Was ist neu in NetApp AFX . . . 123
Wie sich die NetApp AFX-Architektur von Unified ONTAP unterscheidet . . . 123
Performance . . . 142
Management-Tools . . . 150
Netzwerk, Sicherheit und Betrieb . . . 153
Hardware-Details . . . 155
Höchstwerte und Grenzwerte . . . 159
Wo finde ich weitere Informationen . . . 160
Technische Berichte von ONTAP SnapCenter . . . 161
SnapCenter für Oracle . . . 161
SnapCenter für Microsoft SQL Server . . . 161
SnapCenter für Microsoft Exchange Server . . . 161
SnapCenter für SAP HANA . . . 161
SnapCenter-Härtungsleitfaden . . . 162
Technische Berichte zum ONTAP Tiering . . . 163
Technische Berichte zur ONTAP Virtualisierung . . . 164
Rechtliche Hinweise . . . 166
Urheberrecht . . . 166
Marken . . . 166
Patente . . . 166
Datenschutzrichtlinie . . . 166
Open Source . . . 166
ONTAP . . . 166
ONTAP Mediator für MetroCluster IP-Konfigurationen . . . 166

ONTAP Technische Berichte

Technische Berichte zu ONTAP und Applikationen und Datenbanken

ONTAP ist die Grundlage für Datenmanagement und Datensicherung für zahlreiche Enterprise-Applikationen und Datenbanktechnologien. Die folgenden technischen Berichte enthalten Anleitungen zu von NetApp empfohlenen Vorgehensweisen und Implementierungsverfahren für Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA und Epic.

Microsoft SQL Server

SQL Server bildet die Grundlage der Microsoft Datenplattform. Es bietet geschäftskritische Performance mit in-Memory-Technologien und schnelleren Einblick in alle Daten – lokal und in der Cloud.

"Best Practice für Microsoft SQL Server mit ONTAP" Erfahren Sie, wie Storage-Administratoren und Datenbankadministratoren Microsoft SQL Server auf ONTAP Storage erfolgreich bereitstellen können.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4590: Best Practice Guide for Microsoft SQL Server with ONTAP.*

"TR-4976: Virtualisierte Microsoft SQL Server Performance auf NetApp AFF Systemen Der A-Series und C-Series"
Erfahren Sie mehr über die Performance-Eigenschaften von Microsoft SQL Server mit NetApp AFF Systemen Der A- und C-Serie sowie über die Auswahl des richtigen Systems für die Workload-Anforderungen.

"TR-4714: Best Practices für Microsoft SQL Server mit SnapCenter"
Erfahren Sie mehr darüber, wie Sie Microsoft SQL Server erfolgreich auf ONTAP Storage mit SnapCenter Technologie zur Datensicherung implementieren.

MySQL

Dieses Dokument beschreibt die Konfigurationsanforderungen und bietet Anleitung zur Optimierung und Storage-Konfiguration für die Implementierung von MySQL auf ONTAP.

"Best Practices für MySQL Datenbanken auf NetApp ONTAP" MySQL und seine Varianten, darunter MariaDB und Percona, sind weit verbreitet für viele Unternehmensanwendungen. Diese Anwendungen reichen von globalen Websites sozialer Netzwerke und massiven E-Commerce-Systemen bis hin zu SMB-Hosting-Systemen mit Tausenden von Datenbankinstanzen. Erfahren Sie mehr über die Konfigurationsanforderungen und Anleitungen zur Optimierung und Storage-Konfiguration für die Implementierung von MySQL auf ONTAP.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4722: MySQL Database on NetApp ONTAP Best Practices.*

Oracle

ONTAP wurde für Oracle Datenbanken entwickelt. Seit Jahrzehnten ist ONTAP für die speziellen Anforderungen relationaler Datenbank-I/O optimiert. Es wurden mehrere ONTAP-Funktionen speziell dafür entwickelt, die Anforderungen von Oracle Datenbanken zu bedienen – und sogar auf Wunsch von Oracle Inc. Selbst.

"Oracle-Datenbanken auf ONTAP" Erfahren Sie, wie Storage-Administratoren und Datenbankadministratoren Oracle auf ONTAP Storage erfolgreich einsetzen können, und lernen Sie dabei empfohlene Vorgehensweisen kennen.

"Oracle Datensicherung mit ONTAP" Informieren Sie sich über empfohlene Vorgehensweisen, mit denen Storage-Administratoren und Datenbankadministratoren erfolgreich Backups, Recoverys, Replizierungen und Disaster Recovery für Oracle auf ONTAP Storage durchführen können.

"Oracle Disaster Recovery mit ONTAP" Erfahren Sie mehr über empfohlene Verfahren, Testverfahren und andere Überlegungen für den Betrieb von Oracle-Datenbanken auf einer MetroCluster und SnapMirror Business Continuity.

"Migration von Oracle Datenbanken auf ONTAP Storage-Systeme" Erfahren Sie mehr über die allgemeinen Überlegungen bei der Planung einer Migrationsstrategie, die drei verschiedenen Ebenen, auf denen die Datenverschiebung stattfindet, und gehen Sie auf einige der verschiedenen verfügbaren Verfahren ein.

Die oben aufgeführte Dokumentation ersetzt diese zuvor veröffentlichten technischen Berichte *TR-3633: Oracle Databases on ONTAP; TR-4591: Oracle Data Protection: Backup, Recovery, Replizierung; TR-4592: Oracle on MetroCluster; und TR-4534: Migration von Oracle Databases to NetApp Storage Systems*

"TR-4969: Performance von Oracle Database auf AFF A-Series und C-Series"
ONTAP ist eine leistungsstarke Datenmanagementplattform mit nativen Funktionen, die Inline-Komprimierung, unterbrechungsfreie Hardware-Upgrades und die Möglichkeit zum Import einer LUN aus einem fremden Storage-Array umfassen. Bis zu 24 Nodes können in einem Cluster zusammengefasst werden und gleichzeitig Daten über die Protokolle Network File System (NFS), Server Message Block (SMB), iSCSI, Fibre Channel (FC) und Nonvolatile Memory Express (NVMe) bereitstellen. Zudem bildet die Snapshot Technologie die Grundlage für die Erstellung von Zehntausenden von Online-Backups und vollständig einsatzbereiten Datenbankklonen. Neben den umfassenden Funktionen von ONTAP gibt es eine Vielzahl von Benutzeranforderungen, darunter Datenbankgröße, Performance-Anforderungen und Datensicherung. Erfahren Sie mehr über die Performance von Bare Metal-Datenbanken mit AFF Storage-Systemen, einschließlich Der A-Series und C-Series, und es werden sowohl Maximalwerte als auch der praktische Unterschied zwischen den beiden AFF Optionen abgedeckt.

"TR-4971: Virtualisierte Oracle Datenbank-Performance auf AFF A-Series und C-Series"
ONTAP ist eine leistungsstarke Datenmanagementplattform mit nativen Funktionen, die Inline-Komprimierung, unterbrechungsfreie Hardware-Upgrades und die Möglichkeit zum Import einer LUN aus einem fremden Storage-Array umfassen. Bis zu 24 Nodes können in einem Cluster zusammengefasst werden und gleichzeitig Daten über die Protokolle Network File System (NFS), Server Message Block (SMB), iSCSI, Fibre Channel (FC) und Nonvolatile Memory Express (NVMe) bereitstellen. Zudem bildet die Snapshot Technologie die Grundlage für die Erstellung von Zehntausenden von Online-Backups und vollständig einsatzbereiten Datenbankklonen. Neben den umfassenden Funktionen von ONTAP gibt es eine Vielzahl von Benutzeranforderungen, darunter Datenbankgröße, Performance-Anforderungen und Datensicherung. Erfahren Sie mehr über die virtualisierte Datenbank-Performance bei Verwendung von AFF Storage-Systemen, einschließlich A-Series und C-Series, und es werden sowohl Maximalwerte als auch die praktischen Unterschiede zwischen den beiden AFF Optionen behandelt.

"TR-4695: Datenbank-Storage-Tiering mit FabricPool"
Informieren Sie sich über die Vorteile und Konfigurationsoptionen von FabricPool mit unterschiedlichen Datenbanken, wie etwa dem relationalen Datenbankmanagementsystem (RDBMS) von Oracle.

"TR-4899: Transparenter Applikations-Failover für Oracle Database mit SnapMirror Active Sync" SnapMirror Active Sync (ehemals SM-BC) und Oracle Real Application Cluster (RAC) sorgen bei Standortausfällen und echten Ausfällen für transparentes Applikations-Failover (TAF) und Continuity. Erfahren Sie mehr über die

Konfigurationsanleitungen und empfohlene Vorgehensweisen für ein AFF Storage-Array mit SnapMirror Active Sync als Storage-Komponente von Oracle RAC.

"TR-4876:Best Practices für Oracle Mandantenfähigkeit mit ONTAP und Implementierung"
Erfahren Sie mehr über die empfohlenen Vorgehensweisen zur Bereitstellung, zum Management und zur Sicherung von mandantenfähigen Oracle Datenbanken durch die Verwendung von ONTAP Storage. So können Sie die Vorteile der mandantenfähigen Oracle Datenbanken und der Funktionen der ONTAP Software maximieren.

PostgreSQL

PostgreSQL wird mit Varianten wie PostgreSQL, PostgreSQL Plus und EDB Postgres Advanced Server (EPAS) geliefert. PostgreSQL wird typischerweise als Back-End-Datenbank für Multi-Tier-Applikationen implementiert. NetApp ONTAP ist eine ausgezeichnete Wahl für die Ausführung von PostgreSQL-Datenbanken aufgrund seiner Zuverlässigkeit, seiner hohen Performance und seiner effizienten Datenmanagementfunktionen.

"Best Practices für PostgreSQL-Datenbanken auf ONTAP" PostgreSQL wird mit Varianten wie PostgreSQL, PostgreSQL Plus und EDB Postgres Advanced Server (EPAS) geliefert. PostgreSQL wird typischerweise als Back-End-Datenbank für Multi-Tier-Applikationen implementiert. Es wird von gängigen Middleware-Paketen (wie PHP, Java, Python, Tcl/TK, ODBC, Und JDBC) und war in der Vergangenheit eine beliebte Wahl für Open-Source-Datenbankmanagementsysteme. Erfahren Sie mehr über die Konfigurationsanforderungen und Anleitungen zur Optimierung und Storage-Konfiguration für die Implementierung von PostgreSQL auf ONTAP.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4770: PostgreSQL Database on ONTAP Best Practices*.

SAP HANA

"SAP HANA Datenbanklösungen auf ONTAP" Best Practices für die Konfiguration, Verwaltung und Automatisierung von SAP-Lösungen finden Sie auf der Seite NetApp SAP-Lösungen.

Epic

"Epic auf ONTAP Best Practices" Ein Leitfaden, der die Best Practices für die Implementierung von Epic On-Premises und in der Cloud erläutert und gleichzeitig die Konfigurationsstandards für eine ordnungsgemäße Implementierung auf ONTAP erfüllt.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-3923: NetApp Best Practices for Epic*.

Technische Berichte zur Business Continuity

NetApp bietet eine breite Palette an Lösungen, die Ihre Performance kostengünstig optimieren, indem Ihre Applikationen und Daten effizienter gespeichert werden. Datensicherung, Replizierung und kontinuierliche Verfügbarkeit: Das ONTAP Datenmanagement vereinfacht die Datensicherung, da alle Richtlinien für das Storage-Management nur einmal konfiguriert werden und dann von selbst genutzt werden können. Gleichzeitig sichern MetroCluster und SnapMirror die aktive Synchronisierung.

Diese technischen Berichte enthalten eine weitere Erweiterung der "ONTAP SnapMirror Active Sync" und "ONTAP MetroCluster" Produktdokumentation.

SnapMirror Active Sync (ehemals SM-BC)

"TR-4878: SnapMirror Active Sync" SnapMirror Active Sync ist eine kontinuierlich verfügbare Storage-Lösung mit Granularität auf Applikationsebene, die für ONTAP verfügbar ist, die auf AFF- oder ASA-Storage-Systemen (All SAN Array) ausgeführt werden, um die RPO 0- und RTO 0-Anforderungen der kritischsten Business-Applikationen zu erfüllen.

MetroCluster

"TR-4705: NetApp MetroCluster Lösungsarchitektur und Design"
In diesem Dokument werden allgemeine Architektur- und Designkonzepte für MetroCluster Funktionen in ONTAP beschrieben.

MetroCluster IP

"TR-4689: NetApp MetroCluster IP" MetroCluster ist eine kontinuierlich verfügbare Speicherlösung für ONTAP, die auf FAS- und AFF-Systemen läuft. MetroCluster IP ist die neueste Weiterentwicklung, die ein Ethernet-basiertes Backend-Speichernetzwerk verwendet. MetroCluster IP bietet eine hochredundante Konfiguration, um die Anforderungen der kritischsten Geschäftsapplikationen zu erfüllen. MetroCluster IP ist in ONTAP enthalten und bietet NAS- und SAN-Konnektivität für Clients und Server, die ONTAP Storage nutzen.

MetroCluster FC

"TR-4375: NetApp MetroCluster FC" MetroCluster sorgt für kontinuierliche Datenverfügbarkeit über geografisch verteilte Datacenter hinweg für geschäftskritische Applikationen. Erfahren Sie mehr über von MetroCluster FC empfohlene Vorgehensweisen, Designentscheidungen und unterstützte Konfigurationen.

Technische Berichte zur ONTAP Datensicherung und Disaster Recovery

SnapMirror ist eine kostengünstige, benutzerfreundliche und einheitliche Replizierungslösung für die gesamte Data-Fabric-Strategie. Sie repliziert Daten mit hoher Geschwindigkeit über LAN oder WAN. Sie bietet hohe Datenverfügbarkeit und schnelle Datenreplizierung für geschäftskritische Applikationen wie Microsoft Exchange, Microsoft SQL Server und Oracle in virtuellen und herkömmlichen Umgebungen. Durch das Replizieren und ständige Aktualisieren der sekundären Daten auf einem oder mehreren ONTAP Storage-Systemen sind die Daten immer aktuell und verfügbar. Es sind keine externen Replizierungsserver erforderlich.

Diese technischen Berichte erweitern die "ONTAP Datensicherung und Disaster Recovery"Produktdokumentation.

SnapMirror

SnapMirror Asynchron

"TR-4015: Asynchrone Konfiguration mit SnapMirror und Best Practices" Lernen Sie empfohlene Vorgehensweisen für die Konfiguration der asynchronen SnapMirror-Replikation (SM-A) von Volumes, Konsistenzgruppen und virtuellen Storage-Maschinen (SVM-Disaster Recovery) kennen.

"TR-4678: Datensicherheit und Backup-ONTAP FlexGroup-Volumen"
Erfahren Sie mehr über empfohlene Datensicherungs- und Backup-Funktionen für FlexGroup Volumes. Themen sind Snapshot Kopien, SnapMirror und weitere Datensicherungs- und Backup-Lösungen.

SnapMirror Synchronous

"TR-4733: Synchrone Konfiguration mit SnapMirror und Best Practices" Erfahren Sie mehr über empfohlene Vorgehensweisen für die Konfiguration der SnapMirror Synchronous (SM-S) Replikation.

SnapMirror DR mit drei Datacentern

"TR-4832: Drei-Datacenter-Disaster Recovery mit NetApp SnapMirror für ONTAP 9.7" Erfahren Sie mehr über eine Disaster-Recovery-Konfiguration für drei Datacenter mit ONTAP SnapMirror Technologie zur Replizierung.

Applikationen und Infrastruktur mit SnapMirror

"TR-4900: VMware Site Recovery Manager mit ONTAP" ONTAP ist seit seiner Einführung in das moderne Datacenter im Jahr 2002 eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich um innovative Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen. Erfahren Sie mehr über die empfohlene ONTAP-Lösung für VMware Site Recovery Manager (SRM), die branchenführende Disaster Recovery (DR)-Software von VMware. Sie enthält die neuesten Produktinformationen und empfohlene Vorgehensweisen zur Optimierung der Bereitstellung, Risikominderung und Vereinfachung des fortlaufenden Managements.

Cyber-Vault: ONTAP

"Cyber-Vault: ONTAP" Die auf ONTAP basierende Cyber-Vault von NetApp bietet Unternehmen eine umfassende und flexible Lösung für den Schutz ihrer wichtigsten Datenbestände. Dank der Nutzung logischer

Air-Gapping-Verfahren zur robusten Härtung können Sie mit ONTAP sichere, isolierte Storage-Umgebungen erstellen, die gegen neue Cyberbedrohungen gewappnet sind. Mit ONTAP gewährleisten Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten und profitieren gleichzeitig von der Agilität und Effizienz Ihrer Storage-Infrastruktur.

Technische Berichte zu Volumes von ONTAP FlexCache und FlexGroup

NetApp NAS-Lösungen vereinfachen das Datenmanagement, halten mit dem Datenwachstum Schritt und optimieren gleichzeitig die Kosten. Mit NAS-Lösungen von ONTAP erreichen Sie unterbrechungsfreien Betrieb, bewährte Effizienz und nahtlose Skalierbarkeit in einer Unified Architecture. Scale-out-NAS mit ONTAP Technologie nutzt das enorme ONTAP Ecosystem, in dem wir einen bedeutenden Innovationsvorsprung und auch eine Vision für aggressive zukünftige Innovationen haben.

Diese technischen Berichte enthalten eine weitere Erweiterung der "ONTAP FlexCache Volume" und "ONTAP FlexGroup Volume" Produktdokumentation.

FlexCache

"TR-4743: FlexCache im ONTAP"
Bei FlexCache handelt es sich um eine Caching-Technologie, die spärliche, beschreibbare Replikate von Volumes auf demselben oder verschiedenen ONTAP Clustern erstellt. Die Software kann den Benutzer näher bringen, um einen schnelleren Durchsatz bei geringerem Platzbedarf zu erzielen. Erfahren Sie, wie FlexCache eingesetzt werden kann sowie über empfohlene Practices, Grenzen und Überlegungen für Design und Implementierung.

FlexCache Write-Back

"FlexCache Write-Back" Seit ONTAP 9.15.1 ist FlexCache Write-Back ein alternativer Betriebsmodus zum Schreiben in einen Cache. Mit Write-Back kann der Schreibvorgang auf stabilen Storage im Cache übertragen und dem Client bestätigt werden, ohne darauf zu warten, dass die Daten zum Ursprung gebracht werden. Die Daten werden asynchron an den Ursprung zurückgespült. Das Ergebnis ist ein weltweit verteiltes Filesystem, mit dem Schreibvorgänge für spezifische Workloads und Umgebungen mit nahezu lokaler Geschwindigkeit ausgeführt werden können und das mit deutlichen Performance-Vorteilen verbunden ist.

FlexGroup Volumes

"TR-4571: NetApp ONTAP FlexGroup Volumes Best Practices und Implementierungsleitfaden"
Erfahren Sie mehr über FlexGroup Volumes sowie empfohlene Practices und Implementierungstipps. FlexGroup Volumes sind eine Weiterentwicklung von ONTAP-Scale-out-NAS-Containern, die nahezu unbegrenzte Kapazität mit einer planbaren Performance mit niedriger Latenz für Workloads mit vielen Metadaten verbinden.

"TR-4678: Datensicherheit und Backup von FlexGroup Volumen"
Informieren Sie sich über Datensicherung und Backup für FlexGroup Volumes, einschließlich Snapshot Kopien, SnapMirror und anderen Datensicherungs- und Backup-Lösungen.

Technische Berichte zum ONTAP Networking

ONTAP bietet eine Vielzahl verschiedener Netzwerkfunktionen und Konfigurationen für anspruchsvollste Scale-out-Applikationen. Mithilfe der Netzwerkfunktionen und -Funktionen können Unternehmen einen zuverlässigen und sicheren Zugriff auf ihre Daten schaffen.

Diese technischen Berichte erweitern die "ONTAP-Netzwerkmanagement"Produktdokumentation.

Routing

"TR-4949: BGP/VIP mit ONTAP im Rechenzentrum"
Erfahren Sie, wie Sie eine grundlegende BGP-Konfiguration in ONTAP schnell implementieren.

Name Services

"TR-4523: DNS-Lastverteilung in ONTAP"
Erfahren Sie, wie Sie ONTAP für die Verwendung mit DNS-Lastausgleichsmethoden konfigurieren, einschließlich DNS in ONTAP, verschiedene Konfigurationsmethoden und empfohlene Vorgehensweisen.

"TR-4668: Name Services Best Practices Guide"
Erfahren Sie mehr über empfohlene Vorgehensweisen, Einschränkungen und Überlegungen bei der Implementierung von NAS-Lösungen (Network-Attached Storage) wie CIFS/SMB und NFS in ONTAP.

"TR-4835: Konfiguration von LDAP in ONTAP-Multiprotokoll-NAS-Identitätsmanagement"
Erfahren Sie, wie Sie das Lightweight Directory Access Protocol (LDAP)-Identitätsmanagement in ONTAP für Multiprotokoll-NAS konfigurieren.

NFS

ONTAP NFS technische Berichte

NetApp NFS Lösungen vereinfachen die Datenverwaltung und helfen dabei, mit dem Wachstum Schritt zu halten und gleichzeitig die Kosten zu optimieren.

NFS

"TR-4067: NFS in ONTAP Best Practice und Implementierungsleitfaden"
Informieren Sie sich über grundlegende Konzepte, Support-Informationen, Konfigurationstipps und empfohlene Vorgehensweisen für NFS in ONTAP.

"TR-4962: NFSv4.2 – Erweiterte Attribute"
Erfahren Sie mehr über die Aktivierung und Verwendung von erweiterten NFSv4.2-Attributen in ONTAP 9.12.1 und höher.

Multi-Protokoll

"TR-4887: Übersicht über Multiprotokoll-NAS in ONTAP und Best Practices"
Erfahren Sie, wie der Multiprotokoll-NAS-Zugriff in ONTAP funktioniert und welche empfohlenen Praktiken für Multi-Protokoll-Umgebungen kommen.

NFS über TLS

NFS über TLS Übersicht

ONTAP 9.19.1 führt NFS over TLS ein, den lang erwarteten „einfachen Knopf“ zur Verschlüsselung Ihres NFS-Datenverkehrs.

Vor dieser Funktion war die Verschlüsselung Ihrer NFS-Nutzlast während der Übertragung auf IPsec oder Kerberos beschränkt. Beide Methoden sind zwar effektiv, die Konfiguration war jedoch umständlich und die Leistungseinbußen konnten erheblich sein. Beide Methoden waren „Aufsatzlösungen“, also Lösungen, die nicht in einem RFC speziell für NFS definiert waren. "RFC 9289", mit dem Titel „Toward Remote Procedure Call Encryption by Default“, änderte dies. Nun können NFSv3 und NFSv4.x den NFS-RPC-Datenverkehr während der Übertragung mit TLS 1.3 verschlüsseln. Kein Kerberos erforderlich. Kein IPsec erforderlich.

Voraussetzungen

Um ONTAP NFS über TLS zu verwenden, müssen die folgenden Voraussetzungen erfüllt sein.

- … ONTAP 9.19.1 ausführen
  - ONTAP Cloud-Persönlichkeiten werden derzeit nicht unterstützt
- …über eine NFS-Lizenz verfügen
- …ist ein NFS-Client im "NetApp Interoperabilitätsmatrix"

Was es nicht tut

NFS over TLS sichert die Transportschicht, es ändert jedoch nichts daran, wie NFS Benutzer authentifiziert.

Zertifikatbasierte Benutzerauthentifizierung. NFS über TLS **bietet keinen neuen Mechanismus zur Benutzerauthentifizierung**. Es werden weiterhin entweder `auth_sys` oder `krb5` für die Benutzerauthentifizierung benötigt. `krb5i` und `krb5p` können weiterhin verwendet werden, aber durch TLS werden deren Integritäts- und Datenschutzmechanismen überflüssig, und es kommt dennoch zu Leistungseinbußen.

Anwendungsfälle und Arbeitslasten

NFS over TLS eignet sich gut für drei gängige Einsatzszenarien: Verschlüsselung während der Datenübertragung ohne Kerberos-Infrastruktur, TLS-Erzwingung pro Client bei einem gemeinsam genutzten Export und gegenseitige Client-Authentifizierung.

Nicht jede Arbeitslast profitiert gleichermaßen, die Kenntnis der passenden und unpassenden Muster unterstützt die Planung der Bereitstellung.

Anwendungsfälle

NFS-Verschlüsselung während der Übertragung ohne Kerberos-Infrastruktur. Wenn NFS-Datenpfad-Verschlüsselung benötigt wird, aber kein Key Distribution Center (KDC) bereitgestellt und betrieben, keine Keytabs an Clients verteilt oder ein Kerberos-Bereich auf die NAS-Clients ausgeweitet werden soll, bietet NFS über TLS hierfür eine direkte Lösung. Ein Serverzertifikat wird pro Storage Virtual Machine (SVM) installiert, NFS über TLS wird auf jeder Daten Logical Interface (LIF) aktiviert, die verschlüsseltes NFS übertragen soll, und die Clients verhandeln TLS 1.3 im Datenstrom über den Standard-NFS-Port. Kein neuer Authentifizierungsdienst erforderlich.

Clientbezogene TLS-only-Erzwingung auf einem gemeinsam genutzten NFS Export. Wenn sowohl Clients mit als auch ohne Verschlüsselungsanforderung vorhanden sind, ist eine Möglichkeit erforderlich, die regulierten Clients auf den verschlüsselten Pfad zu zwingen, ohne die anderen zu beeinträchtigen. Die Export-Policy-Regeloption `-allow-nfs-tls-only true` erfüllt genau diese Funktion. Nicht-TLS-Mounts von entsprechenden Clients über TCP werden abgelehnt, während andere Export-Policy-Regeln unberührt bleiben.

Gegenseitige Client-Authentifizierung (mTLS) für die Vertrauensstellung zwischen Speicher und Client. Bei Betrieb nach Zero-Trust-Netzwerkprinzipien oder bei Härtungsanforderungen, die verlangen, dass der Storage-Controller die Hostidentität jedes verbindenden Clients überprüft, empfiehlt sich die Option für gegenseitiges TLS pro LIF. Setzen Sie `-enforce-host-auth true` auf `vserver nfs tls interface enable` oder `vserver nfs tls interface modify`. ONTAP validiert dann das X.509-Zertifikat jedes verbindenden Clients anhand der im SVM installierten Zertifizierungsstellen-Vertrauenskette (CA) zum Zeitpunkt des TLS-Handschlags und lehnt Clients ab, die kein vertrauenswürdiges Zertifikat vorlegen. Dadurch erfolgt eine kryptografische Durchsetzung von „Nur meine registrierte Host-Flotte kann auf diese NFS LIF zugreifen“, zusätzlich zu bestehenden Exportrichtlinien-Hostfiltern.

Arbeitslasten

Verschlüsselung ist nicht kostenlos. Der TLS-Handschlag verursacht messbare Kosten, und die TLS-Datensatzverschlüsselung führt bei jedem RPC zu zusätzlichem Aufwand. Die Auswirkungen auf die Leistung variieren stark in Abhängigkeit von Arbeitslast, Plattform und der Verfügbarkeit von Hardware-Offload. Einzelheiten finden sich unter "Performance".

Arbeitslastmuster

Langlebige NFS-Mounts mit einer stabilen Client-Population eignen sich hervorragend. Der TLS-Handschlag ist ein pro Verbindung anfallender Aufwand, der beim Mounten und bei der Wiederherstellung der Sitzung entsteht. Bei einer kleinen, stabilen Gruppe von Clients, die einmal mounten und stunden- oder tagelang verbunden bleiben, wird dieser Aufwand problemlos absorbiert.

Wenn Sie die Zuordnung von LIF zu Hostnamen bereits sauber verwalten, beispielsweise mit DNS-Einträgen unter Ihrer Kontrolle, gestaltet sich die Bereitstellung von NFS über TLS unkompliziert. Die Funktion wird pro LIF konfiguriert: Es wird ein Serverzertifikat installiert, dessen Common Name (CN) mit dem Fully Qualified Domain Name (FQDN) des LIF übereinstimmt und dessen Subject Alternative Name (SAN)-Liste die IP-Adresse des LIF enthält.

NFS over TLS ist das richtige Werkzeug, wenn Vertraulichkeit während der Datenübertragung, Serveridentität und optional die Identität des Client-Hosts zu Ihren Sicherheitsanforderungen gehören, genau die Eigenschaften, die TLS bietet.

Workload-Anti-Patterns

Hohe Verbindungsfluktuation oder große Mount-Stürme sind ungeeignet. Jede neue TLS-Verbindung trägt die Kosten des TLS 1.3-Handschlags, einschließlich asymmetrischer Kryptografie, Zertifikatsvalidierung und optionaler mTLS-Kettenvalidierung. Wenn viele Clients mounten, nur wenig Arbeit verrichten, unmounten und sich wiederholt verbinden, fallen diese Handschlag-Kosten immer wieder an, anstatt sich zu amortisieren.

Architektur

NFS over TLS ist eine pro-LIF-Transportsicherheitsfunktion des ONTAP NFS-Servers. Dabei wird TLS-Schutz auf den NFS-Datenverkehr zwischen dem Client und dem ONTAP NFS-Server angewendet. Die Konfiguration wird über die `vserver nfs tls interface` Befehlsfamilie und die entsprechende `/api/protocols/nfs/tls/interfaces` REST-Ressource verwaltet.

Die Konfiguration ist SVM-bezogen, wird pro LIF angewendet und clusterweit repliziert. Jeder Node, der aktuell das LIF hostet, verwendet dieselben TLS-Einstellungen. Es gibt keinen clusterweiten Ein-/Ausschalter. Aktivieren und Deaktivieren sind pro-LIF-Operationen.

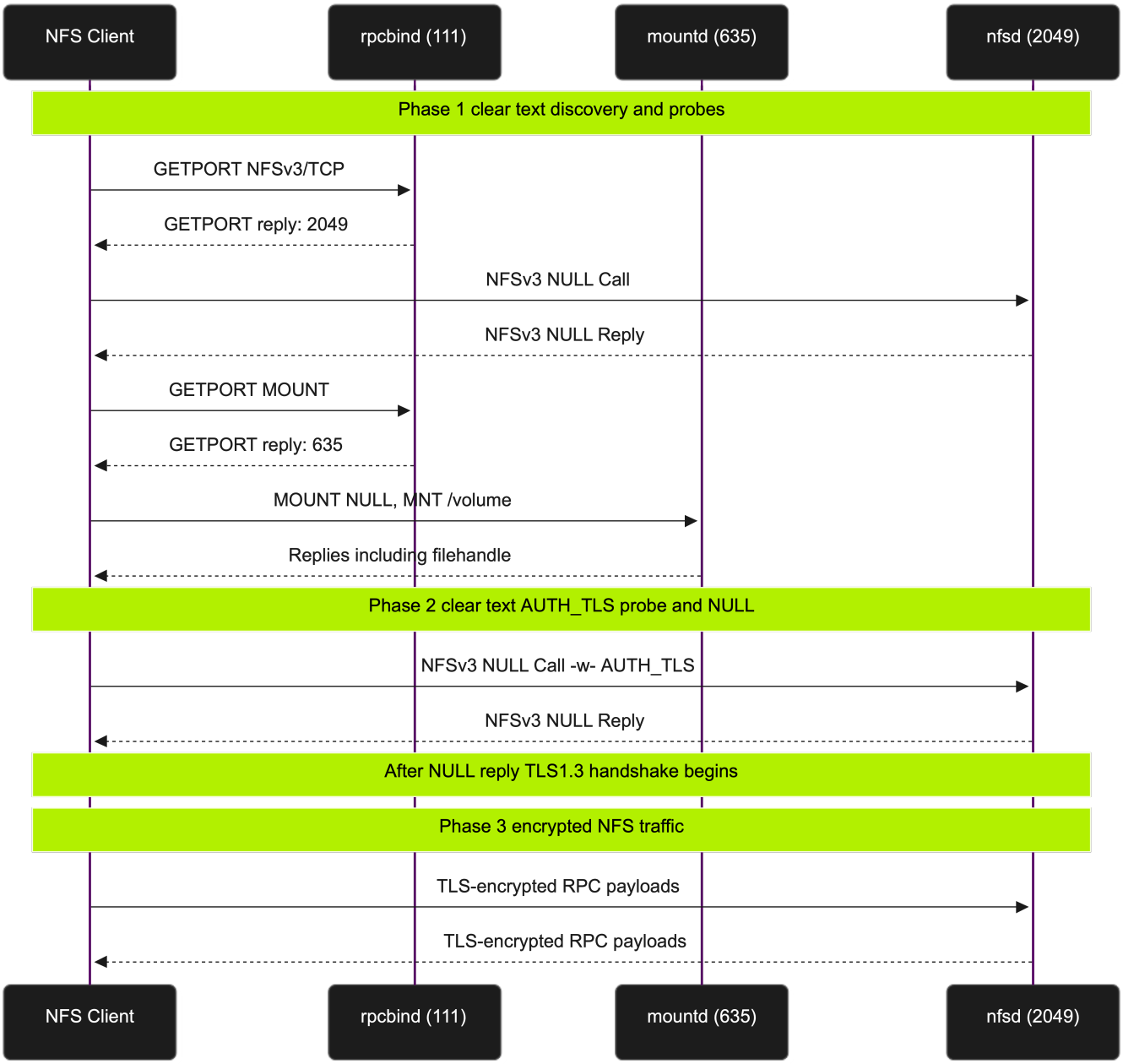
Externe Abhängigkeiten

Vom NFS-TLS-Handshake-Pfad in Version 9.19.1 werden keine ausgehenden Aufrufe an eine externe Zertifizierungsstelle (CA) oder einen OCSP-Responder getätigt. Die Validierung der Zertifikatskette und des Subject Alternative Name (SAN) erfolgt lokal anhand des auf der SVM installierten Zertifikatsmaterials.

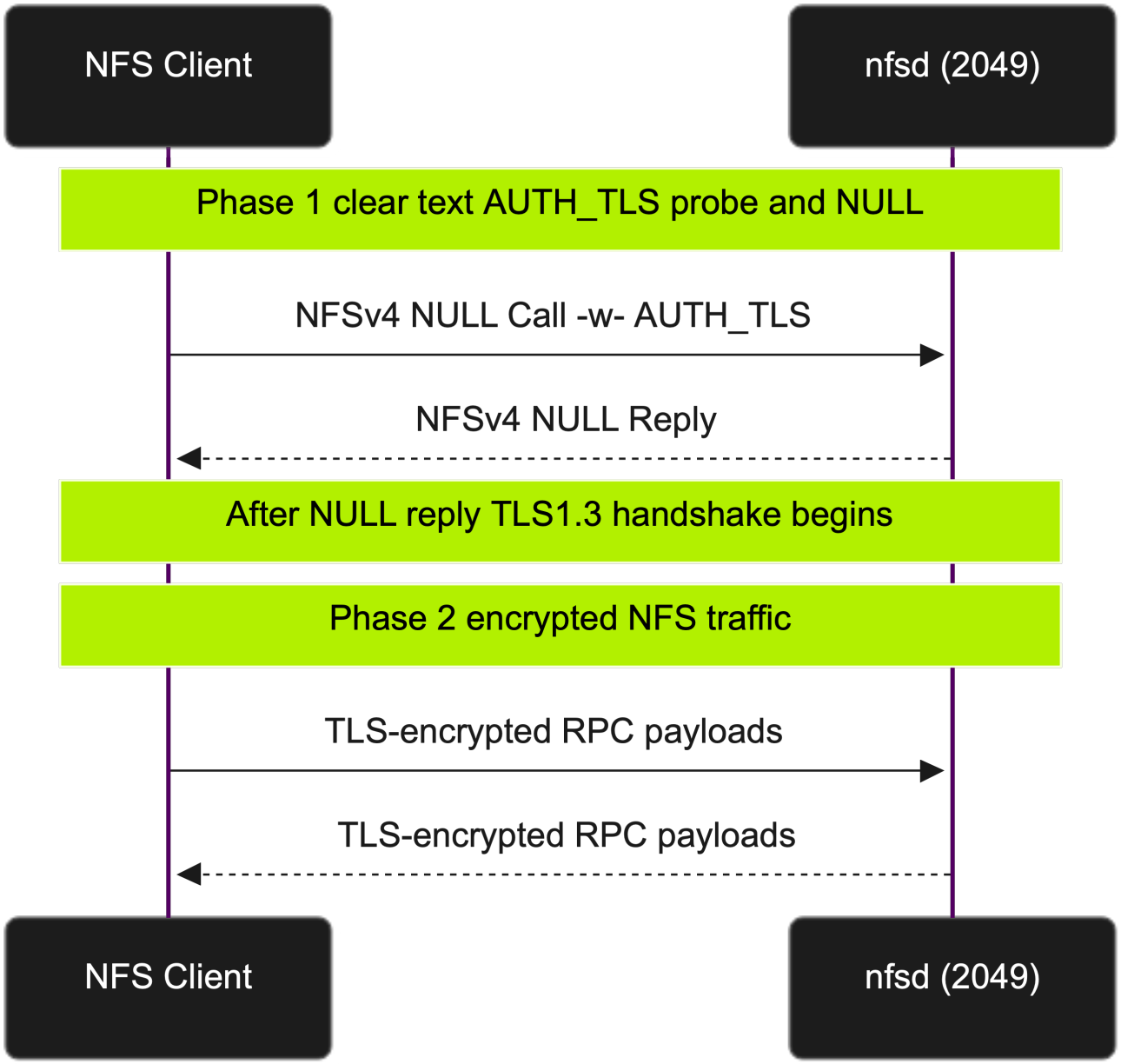
Datenfluss

Sowohl NFSv3 als auch NFSv4 verschlüsseln die gesamte NFS-Nutzlast nach dem ersten NULL-Aufruf/Antwort-Paar an TCP-Port 2049. Der NULL-Aufruf enthält die neue `AUTH_TLS` Anmeldeinformationsart, die in RFC 9289 definiert ist und die Absicht des Clients zur Verwendung von TLS signalisiert. Der Server antwortet mit einer NULL-Antwort, die das TLS-Upgrade entweder akzeptiert oder ablehnt. Erhält der Client eine Akzeptanz, setzt er den TLS 1.3-Handschlag über dieselbe TCP-Verbindung fort. Wenn der Handschlag erfolgreich abgeschlossen wird, werden alle nachfolgenden NFS-RPCs in TLS-Datensätzen gekapselt und während der Übertragung verschlüsselt.

Es gibt einen Unterschied zwischen NFSv3 und NFSv4.x: NFSv3 verwendet zusätzliche Protokolle -`rpcbind` (portmapper), `mountd`, NLM (Network Lock Manager) und NSM (Network Status Monitor), die nicht über die TLS-geschützte Verbindung übertragen werden und unverschlüsselt übertragen werden. Organisationen mit Compliance-Anforderungen, die eine vollständige Verschlüsselung des Speicherdatenverkehrs vorschreiben, sollten dies bei der Wahl zwischen NFSv3 und NFSv4.x berücksichtigen. NFSv4.x eliminiert diese Side-Channel-Protokolle; der gesamte NFSv4.x-Datenverkehr wird auf Port 2049 konsolidiert und nach dem TLS-Handschlag verschlüsselt.



NFSv4.x verwendet keine Hilfsprotokolle, daher werden alle NFSv4.x RPCs nach dem TLS-Handschlag verschlüsselt.



ONTAP beendet TLS am NFS-Server auf dem Knoten, der aktuell die LIF hostet. Oberhalb des Transports verarbeitet der NFS-Server RPCs identisch wie bei einer NFS-Verbindung ohne TLS.

HA Takeover-Verhalten

Bestehende NFS-over-TLS-Sitzungen überstehen weder eine HA-Übernahme noch einen ungeplanten Knotenausfall. TLS ist ein auf TCP basierender Transport auf Sitzungsebene. Wenn TCP-Verbindungen mit dem Knoten abbrechen, werden auch die TLS-Sitzungen beendet.

Nach der Übernahme verbinden sich die Clients erneut und führen einen neuen TLS 1.3 Handschlag durch. Der Partnerknoten verwendet dieselbe replizierte TLS-Konfiguration, also Zertifikatsbindung, Host-Authentifizierungseinstellung und SAN-Validierungseinstellung, da der Konfigurationsdatensatz clusterweit repliziert wird.

TLS-Sitzungstickets und Pre-Shared Keys (PSKs) sind lokal auf dem Knoten und werden nicht an den Partner

übertragen. Bei einer Übernahme ist mit einer Vielzahl von Verbindungsversuchen und vollständigen TLS-Handschlägen zu rechnen.

MetroCluster und SVM-DR-Verhalten

Das TLS-Schnittstellenzertifikat und die Konfiguration werden zusammen mit der SVM über den standardmäßigen SVM-DR- und MetroCluster SVM-Level-Replikationspfad repliziert. Nach einem Identity-Preserve-Switchover verfügt die Ziel-SVM über dieselbe TLS-Konfiguration pro LIF.

Das `-allow-nfs-tls-only`Feld der Exportregel wird zusammen mit dem Rest der Exportregel über den Standardpfad zur Replikation von Exportregeln repliziert. In SVM-DR wird die Regel zusammen mit der Richtlinie übertragen, wenn die Richtlinie mit dem SVM repliziert wird.

NFS über TLS konfigurieren

NFS over TLS wird pro LIF mithilfe der `vserver nfs tls interface` Befehlsfamilie, der `/api/protocols/nfs/tls/interfaces` REST-Endpunkte oder der NFS-Einstellungen von System Manager konfiguriert.

Exportregel erhalten ein zusätzliches Feld, das die Durchsetzung von ausschließlich TLS-basiertem Zugriff für passende Clients ermöglicht. Befehlsreferenzen finden sich unter "docs.netapp.com". Die REST-API kann interaktiv über die integrierte Swagger-Dokumentation erkundet werden, indem der Browser auf `https://<cluster-mgmt-ip>/api/docs` zeigt.

ONTAP-Voraussetzungen

Das nachfolgend beschriebene Verfahren setzt voraus, dass die folgenden Voraussetzungen erfüllt sind:

- ONTAP 9.19.1 oder höher
- Eine SVM mit aktiviertem NFS-Protokoll
- Mindestens eine für den grundlegenden NFS-Zugriff konfigurierte Daten-LIF

Schritt 1: Erstellen einer Stammzertifizierungsstelle auf ONTAP

> **Option „Externe Zertifizierungsstelle“.** Wenn Ihre Organisation eine externe Zertifizierungsstelle verwendet, kann dieser Schritt übersprungen werden. Die CSRs aus Schritt 2 und Schritt 5 werden an die externe Zertifizierungsstelle übermittelt und die resultierenden signierten Zertifikate auf ONTAP installiert. Der restliche Ablauf bleibt unverändert.

ONTAP kann als interne Zertifizierungsstelle (CA) für Labor- und interne Bereitstellungen fungieren. In diesem Schritt wird auf der SVM eine selbstsignierte Stamm-CA erstellt, die zum Signieren des Serverzertifikats (und optional von Client-Zertifikaten für gegenseitiges TLS) verwendet wird.

```
ontap9::> security certificate create -vserver <svm> -common-name <ca-
name> -type root-ca -size 2048 -hash-function SHA256 -expire-days 3652
-country US -state <state> -locality <city> -organization <org> -unit
<unit>
```

Nach Abschluss des Befehls die CA-Seriennummer abrufen und notieren. Sie wird in Schritt 2 und, bei Verwendung von mutual TLS, in Schritt 5 benötigt.

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields serial
```

Notieren Sie die Seriennummer: Diese wird `<ca-serial>` in späteren Schritten benötigt.

Schritt 2: Das Serverzertifikat für die Daten-LIF generieren

ONTAP präsentiert dieses Zertifikat den NFS-Clients während des TLS-Handschlags. Der Common Name (CN) und der Subject Alternative Name (SAN) des Zertifikats müssen mit dem FQDN und der IP-Adresse des LIF übereinstimmen, da tlshd auf dem Client die Serveridentität anhand beider validiert.

> **IP-SAN-Anforderung.** Wenn geplant ist, NFSv4.1 Session Trunking mit NFS über TLS zu konfigurieren oder wenn ein Mount-Befehl eine rohe IP-Adresse anstelle eines Hostnamens verwendet, muss das Zertifikat einen IP-SAN-Eintrag für jede LIF-IP enthalten, zu der Clients eine Verbindung herstellen. Ohne diesen schlägt der TLS-Handschlag für IP-adressierte Pfade mit „Certificate owner unexpected“ fehl.

Der ONTAP CSR-Generator (security certificate generate-csr) unterstützt IP-SANs direkt über `-ipaddr`, der eine durch Kommas getrennte Liste von IP-Adressen akzeptiert.

2a. CSR und privaten Schlüssel generieren.

Fügen Sie `-ipaddr`eine durch Kommas getrennte Liste aller LIF-IP-Adressen hinzu, die NFS over TLS-Datenverkehr übertragen. Fügen Sie `-dns-name`die Hostnamen hinzu, die in Mount-Befehlen verwendet werden.

```
ontap9::> security certificate generate-csr -common-name <lif-fqdn>
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name <lif-fqdn> -ipaddr <lif-ip>[,<lif-ip-2>,...] -country
US -state <state> -locality <city> -organization <org> -unit <unit>
```

Beispiel für ein einzelnes LIF:

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130 -country US
-state CA -locality SanJose -organization "MyOrg" -unit "Storage"
```

Für Session-Trunking über zwei LIF-IPs beide in einer durch Kommas getrennten Liste angeben:

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130,192.0.2.131
-country US -state CA -locality SanJose -organization "MyOrg" -unit
"Storage"
```

Der Befehl erzeugt einen PEM-Block für die Zertifikatsignierungsanforderung (CSR) und einen PEM-Block für den privaten Schlüssel. Beide sollten kopiert und gespeichert werden, da der private Schlüssel nur einmal angezeigt wird.

Um zu überprüfen, ob die CSR die erwarteten SANs enthält, bevor sie signiert wird, kann auf einem beliebigen Client mit OpenSSL folgender Befehl ausgeführt werden:

```
echo <paste CSR PEM> | openssl req -noout -text | grep -A3 "Subject
Alternative"
```

Erwartete Ausgabe:

```
X509v3 Subject Alternative Name: critical
    DNS:nfs.example.com, IP Address:192.0.2.130
```

2b. Den CSR mit der ONTAP CA signieren.

```
ontap9::> security certificate sign -vserver <svm> -ca <ca-name> -ca
-serial <ca-serial> -expire-days 365 -hash-function SHA256
```

Fügen Sie den CSR-PEM-Block ein, wenn Sie dazu aufgefordert werden. Kopieren Sie das signierte Zertifikat-PEM aus der Ausgabe.

2c. Installieren des signierten Serverzertifikats.

```
ontap9::> security certificate install -vserver <svm> -type server -cert
-name <cert-name>
```

Bei entsprechender Aufforderung:

- Fügen Sie das signierte Zertifikat-PEM ein.
- Den privaten Schlüssel im PEM-Format einfügen.
- Wenn nach Zwischen- oder Stammzertifikaten gefragt wird, die CA-Zertifikat-PEM einfügen und die Eingabetaste drücken, dann mit n antworten, um das Hinzufügen weiterer Zertifikate zu beenden.

2d. Das installierte Zertifikat überprüfen.

```
ontap9::> security certificate show -vserver <svm> -type server -common
-name <cert-name>
```

Das Ablaufdatum und das Vorhandensein des Eintrags werden bestätigt.

Schritt 3: NFS über TLS auf dem Daten-LIF aktivieren

Nachdem das Serverzertifikat installiert ist, wird NFS über TLS auf dem Ziel-LIF aktiviert.

```
ontap9::> vserver nfs tls interface enable -vserver <svm> -lif <lif>
-certificate-name <cert-name>
```

Es wird überprüft, ob die LIF TLS-fähig ist.

```
ontap9::> vserver nfs tls interface show -vserver <svm>
```

Erwartete Ausgabe:

```
Vserver:              <svm>
Logical Interface:    <lif>
IP Address:           <lif-ip>
TLS Status:           enabled
TLS Certificate Name: <cert-name>
Enforce Host Authentication: false
```

`TLS Status: enabled` bestätigt, dass ONTAP für diese LIF TLS auf Port 2049 aushandelt. Clients, die `xprtsec=tls` oder `xprtsec=mtls` verwenden, erhalten nun eine TLS-geschützte Verbindung. Clients, die kein TLS anfordern, verbinden sich weiterhin im Klartext, sofern in Schritt 7 keine Erzwingung hinzugefügt wird.

Schritt 4: Installation des CA-Zertifikats auf dem Linux-Client

Der Linux-Client muss der Zertifizierungsstelle vertrauen, die das Serverzertifikat von ONTAP signiert hat. Ohne dies `tlshd` lehnt den TLS-Handschlag ab, da das Serverzertifikat nicht als vertrauenswürdig gilt.

Wenn Sie die ONTAP CA verwendet haben (Schritt 1)

Das CA-Zertifikat aus ONTAP exportieren:

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields cert
```

Kopieren Sie das Zertifikat-PEM aus der Ausgabe und speichern Sie es in einer Datei (zum Beispiel `nfs-ca.crt`). Diese Datei auf den Linux-Client übertragen.

Wenn Sie eine externe Zertifizierungsstelle verwendet haben

Das CA-Zertifikat im PEM-Format aus Ihrer externen CA-Infrastruktur beziehen und in einer Datei speichern (zum Beispiel `nfs-ca.crt`). Diese Datei auf den Linux-Client übertragen.

Das CA-Zertifikat im System-Truststore installieren

RHEL / Rocky / AlmaLinux / Fedora:

```
sudo cp nfs-ca.crt /etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
sudo update-ca-trust
```

Debian / Ubuntu:

```
sudo cp nfs-ca.crt /usr/local/share/ca-certificates/nfs-tls-ca.crt
sudo update-ca-certificates
```

tlshd so konfigurieren, dass diese Zertifizierungsstelle als Vertrauensspeicher verwendet wird

Bearbeiten `/etc/tlshd.conf`:

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
```

Den `x509.truststore`Pfad so anpassen, dass er dem Speicherort des CA-Zertifikats entspricht.

tlshd wird neu gestartet, damit die Konfiguration übernommen wird:

```
sudo systemctl restart tlshd
```

Es wird überprüft, ob tlshd ordnungsgemäß gestartet wurde:

```
journalctl -u tlshd -n 20 --no-pager
```

Die Ausgabe sollte keine Fehlerzeilen enthalten.

Schritt 5: LIF-FQDN auf dem Client auflösen

`tlshd` validiert das Serverzertifikat anhand des im Mount-Befehl verwendeten Hostnamens. Es sollte bestätigt werden, dass `<lif-fqdn>` auf `<lif-ip>` dem Client vor dem Mounten aufgelöst wird.

```
getent hosts <lif-fqdn>
```

Wenn der Hostname nicht über DNS aufgelöst wird, einen statischen Eintrag hinzufügen:

```
echo <lif-ip> <lif-fqdn> | sudo tee -a /etc/hosts
```

Schritt 6: Einbinden mit NFS über TLS

Das Kernel-TLS-Modul laden, falls es noch nicht geladen ist:

```
sudo modprobe tls
```

Erstellen Sie den Einhängepunkt und führen Sie die Einbindung durch:

```
sudo mkdir -p <mountpoint>
sudo mount -t nfs \
  -o vers=4.1,xprtsec=tls \
  <lif-fqdn>:<export-path> <mountpoint>
```

Schritt 7: Die TLS-Verbindung überprüfen

Client-Seite

Bestätigen Sie, dass die Einbindung aktiv ist und `xprtsec=tls` anzeigt:

```
mount | grep nfs
```

Erwartete Ausgabe (Zeile mit dem Mount):

```
<lif-fqdn>:<export-path> on <mountpoint> type nfs4
(rw,...,xprtsec=tls,...)
```

Bestätigt wird, dass `tlshd`ein erfolgreicher TLS-Handschlag abgeschlossen wurde:

```
journalctl -u tlshd -n 10 --no-pager
```

Suchen Sie nach einer Zeile, die Folgendes enthält:

```
Handshake with '<lif-fqdn>' (...) was successful
```

ONTAP Seite

Bestätigen Sie, dass die Verbindung als `TLS/nfs` aufgeführt ist (zunächst eine geringe Menge an E/A

erzeugen, falls die Verbindung gerade erst hergestellt wurde):

```
ontap9::> network connections active show -vserver <svm>
```

Erwarteter Eintrag:

```
<lif>:2049  <client-fqdn>:<port>  TLS/nfs
```

Es sollte überprüft werden, dass keine TLS-Handschlagfehler aufgetreten sind:

```
ontap9::> event log show -severity error -message-name
Nblade.TLSHandshakeFailed
```

Keine neuen Einträge seit dem Mount-Versuch bedeuten, dass der Handschlag erfolgreich war.

Optional: TLS für bestimmte Clients erzwingen (Exportregel-Durchsetzung)

Standardmäßig ist NFS über TLS optional: Clients, die kein TLS anfordern, können sich weiterhin unverschlüsselt über eine TLS-fähige LIF verbinden. Um TLS für eine bestimmte Exportregel zu erzwingen, `-allow-nfs-tls-only true` festlegen.

```
ontap9::> vserver export-policy rule modify -vserver <svm> -policyname
<policy-name> -ruleindex <rule-index> -allow-nfs-tls-only true
```

Nach dieser Konfiguration wird jeder NFS-Client, der durch diese Regel erfasst wird und **kein** TLS verwendet, beim Auswertungspunkt der Exportregel abgewiesen. Bestehende TLS-Verbindungen sind davon nicht betroffen.

Überprüfung:

```
ontap9::> vserver export-policy rule show -vserver <svm> -policyname
<policy-name> -fields allow-nfs-tls-only
```

Optional: Gegenseitiges TLS (Client-Authentifizierung)

Standardmäßiges NFS über TLS authentifiziert den Server gegenüber dem Client (nur serverseitiges TLS). Mutual TLS (`xprtsec=mtls` erfordert zusätzlich, dass der Client ein Zertifikat vorlegt, das von ONTAP validiert wird. Dies bietet eine kryptografische Host-Authentifizierung auf beiden Seiten.

Anforderung an das Client-Betriebssystem. Mutual TLS erfordert `ktls-utils` 0.12 oder höher. Die mit RHEL 9.7 (`ktls-utils 0.11` ausgelieferte Version funktioniert **nicht**, sie sendet unabhängig von der Konfiguration kein Client-Zertifikat. RHEL 10.1 (`ktls-utils 1.2.1` ist validiert. Die `ktls-utils` Version sollte vor dem Fortfahren überprüft werden.

Mount-Option. Verwendung von `xprtsec=mtls`, **nicht** `xprtsec=tls`. Mit `xprtsec=tls` sendet der Kernel den Authentifizierungsmodus `HANDSHAKE_AUTH_UNAUTH` an `tlshd`, was dem anonymen Handschlag-Pfad folgt und kein Client-Zertifikat präsentiert, selbst wenn eines konfiguriert ist.

Schritt 1: Erstellen einer Zertifizierungsstelle für Client-Zertifikate (ONTAP)

Dies kann dieselbe Zertifizierungsstelle wie in Schritt 1 oder eine separate sein. Für den Produktivbetrieb wird die Verwendung einer separaten Zertifizierungsstelle empfohlen, damit die Zertifikatsketten von Server und Client voneinander getrennt sind.

```
ontap9::> security certificate create -vserver <svm> -common-name "NFS-
mTLS-CA" -type root-ca -expire-days 3652 -hash-function SHA256
```

Die Seriennummer ist als `<mtls-ca-serial>` zu notieren.

Schritt 2: Die Zertifizierungsstelle als Client-CA-Vertrauensanker (ONTAP) installieren

Das CA-Zertifikat exportieren:

```
ontap9::> security certificate show -vserver <svm> -common-name "NFS-mTLS-
CA" -type root-ca -fields cert
```

Als Typ `client-ca` installieren:

```
ontap9::> security certificate install -vserver <svm> -type client-ca
```

Fügen Sie das CA-Zertifikat im PEM-Format ein, wenn Sie dazu aufgefordert werden. Überprüfen:

```
ontap9::> security certificate show -vserver <svm> -type client-ca
```

Schritt 3: enforce-host-auth auf dem LIF (ONTAP) aktivieren

```
ontap9::> vserver nfs tls interface modify -vserver <svm> -lif <lif>
-enforce-host-auth true
```

Überprüfung:

```
ontap9::> vserver nfs tls interface show -vserver <svm> -instance
```

Bestätigen: `Enforce Host Authentication: true`.

Schritt 4: Client-Schlüssel und CSR generieren (Linux-Client)

```
sudo mkdir -p /etc/nfs
sudo openssl genrsa -out /etc/nfs/client.key 2048
sudo chmod 600 /etc/nfs/client.key

sudo openssl req -new \
  -key /etc/nfs/client.key \
  -subj "/CN=<client-fqdn>/C=US" \
  -addext "subjectAltName=DNS:<client-fqdn>,IP:<client-ip>" \
  -out /tmp/client.csr

cat /tmp/client.csr
```

Schritt 5: Den Client-CSR mit der ONTAP CA signieren

Auf dem ONTAP Cluster:

```
ontap9::> security certificate sign -vserver <svm> -ca "NFS-mTLS-CA" -ca
-serial <mtls-ca-serial> -expire-days 365 -hash-function SHA256
```

Fügen Sie den Inhalt von `/tmp/client.csr` ein, wenn Sie dazu aufgefordert werden. Die signierte Zertifikat-PEM aus der Ausgabe kopieren.

Schritt 6: Erstellen der Clientzertifikatskettendatei (Linux-Client)

Das signierte Zertifikat unter `/tmp/client-signed.crt` speichern. Auch das CA-Zertifikat PEM (`nfs-mtls-ca.crt` erhalten. Beide zu einer Ketten-Datei zusammenfügen:

```
sudo bash -c "cat /tmp/client-signed.crt /path/to/nfs-mtls-ca.crt \
  > /etc/nfs/client-chain.crt"
sudo chmod 600 /etc/nfs/client-chain.crt
```

Warum eine Zertifikatskettendatei? `tlshd` 1.2.1 verwendet `gnutls_pcert_list_import_x509_raw` und benötigt die vollständige Zertifikatskette (Leaf-Zertifikat gefolgt von der Zertifizierungsstelle), damit GnuTLS den Aussteller während des `find_x509_client_cert`-Callbacks korrekt auflösen kann. Eine Datei, die nur das Leaf-Zertifikat enthält, führt zu einem Fehler bei der GnuTLS-Assertion.

Schritt 7: /etc/tlshd.conf mit dem Clientzertifikat (Linux-Client) aktualisieren

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
x509.certificate=/etc/nfs/client-chain.crt
x509.private_key=/etc/nfs/client.key
```

tlshd neu starten:

```
sudo systemctl restart tlshd
```

Schritt 8: Mount mit xprtsec=mtls

```
sudo mount -t nfs \
  -o vers=4.1,xprtsec=mtls \
  <lif-fqdn>:<export-path> <mountpoint>
```

Schritt 9: Gegenseitige TLS-Verbindung verifizieren

Client:

```
mount | grep nfs
# Confirm: xprtsec=mtls in mount options

journalctl -u tlshd -n 5 --no-pager
# Confirm: "Handshake with '<lif-fqdn>' (...) was successful"
```

ONTAP:

```
ontap9::> network connections active show -vserver <svm>
# Confirm: <lif>:2049  <client-fqdn>:<port>  TLS/nfs

ontap9::> event log show -severity error -message-name
Nblade.TLSHandshakeFailed
# No new entries = success
```

Wichtige Standardeinstellungen

- `-enforce-host-auth = false`NFS über TLS erzwingt standardmäßig keine hostbasierte Authentifizierung. Dies ist die weniger restriktive Vorgehensweise. Wenn diese Option auf `true` gesetzt ist, werden TLS-Verbindungen abgelehnt, deren Zertifikatsidentität nicht mit der Host-Identität des LIF übereinstimmt.
- `-skip-san-validation = false`Die SAN-Prüfung wird standardmäßig durchgeführt. Wenn diese Option auf `true` gesetzt wird, wird die Bindung der Zertifikat- zu LIF-Identität gelockert. Dieser Parameter ist nur schreibbar: Nachfolgende `show` oder `GET` geben den Wert nicht zurück, sodass Administratoren nachträglich nicht feststellen können, ob die SAN-Validierung beim Aktivieren oder Ändern übersprungen wurde.
- `-allow-nfs-tls-only = false`Eine Exportrichtlinienregel erfordert TLS nicht standardmäßig. Die Aktivierung von NFS über TLS auf einem LIF lehnt unverschlüsseltes NFS nicht von selbst ab. Für eine ausschließlich TLS-basierte Haltung ist pro Regel die Option zu wählen, und es muss sichergestellt sein, dass TLS auf allen Daten-LIFs, die diese Clients bedienen, aktiviert ist, da sonst der Zugriff verweigert wird.

Die `vserver export-policy rule create` und `vserver export-policy rule modify` Befehle erhalten ein neues Feld, `-allow-nfs-tls-only`, das die übereinstimmenden Clients auf NFS-over-TLS-Verbindungen beschränkt.

REST-Endpunkte

Die REST-API lässt sich interaktiv über die integrierten Swagger-Dokumente erkunden, indem im Browser `https://<cluster-mgmt-ip>/api/docs` aufgerufen wird. Die NFS over TLS-Endpunkte befinden sich unter dem `/api/protocols/nfs/tls/interfaces` Pfad für die LIF-Konfiguration und unter `/api/protocols/nfs/export-policies/{policy.id}/rules` für das Feld der Export-Policy-Regel.

Sicherheit

Diese Seite behandelt RBAC-Anforderungen, Zertifikatsvalidierung, Verschlüsselungsparameter, Revisionsprotokoll und bekannte Sicherheitsbeschränkungen für NFS über TLS bei ONTAP 9.19.1.

Rollen- und RBAC-Anforderungen

Die `vserver nfs tls interface` Befehlsfamilie-`enable`, `disable`, `modify` und `show` ist SVM-spezifisch. Sie kann von der Cluster `admin`-Rolle oder von der `vsadmin` der zugehörigen SVM ausgeführt werden.

Das `-allow-nfs-tls-only` Feld auf `vserver export-policy rule` ist ein Schreibfeld des bestehenden Exportregel-Objekts. Es verwendet die standardmäßige Export-Policy-Regel-RBAC.

REST-Endpunkte unter `/api/protocols/nfs/tls/interfaces` entsprechen eins zu eins den oben genannten CLI-Befehlen. Es wird die standardmäßige NAS-Admin-RBAC verwendet. Es ist keine separate REST-Rolle definiert.

Authentifizierung und Autorisierung

Die Aktivierung von NFS über TLS auf einem LIF erfordert ein Server-X.509-Zertifikat, das auf der SVM über `security certificate install` installiert ist. Das Zertifikat wird pro LIF zum Zeitpunkt der Aktivierung mit `-certificate-name` gebunden.

ONTAP führt zwei Prüfungen des bereitgestellten Serverzertifikats durch:

1. Der allgemeine Name (CN) des Zertifikats muss mit dem Fully Qualified Domain Name (FQDN) des LIF übereinstimmen.
2. Die IP-Adresse des LIF muss in der Liste der Subject Alternative Names (SAN) des Zertifikats aufgeführt sein.

Ein optionaler `-skip-san-validation`boolescher Wert (Standardwert `false`) unterdrückt die SAN Prüfung beim Aktivieren oder Ändern.

Jeder fehlgeschlagene Prüfvorgang liefert eine eindeutige Fehlermeldung.

Die gegenseitige TLS (mTLS) Host-Authentifizierung ist optional. `-enforce-host-auth true` auf `vserver nfs tls interface enable` oder `modify` kann gesetzt werden, um sie zu aktivieren. Standardmäßig ist `false` eingestellt, was bedeutet, dass nur die Server-Authentifizierung erfolgt. Client-Zertifikate werden anhand der auf dem SVM installierten CA-Vertrauenskette validiert, für deren Bereitstellung Sie verantwortlich sind.

Benutzerauthentifizierung

Die Benutzerauthentifizierung bleibt durch TLS unverändert. TLS ergänzt die Datenübertragung um Vertraulichkeit und Host-Authentifizierung. `AUTH_SYS` UNIX UID/GID oder `RPCSEC_GSS`/Kerberos müssen weiterhin für die RPC-Benutzerauthentifizierung verwendet werden. RFC 9289 stellt dies explizit klar: TLS schützt den Transport, während die bestehenden NFS-Authentifizierungsverfahren die Benutzerauthentifizierung wie bisher übernehmen.

Verschlüsselung

Während der Übertragung

Wenn NFS über TLS auf einem LIF aktiviert ist, wird ausschließlich TLS 1.3 verwendet. Die folgenden Cipher Suites werden unterstützt:

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`
- `TLS_CHACHA20_POLY1305_SHA256`

Der Schlüsselaustausch erfolgt mittels ECDHE auf der `secp384r1` Kurve. Die Verschlüsselung gilt für NFSv3 und NFSv4.x Datenverkehr, der über die TLS-fähige LIF übertragen wird.

Prüfung

Alle Änderungen der NFS-over-TLS-Konfiguration werden im standardmäßigen ONTAP Revisionsprotokoll (`security audit log show`) aufgezeichnet. Die folgenden Vorgänge werden protokolliert:

- `vserver nfs tls interface enable`
- `vserver nfs tls interface modify`
- `vserver nfs tls interface disable`
- `vserver export-policy rule create -allow-nfs-tls-only`
- `vserver export-policy rule modify -allow-nfs-tls-only`

Schreibgeschützte `show` und `GET` Operationen folgen der standardmäßigen ONTAP Revisionsprotokollrichtlinie und werden in der Regel nicht aufgezeichnet, es sei denn, das Revisionsprotokoll ist so konfiguriert, dass sie protokolliert werden.

Drei für den Kunden sichtbare EMS-Ereignisse werden auf dem NFS-over-TLS Datenpfad ausgegeben. Details zu den Ereignissen, Auslösebedingungen und Ratenbegrenzungen sind unter "EMS-Nachrichten" zu finden.

Mandantengrenze

Die NFS over TLS Konfiguration ist pro SVM. Ein SVM-Administrator kann nur die TLS-Konfiguration auf LIFs der eigenen SVM sehen und verwalten. Cluster-Administratoren sehen alle SVMs.

Serverzertifikatsreferenzen sind SVM-lokal. Die Konfiguration wird clusterweit repliziert, sodass jeder Knoten, der einen bestimmten LIF bedient, dieselbe TLS-Konfiguration anwendet.

Bekannte sicherheitsrelevante Einschränkungen

Warnung vor selbstsignierten Zertifikaten. Die CLI `enable` und `modify`-Befehle weisen darauf hin, dass selbstsignierte Zertifikate Sie einem Man-in-the-Middle-Angriff aussetzen. Ein von einer Zertifizierungsstelle signiertes Zertifikat, das über `security certificate install` installiert wurde, sollte verwendet werden.

Mutual TLS ist optional. Mit der Standardeinstellung `-enforce-host-auth false` schützt NFS over TLS die Vertraulichkeit und Integrität der Übertragung und authentifiziert den Server gegenüber dem Client, jedoch erfolgt keine kryptografische Authentifizierung des Client-Hosts. Wenn dies erforderlich ist, muss mTLS explizit aktiviert werden.

Die ausschließliche Verwendung von TLS wird pro Exportrichtlinienregel erzwungen, nicht global. Bis `-allow-nfs-tls-only true` in der entsprechenden Exportrichtlinienregel gesetzt ist, kann derselbe LIF weiterhin Nicht-TLS-NFS-Verbindungen von Clients akzeptieren, die ansonsten durch die Regel zugelassen sind.

NFS über TLS überwachen

NFS over TLS stellt Counter Manager Zähler auf dem `nfs_tls` Objekt sowie vier EMS-Ereignisse bereit, mit denen der Verbindungsstatus und das Durchsetzungsverhalten nachverfolgt werden können.

Counter Manager-Zähler

Alle NFS-over-TLS Counter Manager-Zähler befinden sich auf dem Admin-Scope-Objekt `nfs_tls`. Diese sind mit `statistics show -object nfs_tls` einsehbar. Mit `-counter <name>` kann auf einen einzelnen Zähler gefiltert werden, oder mit `-instance` kann der Bereich auf eine bestimmte SVM oder Node-Zeile eingeschränkt werden.

Identifikator / Bezeichnungszähler (Zeichenkette):

- `nfs_tls:instance_name`--Instanzname (Bestandteil des SVM-Namens) für die Zeile.
- `nfs_tls:instance_uuid`--Instance-UUID für die Zeile (Constituent-SVM-Kennung).
- `nfs_tls:vserver_id`--SVM-Kennungsetikett für eine aggregierte Zeile.
- `nfs_tls:vserver_name`--SVM-Name-Bezeichnung für eine aggregierte Zeile.

- `nfs_tls:node_name`-- Node-Name-Label für eine aggregierte Zeile.

Verbindungs-Volume-Zähler (Rate):

- `nfs_tls:tls_total_connection_requests`--Gesamtanzahl der verarbeiteten NFS-over-TLS-Verbindungsanfragen (Erfolg + Fehler).
- `nfs_tls:tls_connection_success`erfolgreiche NFS-over-TLS Verbindungen.
- `nfs_tls:tls_disabled_connection_failures`--Verbindungen wurden abgelehnt, da NFS über TLS auf der SVM deaktiviert ist.
- `nfs_tls:tls_connection_handshake_failures`--Verbindungen, die während des TLS-Handschlags fehlgeschlagen sind.
- `nfs_tls:tls_configuration_not_found`--Verbindungsversuche wurden abgelehnt, da keine TLS-Konfiguration für das SVM/LIF-Paar existiert.
- `nfs_tls:tls_connection_mismatch`--Verbindungen, die fehlschlugen, weil die im Speicher befindliche Verbindungskennung nicht mit der während des Handschlagabschlusses beobachteten Verbindung übereinstimmte.

Latenzzähler (Durchschnitt):

- `nfs_tls:tls_handshake_average_latency`--durchschnittliche TLS-Handschlag-Latenz in Mikrosekunden. Basiszähler: `tls_connection_success`.

Meldungen des Event Management System (EMS)

Vier für Kunden sichtbare EMS-Ereignisse werden vom NFS-Server auf dem NFS-over-TLS-Datenpfad ausgegeben. Sie können sie mit `event log show` anzeigen.

`Nblade.TLSConfigError`

Schweregrad `ERR`, Ratenbegrenzung 10 Minuten. Wird ausgelöst, wenn ein Client versucht, NFS über TLS auf einer SVM/LIF ohne TLS-Konfiguration zu verwenden. Protokollierte Felder: Client-IP-Adresse, SVM-Name, LIF-IP-Adresse. Zur Behebung die Konfiguration mit `vserver nfs tls interface enable` aktivieren.

`Nblade.TLSHandshakeFailed`

Schweregrad `ERR`, rate-limitiert 10 Minuten. Wird ausgelöst, wenn der TLS-Handschlag zwischen Client und Server fehlschlägt. Protokollierte Felder: SVM-Name, LIF-IP-Adresse, Client-(Remote-)IP-Adresse, Serverzertifikat-UUID. Zur Behebung sollte die TLS-Konfiguration auf dem LIF sowie die Netzwerkgesundheit überprüft werden. Wenn das Problem weiterhin besteht, sollte NetApp Support kontaktiert werden.

`Nblade.NfsTlsDisabled`

Schweregrad `ALERT`, ratenbegrenzt für 24 Stunden. Wird ausgelöst, wenn ein Client versucht, NFS über TLS auf einer SVM zu verwenden, auf der die Funktion deaktiviert ist. Protokollierte Felder: SVM name.

`Nblade.nfsTLSAccessErr`

Schweregrad `ERR`. Wird ausgelöst, wenn ein Client, der einer Exportrichtlinienregel mit `-allow-nfs-tls -only true` entspricht, versucht, den NFS-Pfad ohne TLS einzubinden oder darauf zuzugreifen. Dieses Ereignis dient zur Bestätigung, dass Clients ohne TLS wie vorgesehen blockiert werden.

Performance

TLS verursacht zusätzliche Kosten in drei Ressourcendimensionen: CPU, Speicher und Netzwerk.

Ressourcenkostenübersicht

Die CPU ist der Hauptkostenfaktor. Der TLS 1.3-Handschlag ist ein einmaliger Aufwand pro Verbindung und umfasst asymmetrische Kryptografie, Zertifikatsanalyse und Schlüsselaustausch. Nach dem Aufbau einer Verbindung besteht der laufende Overhead in der symmetrischen Verschlüsselung von Datensätzen mit AES-GCM oder ChaCha20-Poly1305. Auf Plattformen mit Mellanox ConnectX-6 Dx (CX6-Dx) oder ConnectX-7 (CX7) NICs übernimmt die NIC selbst die Ver- und Entschlüsselung über Kernel TLS (KTLS) Offload, wodurch die laufenden CPU-Kosten deutlich reduziert werden.

Die **Memory**-Auswirkung ist gering. TLS fügt einen Sitzungsstatus pro Verbindung und einen TLS-Konfigurationscache pro Node hinzu. Die Cache-Größe ist begrenzt; Einträge werden durch die Time-To-Live (TTL) altern und im Hintergrund aktualisiert.

Der Netzwerk-Overhead ist gering. Die TLS 1.3-Datensatzformatierung verursacht einen festen Overhead pro Datensatz und ein Authentifizierungstag. Der Handschlag fügt nur beim Verbindungsaufbau zusätzliche Roundtrips hinzu, nicht pro RPC.

TLS-Leistungseinbuße

Es gibt zwei unterschiedliche Pfade für NFS über TLS in ONTAP: den Hardware-Offload-Pfad und den Software-TLS-Pfad. Der Hardware-Offload-Pfad ist auf Plattformen mit CX6-Dx oder CX7 NICs verfügbar. Der Software-TLS-Pfad wird auf Plattformen ohne Offload-fähige NICs verwendet.

Auf Plattformen mit Offload-fähigen Netzwerkkarten lag die Leistung über verschiedene Workloads hinweg innerhalb von etwa 10 % der Leistung von unverschlüsseltem NFS. Auf Plattformen ohne Offload-fähige Netzwerkkarten ist der Software-TLS-Pfad stärker von der Workload abhängig und kann im ungünstigsten Fall Durchsatzreduzierungen von etwa 30 % gegenüber unverschlüsseltem NFS aufweisen. Dies sind Charakterisierungswerte, keine garantierten Spezifikationen. Die Ergebnisse variieren je nach Workload-Typ, I/O-Größe und Verbindungsanzahl. Bei einer Mischung aus TLS- und nicht-TLS-Datenverkehr auf demselben Node ist ebenfalls mit Auswirkungen auf den nicht-TLS-Durchsatz zu rechnen.

Skalierungsfaktoren

Die folgenden Faktoren erhöhen die TLS-CPU-Kosten oder die Handschlag-Latenz:

Verbindungsfluktuation. Jede neue Verbindung verursacht die Kosten für den Handschlag. Workloads, die häufig TCP-Verbindungen zum NFS-Server öffnen und schließen, weisen eine höhere aggregierte TLS-CPU-Auslastung auf als Workloads mit langlebigen Verbindungen.

Nach einer Übernahme oder einem Netzwerkereignis können Verbindungsspitzen auftreten. Workloads, bei denen sich viele Clients gleichzeitig wieder verbinden, wie beispielsweise nach einer HA-Übernahme, zahlen die vollen Handschlag-Kosten des TLS 1.3 pro Verbindung. Verbindungsreserve sollte entsprechend überwacht `nfs_tls:tls_handshake_average_latency` und eingeplant werden.

Große Anzahl unterschiedlicher Client-Identitäten (mutual TLS). Mutual TLS (mTLS)-Implementierungen skalieren die Handschlag-CPU mit der Anzahl der zu validierenden eindeutigen Client-Zertifikate.

mTLS vs. reines Server-TLS. Die Aktivierung der Host-Authentifizierung (mTLS) führt zu einer Client-Zertifikatsvalidierung auf der Serverseite, wodurch jeder Handschlag moderat teurer wird als bei reinem

Server-TLS. Die Kosten pro RPC bleiben im Steady-State unverändert.

Taktung der TLS-Konfiguration. Häufige Änderungen an der TLS-Schnittstellenkonfiguration, wie Zertifikatsrotation oder Aktivierungs-/Deaktivierungszyklen, machen den TLS-Konfigurationscache pro Knoten ungültig und erzwingen Abfragen zurück zum Management-Host, was die Handschlag-Latenz kurzzeitig erhöht.

Interoperabilität und Grenzen

NFS over TLS ist mit den standardmäßigen ONTAP Export-Policy-Kontrollen kompatibel, wird über SVM-DR und MetroCluster repliziert und weist einige wenige harte Plattformbeschränkungen sowie Betriebsempfehlungen auf, die vor der Bereitstellung bekannt sein sollten.

Interoperabilität

Unterstützte koexistierende Funktionen

Exportrichtlinien, Qtree-Exporte und Verbindungspfade. Die Exportrichtlinienregel erhält das `-allow-nfs-tls-only` Feld, das TLS regelbasiert vorschreiben kann. Sie wird mit bestehenden Sicherheitskontrollen wie Client-Match, Protokoll, Lese-/Schreibzugriff, Superuser, Anonymität, Chown-Modus, Allow-SUID und NTFS-UNIX kombiniert. Qtree-Exporte und Verbindungspfad-Mounts erben die TLS-Anforderung über denselben Exportrichtlinienmechanismus. System Manager zeigt die `-allow-nfs-tls-only` Einstellung in der NFS-Zugriffsauswahl an.

Die NFS-over-TLS-Replikation und die DR-Unterstützung sind in der folgenden Tabelle zusammengefasst. Hintergrundinformationen zum Replikationsmechanismus finden sich unter "Architektur".

Replikation / DR	NFS über TLS in Version 9.19.1
SVM-DR	**Unterstützt.** Die TLS-Schnittstellenzeile wird auf SVM-Ebene repliziert (Status, Zertifikatsname und UUID, enforce-host-auth). Das `-allow-nfs-tls-only`export-rule Feld wird mit der Exportrichtlinie repliziert.
MetroCluster (Replikation auf SVM-Ebene)	**Unterstützt.** Gleicher Replikationspfad wie SVM-DR. Der Lebenszyklus des Zertifikatsmaterials auf der Ziel-SVM liegt beim Zertifikatsmanager.
SnapMirror (Volumenreplikation)	**Unterstützt.** Orthogonal zum Client-seitigen TLS-Transport.
Cloud-gehostete ONTAP Varianten	**Nicht unterstützt** in 9.19.1.

Funktionen mit Einschränkungen

Client-Anforderungen. Der NFS-Client muss TLS für ONC RPC gemäß "RFC 9289" implementieren. Unter Linux wird dies durch einen im Kernel integrierten NFS-Client bereitgestellt, der die `xprtsec=tls` (oder `xprtsec=mtls`) Mount-Option unterstützt und in Kombination mit dem Userspace-TLS-Handschlag-Helfer `tlshd` aus dem `ktls-utils` Paket verwendet wird. Die vollständige Client-Matrix, einschließlich minimaler Kernel-Versionen, Userspace-Paketversionen und unterstützter Linux-Distributionen, ist im Interoperability Matrix Tool (IMT) zu finden.

Einschränkungen und Vorbehalte

- **Cloud-hosted ONTAP Varianten.** Cloud Volumes ONTAP und andere Cloud-hosted ONTAP Varianten werden unter ONTAP 9.19.1 nicht unterstützt.
- **NFS über Remote Direct Memory Access (RDMA).** NFS über RDMA und NFS über TLS schließen sich auf demselben LIF gegenseitig aus.

Grenzwerte pro Knoten

Derzeit gibt es keine fest codierten Verbindungsgrenzen für NFS-over-TLS in ONTAP. Aktuelle Informationen zu den unterstützten Grenzwerten finden sich unter "Hardware Universe".

BESTE VORGEHENSWEISE: Die Anzahl der NFS-over-TLS-Verbindungen pro Knoten sollte unter 10.000 liegen, damit ausreichend Spielraum für Mount-Stürme und HA-Übernahmen bleibt.

Cluster-spezifische Beschränkungen

Es gibt keine separate clusterweite Obergrenze, die im Code durchgesetzt wird.

Grenzwerte pro LIF und pro Objekt

- Die Konfigurationstabelle ist über das `(SVM, LIF)` Tupel indiziert. Jede LIF enthält entweder null oder eine NFS-over-TLS Konfigurationszeile.
- Genau ein Serverzertifikat wird pro NFS-over-TLS-fähigem LIF gebunden. Das Zertifikat wird zum `vserver nfs tls interface enable`Zeitpunkt angegeben und kann mit `… modify -certificate-name` geändert werden.
- `-allow-nfs-tls-only` ist ein einzelner boolescher Wert pro Export-Policy-Regel. Diese Funktion fügt keine separate Obergrenze für die Regelanzahl hinzu, die standardmäßigen Maximalwerte pro Policy und pro SVM für Export-Regeln gelten.

Durchsetzungsverhalten

`-allow-nfs-tls-only true`Durchsetzung. Wenn dieses Feld `true`in einer übereinstimmenden Exportrichtlinienregel enthalten ist, werden NFS-Verbindungsversuche von übereinstimmenden Clients, die TLS für ONC RPC gemäß RFC 9289 nicht verwenden, bei der Auswertung der Exportrichtlinie abgelehnt. Bestehende TLS-Verbindungen dieser Clients sind davon nicht betroffen.

`-enforce-host-auth true`-Durchsetzung. Wenn `true` auf einem `(SVM, LIF)` TLS-Handschläge, deren Clientzertifikatsidentität nicht mit der konfigurierten Hostidentität für die LIF übereinstimmt, werden diese während des TLS-Handschlags abgelehnt. Das EMS-Ereignis `Nblade.TLSHandshakeFailed` (Schweregrad `ERR`, auf eine Meldung pro 10 Minuten und Ereignisquelle begrenzt) wird für jeden fehlgeschlagenen Handschlag ausgegeben.

EMS-Ratenbegrenzungen.
`Nblade.TLSConfigError` und `Nblade.TLSHandshakeFailed` sind auf einmal alle 10 Minuten pro Ereignisquelle begrenzt. `Nblade.NfsTlsDisabled` ist auf einmal alle 24 Stunden pro Ereignisquelle begrenzt. Dies sind beabsichtigte Obergrenzen für das Ereignisprotokollvolumen bei kontinuierlichen Fehlerbedingungen. Während eines Bursts wird nur das erste Ereignis innerhalb jedes Ratenbegrenzungsfensters protokolliert.

Weiche Grenzen und Empfehlungen

Die folgenden Angaben sind Empfehlungen, keine strikten Maximalwerte.

- **Die Anzahl der NFS-over-TLS-Verbindungen pro Knoten sollte unter 10.000 gehalten werden.** Es gibt keine fest codierte Obergrenze, jedoch sollte die Anzahl der NFS-over-TLS-Verbindungen pro Knoten bei oder unter 10.000 liegen.
- **Nach der HA-Übernahme ist ein vollständiger TLS-Re-Handschlag einzuplanen.** TLS-Sitzungen sind auf TCP beschränkt und überstehen eine Übernahme nicht. Jeder Client stellt auf dem verbleibenden oder Zielknoten eine neue TLS 1.3-Handshake-Verbindung her, sodass mit einem Mount-Sturm zu rechnen ist. Wenn die Anzahl der Verbindungen deutlich unter 10.000 gehalten wird, bleibt ausreichend Spielraum, um diesen Anstieg aufzufangen.

Technische Berichte zum ONTAP SAN

ONTAP SAN-Storage sorgt für eine vereinfachte SAN-Erfahrung und bietet Hochverfügbarkeit für geschäftskritische Datenbanken und andere SAN Workloads Ihres Unternehmens. Durch die Integration erstklassiger Datenservices in Oracle-, SAP- und Microsoft SQL Server-Datenbanken, VMware und andere führende Hypervisoren bietet ONTAP SAN eine schnellere Amortisierung für Enterprise-Datenbankapplikationen.

Diese technischen Berichte erweitern die "ONTAP SAN Storage-Management"Produktdokumentation.

"TR-4080: Best Practices für modernes SAN in ONTAP"
Erfahren Sie mehr über Blockprotokolle in ONTAP sowie Empfehlungen.

"TR-4684: Implementation and Configuring Modern SANs with NVMe over Fabrics (NVMe-of)"
Erfahren Sie, wie Sie NVMe over Fabrics-Übertragungen (NVMe over Fibre Channel und NVMe over TCP) implementieren und konfigurieren. Die Themen umfassen Design, Implementierung, Konfiguration, Management-Richtlinien und empfohlene Praktiken zum Aufbau von hochverfügbaren, hochperformanten modernen SAN-Lösungen unter Verwendung von NVMe-Protokollen und -Übertragungen.

"TR-4968: NetApp All-SAN-Array Datenverfügbarkeit und -Integrität"
Erfahren Sie, wie die verschiedenen Datenschutz- und Datenintegritätsfunktionen eines All-SAN-Array-Systems eine maximale Applikations-Uptime erreichen und empfohlene Vorgehensweisen für das Design, die Implementierung und das Management eines SAN-Netzwerks erhalten.

"Moderne SAN-Flash-Lösung mit Cloud-Integration"
Diese NetApp Verifizierte Architektur wurde von NetApp, VMware und Broadcom gemeinsam entwickelt und verifiziert. Dabei kommen die neuesten Technologielösungen von Brocade, Emulex und VMware vSphere zusammen mit NetApp All-Flash-Storage zum Einsatz, der neue Standards für SAN Storage der Enterprise-Klasse und Datensicherung setzt, die einen überragenden geschäftlichen Nutzen erzielen.

Sicherheit

Technische Berichte zur Sicherheit von ONTAP

ONTAP entwickelt sich weiter und Sicherheit ist dabei ein integraler Bestandteil der Lösung. Die neueste Version von ONTAP enthält viele neue Sicherheitsfunktionen, die für Ihr Unternehmen von unschätzbarem Wert sind, um die Daten in der gesamten Hybrid Cloud zu schützen, Ransomware-Angriffen vorzubeugen und die von der Branche empfohlenen Vorgehensweisen einzuhalten. Diese neuen Funktionen unterstützen Ihr Unternehmen außerdem dabei, sich weiter in Richtung eines Zero-Trust-Modells zu bewegen.

Diese technischen Berichte erweitern die "ONTAP Sicherheit und Datenverschlüsselung"Produktdokumentation.

Cyber-Vault: ONTAP

"Cyber-Vault: ONTAP" Die auf ONTAP basierende Cyber-Vault von NetApp bietet Unternehmen eine umfassende und flexible Lösung für den Schutz ihrer wichtigsten Datenbestände. Dank der Nutzung logischer Air-Gapping-Verfahren zur robusten Härtung können Sie mit ONTAP sichere, isolierte Storage-Umgebungen erstellen, die gegen neue Cyberbedrohungen gewappnet sind. Mit ONTAP gewährleisten Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten und profitieren gleichzeitig von der Agilität und Effizienz Ihrer Storage-Infrastruktur.

Ransomware

"TR-4572: Die NetApp Lösung für Ransomware" Erfahren Sie, wie sich Ransomware weiterentwickelt hat, und wie Sie Angriffe identifizieren, die Ausbreitung verhindern und mit der NetApp Lösung für Ransomware so schnell wie möglich wiederherstellen können. Die in diesem Dokument enthaltenen Anleitungen und Lösungen sollen Unternehmen dabei helfen, über Cyber-resiliente Lösungen zu verfügen und gleichzeitig ihre vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu erfüllen.

"TR-4526: Konformer WORM Storage mit NetApp SnapLock"
Viele Unternehmen setzen auf WORM-Storage (Write Once, Read Many), um gesetzliche Vorgaben einzuhalten oder einfach nur um eine weitere Schicht zu ihrer Datensicherungsstrategie hinzuzufügen. Erfahren Sie, wie Sie SnapLock, die WORM-Lösung in ONTAP, in Umgebungen integrieren, die WORM-Datenspeicher erfordern.

Zero Trust

"NetApp und Zero Trust" Zero Trust war bisher ein netzwerkorientierter Ansatz der Architektur von Microcore and Perimeter (MCAP) zum Schutz von Daten, Services, Applikationen oder Assets mit Kontrolloptionen, die als Segmentierungsgateway bekannt sind. ONTAP verfolgt für Zero Trust einen Daten-orientierten Ansatz, bei dem das Storage-Managementsystem zum Segmentierungs-Gateway wird, um die Daten unserer Kunden zu schützen und den Zugriff darauf zu überwachen. Insbesondere die FPolicy Zero Trust Engine und das FPolicy Partner-Ecosystem werden zum Kontrollzentrum, um normale und fehlende Datenzugriffsmuster detailliert zu verstehen und Bedrohungen von innen zu erkennen.

Multi-Faktor-Authentifizierung

"TR-4647: Multi-Faktor-Authentifizierung in ONTAP Best Practices and Implementation Guide"
Informieren Sie sich über die Multi-Faktor-Authentifizierung von ONTAP für administrativen Zugriff über System Manager, Active IQ Unified Manager und ONTAP Secure Shell (SSH)-CLI-Authentifizierung.

"TR-4717: ONTAP-SSH-Authentifizierung mit einer gemeinsamen Zugriffskarte"
Erfahren Sie, wie Sie SSH-Clients von Drittanbietern in Verbindung mit der ActivClient-Software konfigurieren und testen, um einen ONTAP-Storage-Administrator über den öffentlichen Schlüssel zu authentifizieren, der auf einer Common Access Card (CAC) gespeichert ist, wenn er in ONTAP konfiguriert ist.

Mandantenfähigkeit

"TR-4160: Sichere Mandantenfähigkeit in ONTAP"
Erfahren Sie, wie Sie mithilfe von Storage-VMs in ONTAP sichere Mandantenfähigkeit implementieren. Hierzu gehören auch Entwurfsüberlegungen und empfohlene Vorgehensweisen.

Standards

"TR-4401: PCI-DSS 4.0 und ONTAP"
Erfahren Sie, wie Sie ein System anhand des PCI DSS 4.0-Standards validieren und die Anforderungen der für ein NetApp ONTAP-System geltenden Kontrollen erfüllen.

Attributbasierte Zugriffssteuerung

"Attributbasierte Zugriffssteuerung mit ONTAP" Erfahren Sie, wie Sie die NFSv4.2-Sicherheitsetiketten und erweiterten Attribute (xattrs) konfigurieren, um die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und die attributbasierte Zugriffskontrolle (ABAC) zu unterstützen. Dabei handelt es sich um eine Autorisierungsstrategie, die Berechtigungen auf Basis von Benutzer-, Ressourcen- und Umgebungsattributen definiert.

NetApp Lösung für Ransomware

Ransomware und das Datensicherungsportfolio von NetApp

Ransomware ist nach wie vor eine der größten Bedrohungen, die 2024 für Geschäftsunterbrechungen verantwortlich sind. Laut den "Sophos State of Ransomware 2024", Ransomware-Angriffe betroffen 72 % der befragten Publikum . Ransomware-Angriffe sind heute raffinierter und gezielter ausgeführt. Bedrohungsakteure setzen fortschrittliche Techniken wie künstliche Intelligenz ein, um ihre Wirkung und ihren Gewinn zu maximieren.

Unternehmen müssen die gesamte Sicherheitslage in ihren Bereichen wie Umgebung, Netzwerk, Identität, Applikation und Speicherort der Daten auf Storage-Ebene prüfen und diese Ebenen sichern. In der heutigen Bedrohungslandschaft wird ein datenorientierter Ansatz für Cyberschutz auf Storage-Ebene eingeführt. Obwohl keine einzige Lösung alle Angriffe vereiteln kann, bietet die Verwendung eines Portfolios von Lösungen, einschließlich Partnerschaften und Dritter, eine mehrstufige Verteidigung.

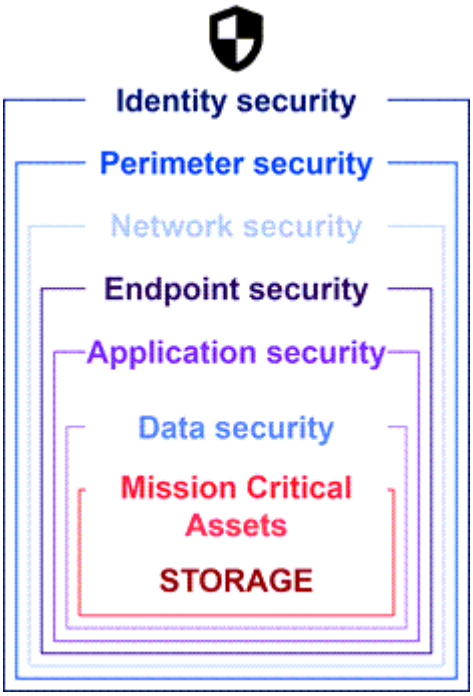
Das NetApp Produktportfolio bietet verschiedene effektive Tools für Transparenz, Erkennung und Problembehebung, damit Sie Ransomware frühzeitig erkennen, eine Ausbreitung vermeiden und bei Bedarf schnell eine Wiederherstellung durchführen können, um kostspielige Ausfallzeiten zu vermeiden. Traditionelle

mehrschichtige Verteidigungslösungen sind nach wie vor weit verbreitet, ebenso wie Lösungen von Drittanbietern und Partnern für Transparenz und Erkennung. Eine effektive Gegenmaßnahmen sind nach wie vor ein wichtiger Teil der Reaktion auf Bedrohungen. Der einzigartige Branchenansatz, der die unveränderliche NetApp Snapshot Technologie und die logische Air Gap-Lösung von SnapLock nutzt, ist ein Alleinstellungsmerkmal in der Branche und die Best Practice zur Behebung von Ransomware-Angriffen.

Ab Juli 2024 ist der Inhalt des zuvor als PDF veröffentlichten technischen Berichts *TR-4572: NetApp Ransomware Protection* auf docs.netapp.com verfügbar.

Daten sind das primäre Ziel

Cyberkriminelle setzen Daten zunehmend direkt ins Visier und erkennen ihren Wert. Die Sicherheit von Umgebung, Netzwerk und Anwendung ist zwar wichtig, kann aber umgangen werden. Die Storage-Ebene konzentriert sich auf den Schutz der Daten an der Quelle und stellt eine entscheidende letzte Verteidigungslinie dar. Ziel von Ransomware-Angriffen ist es, Zugang zu Produktionsdaten zu erhalten und sie zu verschlüsseln oder unzugänglich zu machen. Um dorthin zu gelangen, müssen Angreifer bereits vorhandene Verteidigungsmechanismen durchbohrt haben, die von Unternehmen heute eingesetzt werden, von Perimeter bis Anwendungssicherheit.



Leider nutzen viele Unternehmen die Sicherheitsfunktionen auf Datenebene nicht. An dieser Stelle kommt das NetApp Portfolio für Ransomware-Schutz ins Spiel, das Sie in der letzten Verteidigungslinie schützt.

Die realen Kosten von Ransomware

Die Lösegeldzahlung selbst ist nicht der größte monetäre Effekt auf ein Unternehmen. Obwohl die Zahlung nicht unbedeutend ist, verblasst sie im Vergleich zu den Downtime-Kosten, die durch einen Ransomware-Vorfall verursacht werden.

Lösegeldzahlungen sind nur ein Element der Recovery-Kosten im Zusammenhang mit Ransomware-Ereignissen. Ohne gezahlte Lösegeld gaben 2024 Unternehmen nach einem Ransomware-Angriff durchschnittliche Kosten für "2024 Sophos State of Ransomware" die Wiederherstellung von 2,73 Millionen US-Dollar an. Dies entspricht einem Anstieg von fast 1 Millionen US-Dollar gegenüber den 1,82 Millionen US-Dollar, die 2023 laut Bericht gemeldet wurden. Für Unternehmen, die stark von der IT-Verfügbarkeit abhängig

sind, wie E-Commerce, Aktienhandel und Gesundheitswesen, können die Kosten 10-mal höher oder höher sein.

Auch die Kosten für Cyberversicherungen steigen weiter, da die Wahrscheinlichkeit eines Ransomware-Angriffs auf Versicherte sehr hoch ist.

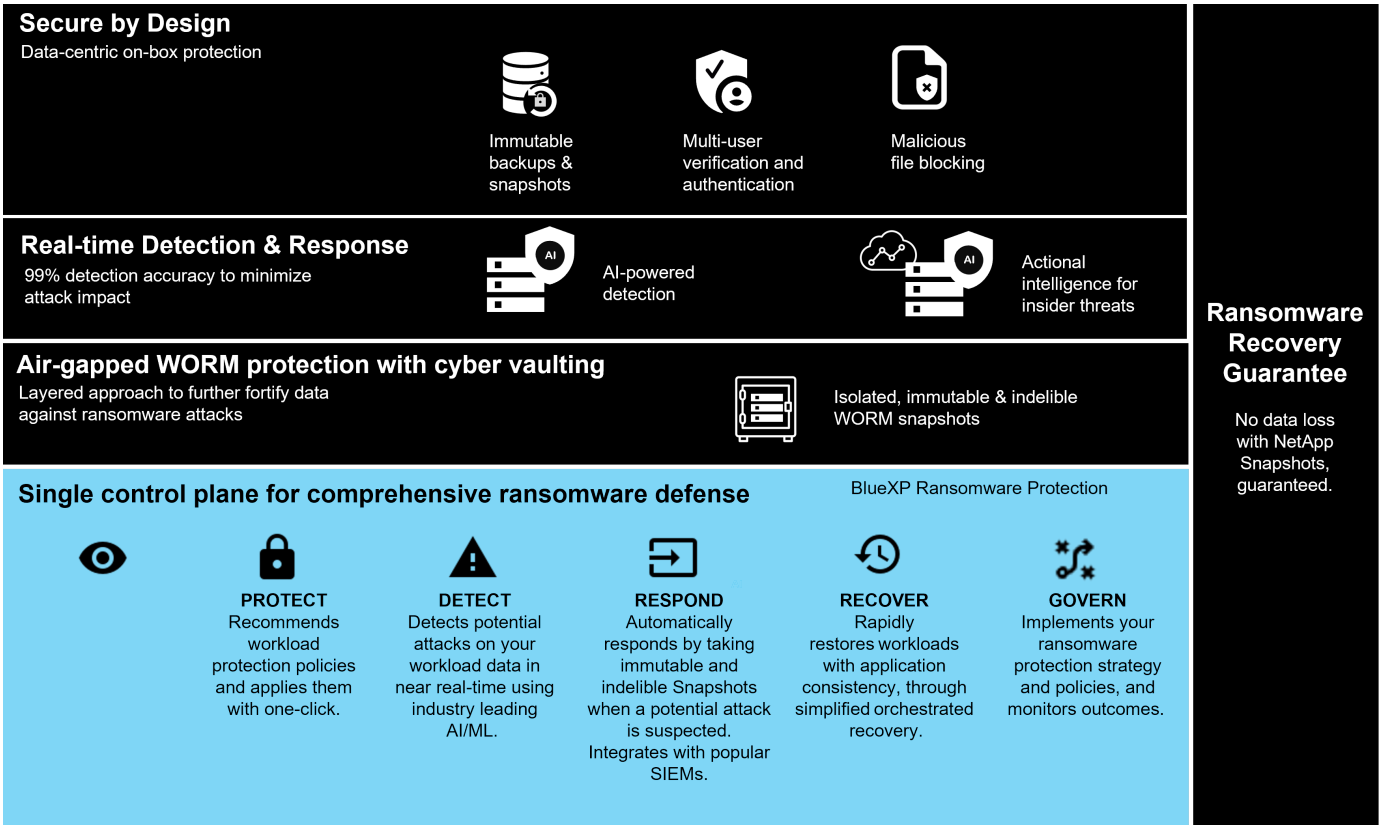
Schutz vor Ransomware auf Datenebene

NetApp versteht die umfassende Sicherheit Ihres Unternehmens, von der Umgebung bis zum Speicherort Ihrer Daten auf der Storage-Ebene. Ihr Sicherheits-Stack ist komplex und sollte Sicherheit auf jeder Ebene Ihres Technologie-Stacks bieten.

Der Echtzeitschutz auf Datenebene ist noch wichtiger und hat spezielle Anforderungen. Um effektiv zu sein, müssen Lösungen auf dieser Ebene folgende wichtige Attribute aufweisen:

- **Sicherheit durch Design**, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren
- * Echtzeit-Erkennung und Reaktion*, um die Auswirkungen eines erfolgreichen Angriffs zu minimieren
- **Air-Gap WORM-Schutz** zur Isolierung kritischer Daten-Backups
- **Eine einzelne Kontrollebene** für umfassende Ransomware-Verteidigung

NetApp kann all dies und noch mehr bieten.



Das NetApp Portfolio für Ransomware-Schutz

NetApp "Integrierter Ransomware-Schutz"bietet robusten und vielseitigen Schutz Ihrer kritischen Daten in Echtzeit. Im Kern überwachen fortschrittliche KI-gestützte Erkennungsalgorithmen kontinuierlich die Datenmuster und identifizieren potenzielle Ransomware-Bedrohungen schnell mit einer Genauigkeit von 99 %. Durch schnelle Reaktion auf Angriffe kann unser Storage schnell Snapshot von Daten erstellen und die Kopien

sichern, was zu einer schnellen Wiederherstellung führt.

Zur weiteren Stärkung der Daten "Cyber-Vaulting"isoliert die Funktion von NetApp Daten über einen logischen Air Gap. Durch den Schutz wichtiger Daten gewährleisten wir eine schnelle Business Continuity.

NetApp"NetApp Ransomware-Schutz" reduziert den Betriebsaufwand mit einer einzigen Steuerungsebene zur intelligenten Koordination und Ausführung einer durchgängigen, Workload-zentrierten Ransomware-Abwehr. So können Sie gefährdete kritische Workload-Daten mit einem einzigen Klick identifizieren und schützen, die Auswirkungen eines potenziellen Angriffs präzise und automatisch erkennen und darauf reagieren, um diese zu begrenzen, und Workloads innerhalb von Minuten (nicht Tagen) wiederherstellen. So bleiben Ihre wertvollen Workload-Daten geschützt und kostspielige Unterbrechungen werden minimiert.

Als native, integrierte ONTAP-Lösung zum Schutz von unberechtigtem Zugriff auf Daten "Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)"verfügt über eine robuste Reihe von Funktionen, die dafür sorgen, dass Vorgänge wie Löschen von Volumes, Erstellen zusätzlicher administrativer Benutzer oder Löschen von Snapshots nur nach Genehmigung durch mindestens einen zweiten designierten Administrator ausgeführt werden können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen. Sie können so viele festgelegte Administratorgenehmiger konfigurieren, wie Sie möchten, bevor ein Snapshot gelöscht werden kann.

NetApp ONTAP erfüllt die Anforderungen an webbasierte "Multi-Faktor-Authentifizierung (MFA)" System Manager und an die SSH CLI-Authentifizierung.

Der NetApp Schutz vor Ransomware sorgt in einer sich ständig weiterentwickelnden Bedrohungslandschaft für ein gutes Gefühl. Ihr umfassender Ansatz schützt nicht nur vor aktuellen Ransomware-Varianten, sondern passt sich auch neuen Bedrohungen an. So bietet er langfristige Sicherheit für Ihre Dateninfrastruktur.

Weitere Schutzoptionen

- "Digital Advisor Ransomware-Schutz"
- "Data Infrastructure Insights Speicher-Workload-Sicherheit"
- "FPolicy"
- "SnapLock und manipulationssichere Snapshots"

Recovery-Garantie bei Ransomware

NetApp bietet die Garantie, Snapshot-Daten bei einem Ransomware-Angriff wiederherzustellen. Unser Versprechen: Wenn wir Ihnen bei der Wiederherstellung Ihrer Snapshot-Daten nicht helfen können, machen wir es richtig. Die Garantie gilt für Neukäufe von AFF Systemen der A-Serie, AFF C-Serie, ASA und FAS.

Weitere Informationen .

- "Recovery Garantie Servicebeschreibung"
- "Blog zur Recovery-Garantie von Ransomware".

Verwandte Informationen

- "Ressourcen-Seite auf der NetApp Support Site"
- "NetApp Produktsicherheit"

SnapLock und manipulationssichere Snapshots für den Schutz vor Ransomware

Eine entscheidende Waffe im Snap-Arsenal von NetApp ist SnapLock, das sich beim Schutz vor Ransomware-Bedrohungen als äußerst effektiv erwiesen hat. Indem

SnapLock das Löschen von Daten durch Unbefugte verhindert, bietet es eine zusätzliche Sicherheitsschicht, die auch bei Angriffen die Unversehrtheit und den Zugriff auf kritische Daten sicherstellt.

SnapLock-Compliance

SnapLock Compliance (SLC) bietet unlöschbaren Schutz Ihrer Daten. SLC verhindert das Löschen von Daten, selbst wenn ein Administrator versucht, das Array neu zu initialisieren. Im Gegensatz zu anderen Konkurrenzprodukten ist SnapLock Compliance nicht anfällig für Social Engineering-Hacks durch die Support-Teams dieser Produkte. Daten, die durch SnapLock Compliance Volumes geschützt sind, können wiederhergestellt werden, bis sie ihr Ablaufdatum erreicht haben.

Zur Aktivierung von SnapLock "ONTAP One"ist eine Lizenz erforderlich.

Weitere Informationen .

- "SnapLock Dokumentation"

Manipulationssichere Snapshots

Manipulationssichere Snapshot Kopien (TPS) bieten eine praktische und schnelle Möglichkeit, Daten vor böswilligen Handlungen zu schützen. Im Gegensatz zu SnapLock Compliance wird TPS in der Regel auf Primärsystemen verwendet, auf denen der Benutzer die Daten für einen bestimmten Zeitraum schützen und lokal für schnelle Wiederherstellungen belassen kann oder wenn Daten nicht vom Primärsystem repliziert werden müssen. TPS verwendet SnapLock-Technologien, um zu verhindern, dass der primäre Snapshot auch von einem ONTAP-Administrator gelöscht wird, der dieselbe SnapLock-Aufbewahrungsfrist verwendet. Das Löschen von Snapshots wird auch dann verhindert, wenn das Volume nicht SnapLock aktiviert ist, obwohl Snapshots nicht dieselbe unlöschbare Eigenschaft von SnapLock Compliance Volumes aufweisen.

Um Snapshots manipulationssicher zu machen, ist eine "ONTAP One" Lizenz erforderlich.

Weitere Informationen .

- "Sperren Sie einen Snapshot, um sich vor Ransomware-Angriffen zu schützen".

FPolicy Dateisperrung

FPolicy verhindert das Speichern unerwünschter Dateien auf einer Storage Appliance der Enterprise-Klasse. FPolicy bietet Ihnen auch eine Möglichkeit, bekannte Ransomware-Dateierweiterungen zu blockieren. Ein Benutzer hat weiterhin volle Zugriffsrechte auf den Home-Ordner, aber FPolicy lässt es einem Benutzer nicht zu, Dateien zu speichern, die von seinem Administrator als blockiert markiert wurden. Es spielt keine Rolle, ob diese Dateien MP3-Dateien oder bekannte Ransomware-Dateierweiterungen sind.

Blockieren Sie bösartige Dateien mit dem nativen FPolicy-Modus

Der native Modus von NetApp FPolicy (eine Weiterentwicklung des Namens, Dateirichtlinie) ist ein blockierendes Framework mit Dateierweiterungen, mit dem Sie unerwünschte Dateierweiterungen je nach Eingang in Ihre Umgebung blockieren können. Seit über einem Jahrzehnt ist ONTAP Cloud Teil von ONTAP. Es ist unglaublich hilfreich, wenn es darum geht, Sie beim Schutz vor Ransomware zu unterstützen. Diese Zero Trust Engine ist wertvoll, weil Sie zusätzliche Sicherheitsmaßnahmen erhalten, die über die Zugriffssteuerungslisten (ACL)-Berechtigungen hinausgehen.

Im ONTAP System Manager und der NetApp Console steht eine Liste mit über 3000 Dateierweiterungen als

Referenz zur Verfügung.

> Einige Erweiterungen können in Ihrer Umgebung legitim sein, und das Blockieren kann zu unerwarteten Problemen führen. Erstellen Sie zunächst Ihre eigene Liste, die für die jeweilige Umgebung geeignet ist, bevor Sie native FPolicy konfigurieren.

Der native FPolicy-Modus ist in allen ONTAP Lizenzen enthalten.

Weitere Informationen .

- "Blog: Kampf gegen Ransomware: Teil drei – ONTAP FPolicy, ein weiteres leistungsstarkes natives Tool (aka kostenlos)"

Aktivieren Sie UEBA (User and Entity Behavior Analytics) mit dem externen FPolicy-Modus

Der externe FPolicy-Modus ist ein Benachrichtigungs- und Kontrollframework für die Dateiaktivität, das eine Übersicht über die Datei- und Benutzeraktivität bietet. Diese Benachrichtigungen können von einer externen Lösung verwendet werden, um KI-basierte Analysen durchzuführen, um schädliches Verhalten zu erkennen.

Der externe FPolicy-Modus kann auch so konfiguriert werden, dass er auf die Genehmigung des FPolicy-Servers wartet, bevor bestimmte Aktivitäten durchlaufen werden. Mehrere Richtlinien wie diese können auf einem Cluster konfiguriert werden, was für ein hohes Maß an Flexibilität sorgt.

> FPolicy-Server müssen auf FPolicy-Anfragen reagieren, wenn sie für eine Genehmigung konfiguriert sind. Andernfalls kann die Storage-System-Performance beeinträchtigt werden.

Der externe FPolicy-Modus ist in enthalten"Alle ONTAP Lizenzen".

Weitere Informationen .

- "Blog: Kampf gegen Ransomware: Teil vier – UBA und ONTAP mit FPolicy externen Modus."

Data Infrastructure Insights Speicher-Workload-Sicherheit

Storage Workload Security (SWS) ist eine Funktion von NetApp Data Infrastructure Insights, die die Sicherheitslage, Wiederherstellbarkeit und Verantwortlichkeit einer ONTAP Umgebung erheblich verbessert. SWS verfolgt einen benutzerzentrierten Ansatz und verfolgt alle Dateiaktivitäten jedes authentifizierten Benutzers in der Umgebung. Es verwendet erweiterte Analysen, um normale und saisonale Zugriffsmuster für jeden Benutzer zu ermitteln. Diese Muster werden verwendet, um verdächtiges Verhalten schnell zu erkennen, ohne dass Ransomware-Signaturen erforderlich sind.

Wenn SWS eine potenzielle Ransomware oder Datenlöschung erkennt, kann es beispielsweise folgende automatische Maßnahmen ergreifen:

- Erstellen Sie einen Snapshot des betroffenen Volumes.
- Blockieren Sie das Benutzerkonto und die IP-Adresse, die möglicherweise von schädlicher Aktivität vermutet werden.
- Senden Sie eine Benachrichtigung an Administratoren.

Da SWS automatisierte Maßnahmen ergreifen kann, um Bedrohungen von innen schnell zu stoppen und alle Dateiaktivitäten zu verfolgen, macht die Recovery nach einem Ransomware-Ereignis erheblich einfacher und schneller. Mit den integrierten erweiterten Tools für die Prüfung und Forensik können Benutzer sofort sehen,

welche Volumes und Dateien von einem Angriff betroffen waren, von welchem Benutzerkonto der Angriff stammte und welche böswilligen Aktionen ausgeführt wurden. Automatische Snapshots verringern den Schaden und beschleunigen die Dateiwiederherstellung.

Warnmeldungen aus dem Autonomen Ransomware-Schutz (ARP) von ONTAP sind auch in SWS sichtbar und bieten Kunden, die sowohl ARP als auch SWS zum Schutz vor Ransomware-Angriffen verwenden, eine einzige Schnittstelle.

Weitere Informationen .

- "Einblicke in die NetApp Data Infrastructure Insights"

In NetApp ONTAP integrierte, KI-basierte Erkennung und Reaktion

Ransomware-Bedrohungen werden immer raffinierter – auch Ihre Abwehrmechanismen sollten sich auswachsen. Der autonome Ransomware-Schutz (ARP) von NetApp wird über KI mit intelligenter Anomalieerkennung bereitgestellt, die in ONTAP integriert ist. Aktivieren Sie diese Möglichkeit, um Ihre Cyber-Resilienz um eine weitere Verteidigungsebene zu erweitern.

ARP und ARP/AI können über die integrierte Management-Schnittstelle von ONTAP, System Manager, konfiguriert und für einzelne Volumes aktiviert werden.

Autonomer Schutz durch Ransomware (ARP)

Autonomous Ransomware Protection (ARP), eine weitere seit 9.10.1 integrierte native ONTAP-Lösung, untersucht die Dateiaktivität und Datenentropie des NAS-Storage-Volumes, um potenzielle Ransomware-Angriffe automatisch zu erkennen. ARP bietet Administratoren Erkennung in Echtzeit, Einblicke und einen Punkt für die Daten-Recovery für eine nie dagewesene Erkennung potenzieller Ransomware.

Bei ONTAP 9.15.1 und älteren Versionen, die ARP unterstützen, startet ARP im Lernmodus, um die typische Workload-Datenaktivität zu erlernen. Dies kann in den meisten Umgebungen sieben Tage dauern. Nach Abschluss des Lernmodus wechselt ARP automatisch in den aktiven Modus und sucht nach abnormalen Workload-Aktivitäten, die möglicherweise eine Ransomware sein könnten.

Wenn eine anormale Aktivität erkannt wird, wird sofort ein automatischer Snapshot erstellt. Dieser bietet einen Wiederherstellungspunkt, der dem Zeitpunkt des Angriffs mit minimalen infizierten Daten so nahe wie möglich liegt. Gleichzeitig wird eine automatische Warnung (konfigurierbar) generiert, mit der Administratoren die anormalen Dateiaktivitäten sehen können, damit sie feststellen können, ob die Aktivität tatsächlich schädlich ist, und entsprechende Maßnahmen ergreifen können.

Wenn es sich bei der Aktivität um eine zu erwartende Arbeitslast handelt, können Administratoren sie leicht als

falsch positiv markieren. ARP lernt diese Änderung als normale Workload-Aktivität und markiert sie nicht mehr als einen potenziellen Angriff in der Zukunft.

Um ARP zu aktivieren, "ONTAP One"ist eine Lizenz erforderlich.

Weitere Informationen .

- "Autonomer Schutz Durch Ransomware"

Autonomer Ransomware-Schutz/KI (ARP/AI)

ARP/AI wurde als Tech Preview in ONTAP 9.15.1 eingeführt und ermöglicht eine neue Stufe der Echtzeiterkennung von NAS-Storage-Systemen. Die neue KI-gestützte Erkennungstechnologie ist mit über einer Million Dateien und verschiedenen bekannten Ransomware-Angriffen trainiert. Neben den in ARP verwendeten Signalen erkennt ARP/AI auch die Header-Verschlüsselung. Dank der AI-Leistung und der zusätzlichen Signale kann ARP/AI eine Erkennungsgenauigkeit von über 99 % erzielen. Dies wurde von SE Labs validiert, einem unabhängigen Testlabor, das ARP/AI die höchste AAA-Bewertung verlieh.

Da das Training der Modelle kontinuierlich in der Cloud stattfindet, ist für ARP/AI kein Lernmodus erforderlich. Er ist aktiv, sobald er eingeschaltet wird. Ein kontinuierliches Training bedeutet auch, dass ARP/AI immer gegen neue Arten von Ransomware-Angriffen validiert wird, sobald sie auftreten. ARP/AI verfügt außerdem über Funktionen für automatische Updates, die für alle Kunden neue Parameter bereitstellen, um die Ransomware-Erkennung auf dem neuesten Stand zu halten. Alle anderen Erkennungs-, Erkennungs- und Wiederherstellungspunkt-Funktionen von ARP werden für ARP/AI gepflegt.

Um ARP/AI "ONTAP One"zu aktivieren, ist eine Lizenz erforderlich.

Weitere Informationen .

- "Blog: Die KI-basierte Echtzeit-Ransomware-Erkennungslösung von NetApp erreicht AAA-Bewertung"

Luftgewindelter WORM-Schutz mit Cyber-Vaulting in ONTAP

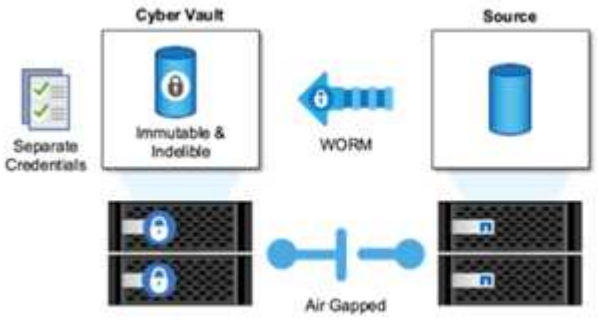
Der Ansatz von NetApp bei einer Cyber-Vault ist eine speziell entwickelte Referenzarchitektur für eine logisch luftgefragte Cyber-Vault. Dieser Ansatz nutzt Technologien zur Erhöhung der Sicherheit und Compliance wie SnapLock, um unveränderliche und nicht löschbare Snapshots zu ermöglichen.

Cyber-Vaulting mit SnapLock Compliance und eine logische Luftspalt

Ein wachsender Trend ist für Angreifer, die Sicherungskopien zu zerstören und in einigen Fällen sogar zu verschlüsseln. Aus diesem Grund empfehlen viele in der Cybersecurity-Branche, Air Gap-Backups als Teil einer umfassenden Cyber-Resilienz-Strategie zu verwenden.

Das Problem besteht darin, dass herkömmliche Luftspalten (Band- und Offline-Medien) die Wiederherstellungszeit erheblich erhöhen können und somit die Ausfallzeiten und die damit verbundenen Gesamtkosten erhöhen. Auch ein moderner Ansatz für eine Luftspaltlösung kann sich als problematisch erweisen. Wenn beispielsweise der Backup-Vault vorübergehend geöffnet wird, um neue Sicherungskopien zu erhalten, und dann die Verbindung zu den primären Daten getrennt und die Netzwerkverbindung geschlossen wird, um wieder „Air Gap“ zu erhalten, kann ein Angreifer die temporäre Öffnung nutzen. Während der Online-Verbindung kann ein Angreifer die Daten kompromittieren oder zerstören. Durch diese Art von Konfiguration wird auch in der Regel unerwünschte Komplexität erhöht. Eine logische Luftspalte ist ein ausgezeichneter Ersatz für eine traditionelle oder moderne Luftspalte, weil sie die gleichen Sicherheitsschutzprinzipien hat und gleichzeitig das Backup online hält. Mit NetApp lösen Sie die Komplexität von Tape- oder Festplattenluftapping mit logischem Air Gating, das sich mit unveränderlichen Snapshots und NetApp SnapLock Compliance

erreichen lässt.



NetApp hat die Funktion SnapLock vor mehr als 10 Jahren veröffentlicht, um den Anforderungen an die Daten-Compliance gerecht zu werden, beispielsweise den Health Insurance Portability and Accountability Act (HIPAA), den Sarbanes-Oxley Act (Sarbanes-Oxley) und weitere gesetzliche Datenvorschriften. Sie können außerdem primäre Snapshots in SnapLock Volumes speichern, um den WORM-Vorgang durchzuführen und so das Löschen zu verhindern. Es gibt zwei SnapLock-Lizenzversionen: SnapLock Compliance und SnapLock Enterprise. Als Schutz vor Ransomware empfiehlt NetApp SnapLock Compliance, da Sie einen bestimmten Aufbewahrungszeitraum festlegen können, in dem Snapshots gesperrt sind. Snapshots können selbst von ONTAP Administratoren oder der Unterstützung von NetApp nicht gelöscht werden.

Weitere Informationen .

- "Blog: Übersicht über die ONTAP Cyber-Vault"

Manipulationssichere Snapshots

SnapLock Compliance als logische Air Gap bietet Ihnen den ultimativen Schutz, um zu verhindern, dass Angreifer Ihre Backup-Kopien löschen. Allerdings müssen Sie die Snapshots mit SnapVault auf ein sekundäres Volume mit SnapLock-Aktivierung verschieben. Daher implementieren viele Kunden diese Konfiguration auf einem Sekundärspeicher im gesamten Netzwerk. Dies kann zu längeren Wiederherstellungszeiten führen, im Gegensatz zur Wiederherstellung eines Snapshots eines primären Volumes auf dem Primärspeicher.

Ab ONTAP 9.12.1 bieten manipulationssichere Snapshots Schutz auf SnapLock Compliance-Ebene für Ihre Snapshots auf dem primären Storage und in primären Volumes nahe an. Es ist nicht erforderlich, den Snapshot mit SnapVault auf ein sekundäres SnapLocked-Volume zu speichern. Manipulationssichere Snapshots setzen die SnapLock Technologie ein, um zu verhindern, dass der primäre Snapshot gelöscht wird, selbst wenn ein vollständiger ONTAP Administrator dieselbe Aufbewahrungsfrist für SnapLock verwendet. Dies sorgt für schnellere Wiederherstellungszeiten und die Möglichkeit, dass ein FlexClone-Volume durch einen manipulationssicheren, geschützten Snapshot gesichert wird. Dies ist mit einem herkömmlichen, archivierten SnapLock Compliance Snapshot nicht möglich.

Der Hauptunterschied zwischen SnapLock Compliance und manipulationssicheren Snapshots besteht darin, dass SnapLock Compliance das ONTAP-Array nicht initialisiert und gelöscht werden kann, wenn SnapLock Compliance-Volumes mit archivierten Snapshots existieren, die ihr Ablaufdatum noch nicht erreicht haben. Um Snapshots manipulationssicher zu machen, ist eine SnapLock Compliance Lizenz erforderlich.

Weitere Informationen .

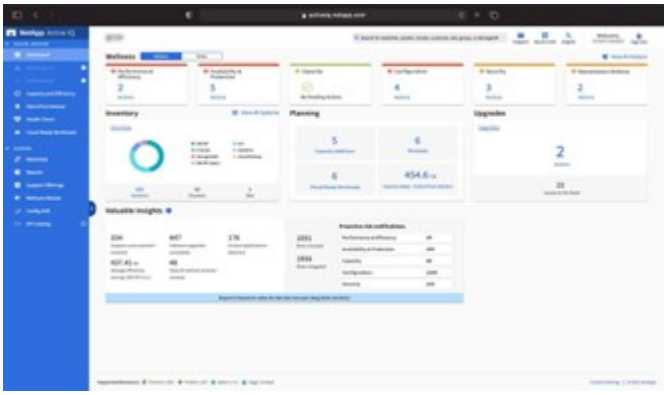
- "Sperren Sie einen Snapshot, um sich vor Ransomware-Angriffen zu schützen"

Digital Advisor Ransomware-Schutz

Digital Advisor powered by Active IQ vereinfacht die proaktive Pflege und Optimierung

von NetApp Storage mit umsetzbarer Intelligenz für optimales Datenmanagement. Gestützt auf Telemetriedaten aus unserer hochdiversen Installationsbasis nutzt es fortschrittliche KI- und ML-Techniken, um Möglichkeiten zur Risikominderung sowie zur Verbesserung der Leistung und Effizienz Ihrer Speicherumgebung aufzudecken.

Nicht nur kann "Digitaler Berater von NetApp" helfen "Beseitigung von Sicherheitslücken", sondern es bietet auch Einblicke und Anleitungen speziell zum Schutz vor Ransomware. Eine spezielle Statuskarte zeigt die erforderlichen Maßnahmen und die adressierten Risiken an, sodass Sie sicher sein können, dass Ihre Systeme den Empfehlungen für bewährte Verfahren entsprechen.



Zu den Risiken und Maßnahmen, die auf der Seite „Ransomware Defense Wellness“ nachverfolgt werden, gehören Folgendes (und vieles mehr):

- Die Anzahl der Volume-Snapshots ist niedrig. Dies verringert den potenziellen Schutz vor Ransomware.
- FPolicy ist nicht für alle Storage Virtual Machines (SVMs) aktiviert, die für NAS-Protokolle konfiguriert sind.

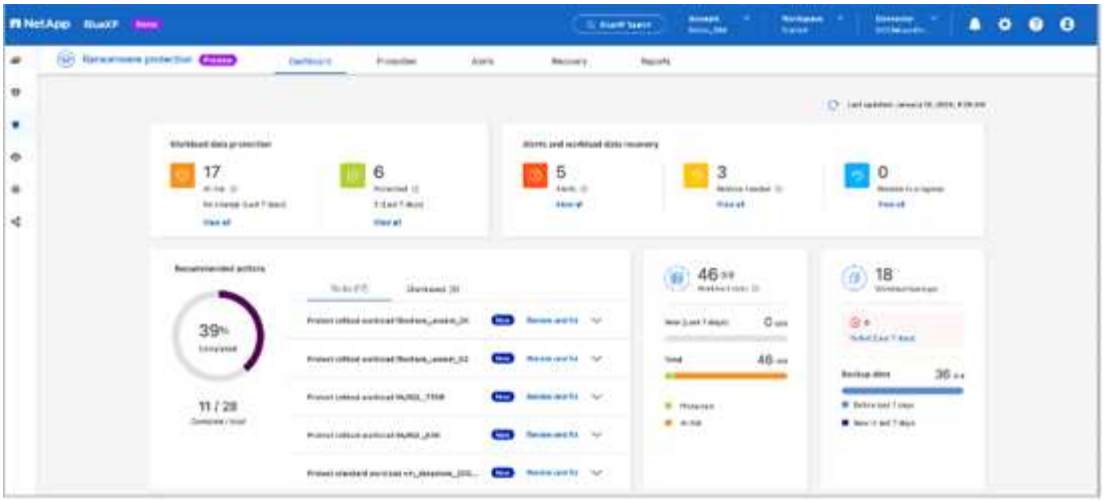
Ein Beispiel für den Ransomware-Schutz findet sich unter "Digital Advisor".

Umfassende Ausfallsicherheit mit NetApp Ransomware-Schutz

Es ist wichtig, dass Ransomware so früh wie möglich erkannt wird, damit Sie die Verbreitung verhindern und kostspielige Ausfallzeiten vermeiden können. Eine wirksame Strategie zur Erkennung von Ransomware sollte jedoch mehr als nur eine Schutzebene umfassen. Der Ransomware-Schutz von NetApp verfolgt einen umfassenden Ansatz, der Echtzeit-On-Box-Funktionen umfasst, die sich über die NetApp Console auf Datendienste erstrecken, sowie eine isolierte, mehrschichtige Lösung für Cyber-Vaulting.

NetApp Ransomware-Schutz

Die NetApp Console ist eine einzelne Steuerebene zur intelligenten Orchestrierung einer umfassenden, Workload-zentrierten Ransomware-Abwehr. Der NetApp Ransomware-Schutz vereint die leistungsstarken Cyber-Resilience-Funktionen von ONTAP, wie ARP, FPolicy und manipulationssichere Snapshots, und NetApp -Datendienste, wie NetApp Backup and Recovery. Darüber hinaus werden Empfehlungen und Anleitungen mit automatisierten Workflows hinzugefügt, um eine End-to-End-Verteidigung über eine einzige Benutzeroberfläche bereitzustellen. Es arbeitet auf Workload-Ebene, um sicherzustellen, dass die Anwendungen, die Ihr Unternehmen betreiben, geschützt sind und im Falle eines Angriffs so schnell wie möglich wiederhergestellt werden können.



Kundenvorteile:

- Durch unterstützte Ransomware-Vorbereitung wird der betriebliche Overhead verringert und die Effizienz verbessert
- Die KI/ML-gestützte Anomalieerkennung bietet eine höhere Genauigkeit und schnellere Reaktionen zur Eindämmung von Risiken
- Mithilfe der applikationskonsistenten Wiederherstellung lassen sich Workloads einfacher und in wenigen Minuten wiederherstellen

"NetApp Ransomware-Schutz"erleichtert das Erreichen dieser NIST-Funktionen:

- Automatische Erkennung* und Priorisierung von Daten im NetApp-Speicher * mit Fokus auf die wichtigsten anwendungsbasierten Workloads *.
- **One-Click-Schutz** für Datensicherung mit Top-Workload, unveränderliche, sichere Konfiguration, bösartige Dateiblockierung und verschiedene Sicherheitsdomänen.
- * Mit * KI-basierter Anomalieerkennung der nächsten Generation * Ransomware so schnell wie möglich genau erkennen*
- Automatisierte Reaktion und Workflows sowie Integration mit Top * SIEM und XDR Lösungen.*
- Schnelle Datenwiederherstellung mit einer vereinfachten **orchestrierten Recovery** zur Beschleunigung der Applikations-Uptime.
- Implementieren Sie Ihren Ransomware-Schutz **Strategie** und **Richtlinien** und **Ergebnisse überwachen**.

NetApp und Zero Trust

NetApp und Zero Trust

Zero Trust war bisher ein netzwerkorientierter Ansatz der Architektur von Microcore and Perimeter (MCAP) zum Schutz von Daten, Services, Applikationen oder Assets mit Kontrolloptionen, die als Segmentierungsgateway bekannt sind. NetApp ONTAP verfolgt bei der Zero-Trust-Strategie einen Daten-orientierten Ansatz, bei dem das Storage-Managementsystem zum Segmentierungs-Gateway wird, um die Daten unserer Kunden zu schützen und den Zugriff darauf zu überwachen. Insbesondere die FPolicy Zero Trust Engine und das FPolicy Partner-Ecosystem werden zum Kontrollzentrum, um normale und fehlende Datenzugriffsmuster detailliert zu verstehen und Bedrohungen von innen zu

erkennen.

> Ab Juli 2024 ist der Inhalt des technischen Berichts *TR-4829: NetApp and Zero Trust: Enabling a Data-Centric Zero Trust model*, der zuvor als PDF veröffentlicht wurde, auf docs.netapp.com verfügbar.

Daten sind das wichtigste Gut Ihres Unternehmens. Insiderbedrohungen sind laut dem Bericht von 2022 die Ursache für 18 % aller Datenschutzverletzungen "Verizon Data Breach Investigations Report". Unternehmen können ihre Wachsamkeit erhöhen, indem sie branchenführende Zero Trust-Kontrollen rund um Daten mit der NetApp ONTAP Datenmanagement-Software einsetzen.

Was Ist Zero Trust?

Das Zero-Trust-Modell wurde zuerst von John Kindervag bei Forrester Research entwickelt. Sie sieht Netzwerksicherheit von innen nach außen statt von außen vor. Der Inside-Out Zero Trust-Ansatz identifiziert einen Microcore und Perimeter (MCAP). Bei MCAP handelt es sich um eine interne Definition von Daten, Services, Applikationen und Assets, die durch umfassende Kontrollen geschützt werden. Das Konzept eines sicheren äußeren Perimeters ist veraltet. Entitäten, denen eine vertrauenswürdige und erfolgreiche Authentifizierung über den Perimeter gestattet ist, können das Unternehmen dann anfällig für Angriffe machen. Insider befinden sich per Definition bereits innerhalb des sicheren Perimeters. Mitarbeiter, Auftragnehmer und Partner sind Insider und müssen für den Betrieb mit entsprechenden Kontrollmechanismen in der Infrastruktur Ihres Unternehmens sorgen.

Zero Trust wurde im September 2019 als eine Technologie genannt, die dem DoD Versprechen gibt "GJ19-23 DoD Strategie zur digitalen Modernisierung". Zero Trust ist Eine Cybersicherheitsstrategie, die in der gesamten Architektur Sicherheit einbettet, um Datenschutzverletzungen zu stoppen. Dieses datenorientierte Sicherheitsmodell beseitigt die Idee vertrauenswürdiger oder nicht vertrauenswürdiger Netzwerke, Geräte, Personas oder Prozesse und wechselt zu auf Multi-Attribut-basierten Vertrauensstufen, die Authentifizierungs- und Autorisierungsrichtlinien unter dem Begriff „Least Privileged Access“ ermöglichen. Um Zero Trust zu implementieren, müssen wir überdenken, wie wir die vorhandene Infrastruktur nutzen, um Sicherheit einfacher und effizienter zu implementieren und gleichzeitig einen ungehinderten Betrieb zu ermöglichen.“

Im August 2020 veröffentlichte der NIST "Spezielle Pub 800-207 Zero Trust-Architektur" (ZTA). ZTA konzentriert sich auf den Schutz von Ressourcen und nicht auf Netzwerksegmente, da der Standort des Netzwerks nicht mehr als Hauptkomponente der Sicherheitslage der Ressource angesehen wird. Ressourcen sind Daten und Computing. ZTA-Strategien sind für Enterprise Network Architects. ZTA führt einige neue Terminologie aus den ursprünglichen Forrester-Konzepten ein. Sicherungsmechanismen, die als Policy Decision Point (PDP) und Policy Enforcement Point (PEP) bezeichnet werden, sind analog zu einem Forrester Segmentierungs-Gateway. ZTA stellt vier Implementierungsmodelle vor:

- Geräte-Agent- oder Gateway-basierte Bereitstellung
- Enclave-basierte Implementierung (entspricht in etwa dem Forrester MCAP)
- Portalbasierte Implementierung von Ressourcen
- Geräteanwendung Sandbox

Für die Zwecke dieser Dokumentation verwenden wir Konzepte und Terminologie von Forrester Research und nicht die NIST ZTA.

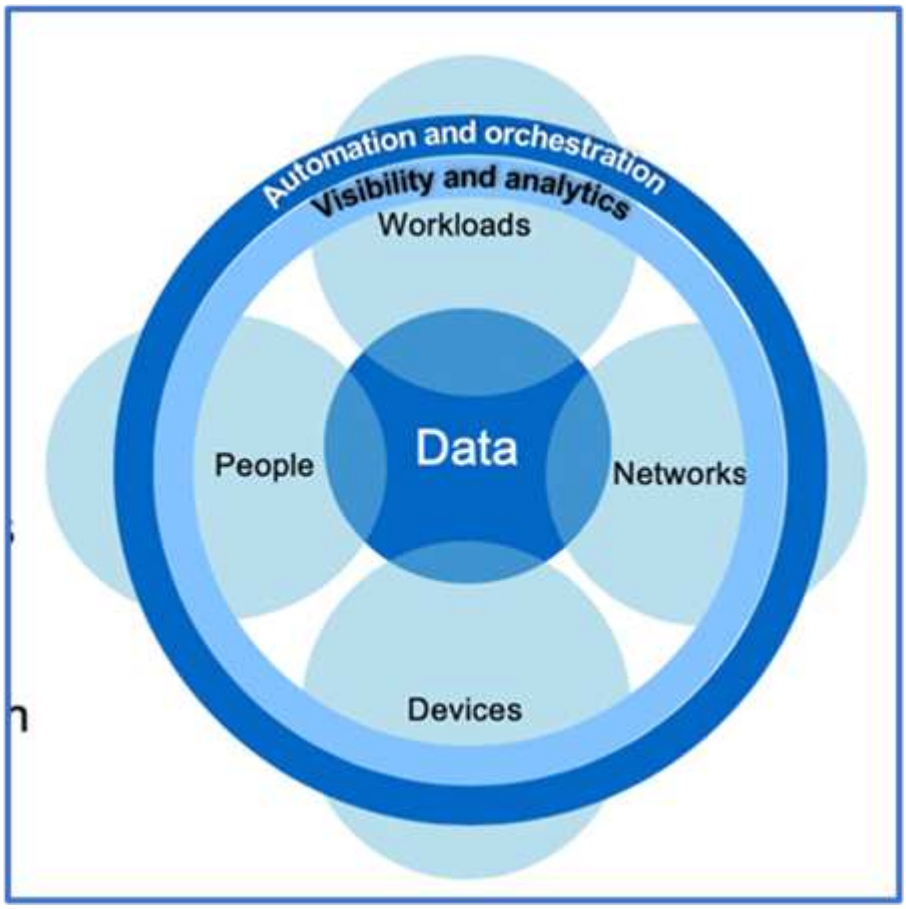
Sicherheitsressourcen

Informationen zur Meldung von Schwachstellen und Vorfällen, NetApp Sicherheitsreaktionen und Vertraulichkeit der Kundenvertraulichkeit finden Sie im "Sicherheitsportal von NetApp".

Entwerfen eines datenorientierten Ansatzes für Zero Trust mit ONTAP

Ein Zero-Trust-Netzwerk wird durch einen datenorientierten Ansatz definiert, bei dem die Sicherheitskontrollen so nah wie möglich an den Daten sein sollten. Die Funktionen von ONTAP in Kombination mit dem NetApp FPolicy Partner-Ecosystem bieten die erforderlichen Kontrollen für das datenorientierte Zero-Trust-Modell.

ONTAP ist eine sicherheitsreiche Datenmanagement-Software von NetApp und die FPolicy Zero Trust Engine ist eine branchenführende ONTAP-Funktion, die eine granulare, dateibasierte Ereignisbenachrichtigung bietet. NetApp FPolicy Partner können diese Schnittstelle nutzen, um den Datenzugriff innerhalb von ONTAP besser zu nutzen.



Entwerfen Sie eine datenorientierte MCAP mit Zero Trust

Gehen Sie wie folgt vor, um einen datenorientierten Zero Trust MCAP zu entwickeln:

1. Ermitteln Sie den Standort aller Unternehmensdaten.
2. Daten klassifizieren:
3. Entsorgen Sie Daten, die Sie nicht mehr benötigen.
4. Welche Rollen sollten auf die Datenklassifizierungen zugreifen können?
5. Wenden Sie das Prinzip „Least Privilege“ an, um Zugriffskontrollen durchzusetzen.
6. Multi-Faktor-Authentifizierung für administrativen Zugriff und Datenzugriff
7. Verschlüsselung von Daten im Ruhezustand und aktiven Daten

8. Überwachen und protokollieren Sie den gesamten Zugriff.
9. Alarmieren Sie verdächtige Zugriffe oder Verhaltensweisen.

Ermitteln Sie den Standort aller Unternehmensdaten

Mit der FPolicy Funktion von ONTAP und dem NetApp Alliance Partner Ecosystem von FPolicy Partnern können Sie herausfinden, wo sich die Daten Ihres Unternehmens befinden und wer Zugriff auf sie hat. Dies erfolgt mithilfe von Benutzerverhaltensanalysen, die feststellen, ob Datenzugriffsmuster gültig sind. Weitere Details zu User Behavioral Analytics werden unter Überwachen und Protokollieren aller Zugriffe erläutert. Wenn Sie nicht verstehen, wo sich Ihre Daten befinden und wer Zugriff darauf hat, kann die Verhaltensanalyse von Benutzern als Grundlage für die Erstellung von Klassifizierungen und Richtlinien anhand empirischer Beobachtungen dienen.

Daten klassifizieren

In der Terminologie des Zero-Trust-Modells umfasst die Klassifizierung von Daten die Identifizierung toxischer Daten. Toxische Daten sind sensible Daten, die nicht außerhalb einer Organisation offengelegt werden sollen. Die Offenlegung toxischer Daten könnte gegen regulatorische Vorgaben verstoßen und den Ruf einer Organisation schädigen. Im Hinblick auf regulatorische Vorgaben zählen zu toxischen Daten Karteninhaberdaten für die "Payment Card Industry Data Security Standard (PCI-DSS)", personenbezogene Daten für die EU "DSGVO (Datenschutz-Grundverordnung)" oder Gesundheitsdaten für die "Health Insurance Portability and Accountability Act (HIPAA)". Mit NetApp "NetApp Data Classification" (ehemals Cloud Data Sense), einem KI-gestützten Toolkit, lassen sich Ihre Daten automatisch scannen, analysieren und kategorisieren.

Entsorgen Sie Daten, die Sie nicht mehr benötigen

Nach der Klassifizierung Ihrer Unternehmensdaten stellen Sie möglicherweise fest, dass einige Ihrer Daten für die Funktion Ihres Unternehmens nicht mehr erforderlich oder relevant sind. Die Aufbewahrung unnötiger Daten ist eine Haftung, und diese Daten sollten gelöscht werden. Einen erweiterten Mechanismus zum kryptografischen Löschen von Daten finden Sie in der Beschreibung zum sicheren Löschen von Daten im Ruhezustand.

Verstehen Sie, welche Rollen auf die Datenklassifizierungen zugreifen sollten, und wenden Sie das Prinzip der geringsten Berechtigungen an, um Zugriffskontrollen durchzusetzen

Das Zuordnen von Zugriff auf sensible Daten und die Anwendung des Prinzips der geringsten Rechte bedeutet, dass Mitarbeiter in Ihrem Unternehmen nur auf die Daten zugreifen können, die für die Ausführung ihrer Aufgaben erforderlich sind. Dieser Prozess beinhaltet eine rollenbasierte Zugriffssteuerung ("RBAC", die für den Datenzugriff und administrativen Zugriff gilt.

Mit ONTAP kann eine Storage Virtual Machine (SVM) verwendet werden, um den Zugriff auf Unternehmensdaten durch Mandanten innerhalb eines ONTAP Clusters zu segmentieren. RBAC kann sowohl auf den Datenzugriff als auch auf den administrativen Zugriff auf die SVM angewendet werden. RBAC kann auch auf der Cluster-Administrationsebene angewendet werden.

Zusätzlich zu RBAC können Sie ONTAP (MAV) verwenden "Verifizierung durch mehrere Administratoren" , damit ein oder mehrere Administratoren Befehle wie oder genehmigen müssen `volume delete` `volume snapshot delete`. Wenn MAV aktiviert ist, muss MAV durch Ändern oder Deaktivieren der MAV-Administratorfreigabe genehmigt werden.

Eine andere Möglichkeit, Snapshots zu schützen, ist mit ONTAP "Snapshot wird gesperrt". Beim Snapshot-Sperren handelt es sich um eine SnapLock-Funktion, bei der Snapshots manuell oder automatisch mit einer Aufbewahrungsfrist auf der Snapshot-Richtlinie des Volumes unlöschbar gemacht werden. Snapshot-Sperrung wird auch als manipulationssichere Snapshot Sperrung bezeichnet. Mit dem Zweck der Snapshot-Sperrung

können Sie verhindern, dass abnormale oder nicht vertrauenswürdige Administratoren Snapshots auf primären und sekundären ONTAP Systemen löschen. Eine schnelle Recovery von gesperrten Snapshots auf Primärsystemen kann zur Wiederherstellung von durch Ransomware beschädigten Volumes erreicht werden.

Multi-Faktor-Authentifizierung für administrativen Zugriff und Datenzugriff

Zusätzlich zur rollenbasierten Zugriffskontrolle (RBAC) für die Clusterverwaltung kann "Multi-Faktor-Authentifizierung (MFA)" für den administrativen Webzugriff auf ONTAP und den Secure Shell (SSH) Befehlszeilenzugriff eingesetzt werden. MFA für administrativen Zugriff ist eine Anforderung für US-amerikanische Organisationen des öffentlichen Sektors oder für solche, die den PCI-DSS einhalten müssen. MFA macht es einem Angreifer unmöglich, ein Konto allein mit Benutzername und Passwort zu kompromittieren. MFA erfordert zwei oder mehr unabhängige Faktoren zur Authentifizierung. Ein Beispiel für Zwei-Faktor-Authentifizierung ist etwas, das ein Benutzer besitzt, wie ein privater Schlüssel, und etwas, das ein Benutzer weiß, wie ein Passwort. Administrativer Webzugriff auf ONTAP System Manager oder Active IQ Unified Manager wird durch Security Assertion Markup Language (SAML) 2.0 ermöglicht. SSH Befehlszeilenzugriff verwendet eine verkettete Zwei-Faktor-Authentifizierung mit einem öffentlichen Schlüssel und einem Passwort.

Mit den Identitäts- und Zugriffsverwaltungsfunktionen von ONTAP können Sie den Benutzer- und Maschinenzugriff über APIs steuern:

- Benutzer:
  - **Authentifizierung und Autorisierung.** Über NAS-Protokollfunktionen für SMB und NFS.
  - **Audit.** Syslog für Zugriff und Ereignisse Detaillierte Audit-Protokollierung des CIFS-Protokolls zum Testen von Authentifizierungs- und Autorisierungsrichtlinien Fein abgestimmte FPolicy-Prüfung von detailliertem NAS-Zugriff auf Dateiebene
- Gerät:
  - **Authentifizierung.** Zertifikatbasierte Authentifizierung für API-Zugriff.
  - **Genehmigung.** Standardmäßige oder benutzerdefinierte rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)
  - **Audit.** Syslog aller durchgeführten Aktionen.

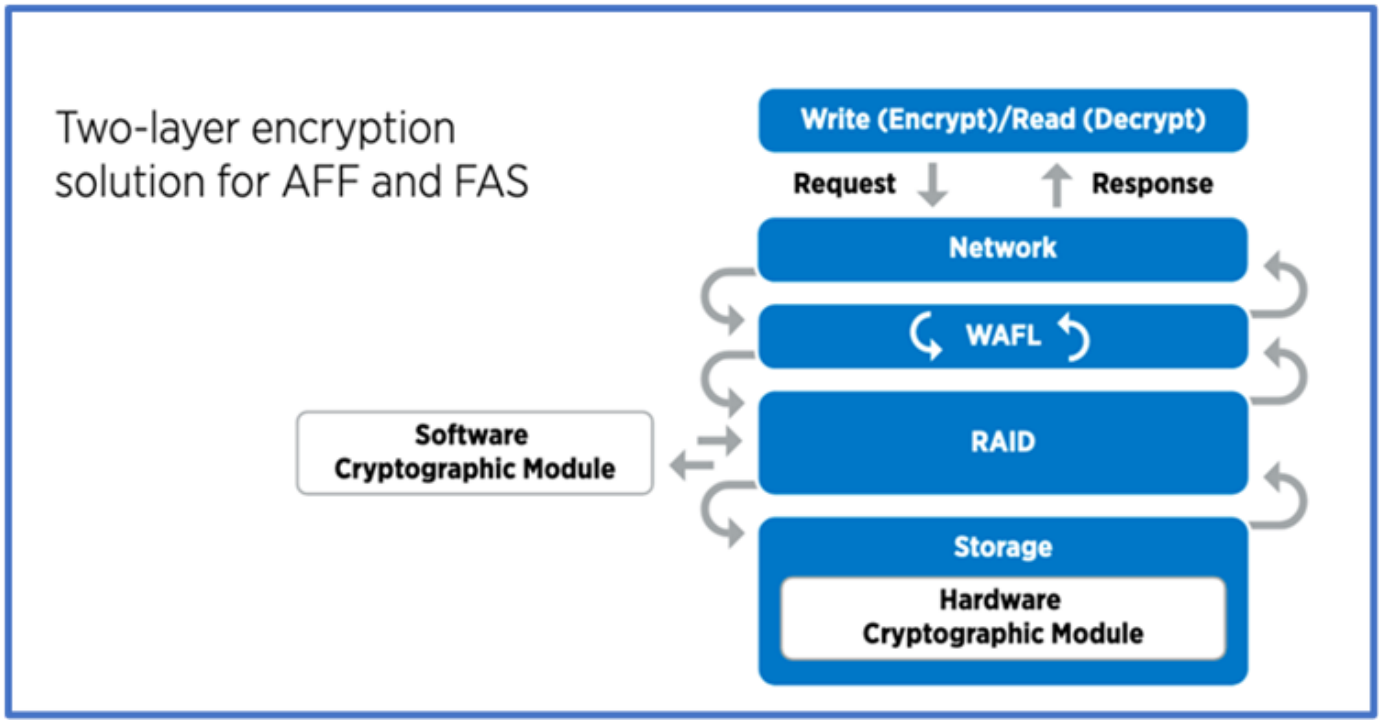
Verschlüsselung von Daten im Ruhezustand und aktiven Daten

Verschlüsselung von Daten im Ruhezustand

Täglich entstehen neue Anforderungen an die Risikominderung von Speichersystemen und die Schließung von Infrastrukturlücken, wenn ein Unternehmen Festplatten wiederverwendet, defekte Festplatten zurückgibt oder durch Verkauf oder Inzahlungnahme auf größere Festplatten umsteigt. Als Administratoren und Betreiber von Daten sind Speichertechniker verpflichtet, Daten während ihres gesamten Lebenszyklus sicher zu verwalten und zu pflegen. "NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), NetApp Aggregate Encryption" helfen dabei, alle Ihre Daten im Ruhezustand jederzeit zu verschlüsseln, unabhängig davon, ob sie toxisch sind oder nicht, und ohne den täglichen Betrieb zu beeinträchtigen. "NSE" ist eine ONTAP Hardware "Daten im Ruhezustand" Lösung, die FIPS 140-2 Level 2-validierte selbstverschlüsselnde Festplatten verwendet. "NVE und NAE" sind eine ONTAP Software "Daten im Ruhezustand" Lösung, die "Validiertes NetApp Cryptographic Module nach FIPS 140-2 Level 1" verwendet. Mit NVE und NAE können sowohl Festplatten als auch Solid-State-Laufwerke für die Verschlüsselung von Daten im Ruhezustand eingesetzt werden. Außerdem können NSE-Laufwerke eine native, mehrschichtige Verschlüsselungslösung bereitstellen, die Verschlüsselungsredundanz und zusätzliche Sicherheit bietet. Wird eine Schicht kompromittiert, schützt die zweite Schicht die Daten weiterhin. Diese Funktionen machen ONTAP bestens geeignet für "Quantum-fähige Verschlüsselung".

NVE bietet zudem eine Funktion namens „ "Sicheres Löschen" kryptografisch“ zur Beseitigung toxischer Daten bei Verschütten von Daten, wenn sensible Dateien auf ein nicht klassifiziertes Volume geschrieben werden.

Entweder der "Onboard Key Manager (OKM)"in ONTAP integrierte Schlüsselmanager oder "Genehmigt" ein Drittanbieter "Externe Schlüsselmanager" kann mit NSE und NVE zum sicheren Speichern von Schlüsseln verwendet werden.



Wie in der Abbildung oben zu sehen ist, kann die Hardware- und softwarebasierte Verschlüsselung kombiniert werden. Diese Fähigkeit führte zu der, die die "Validierung von ONTAP in die kommerziellen Lösungen der NSA für das klassifizierte Programm" Speicherung von streng geheimen Daten ermöglicht.

Verschlüsselung von aktiven Daten

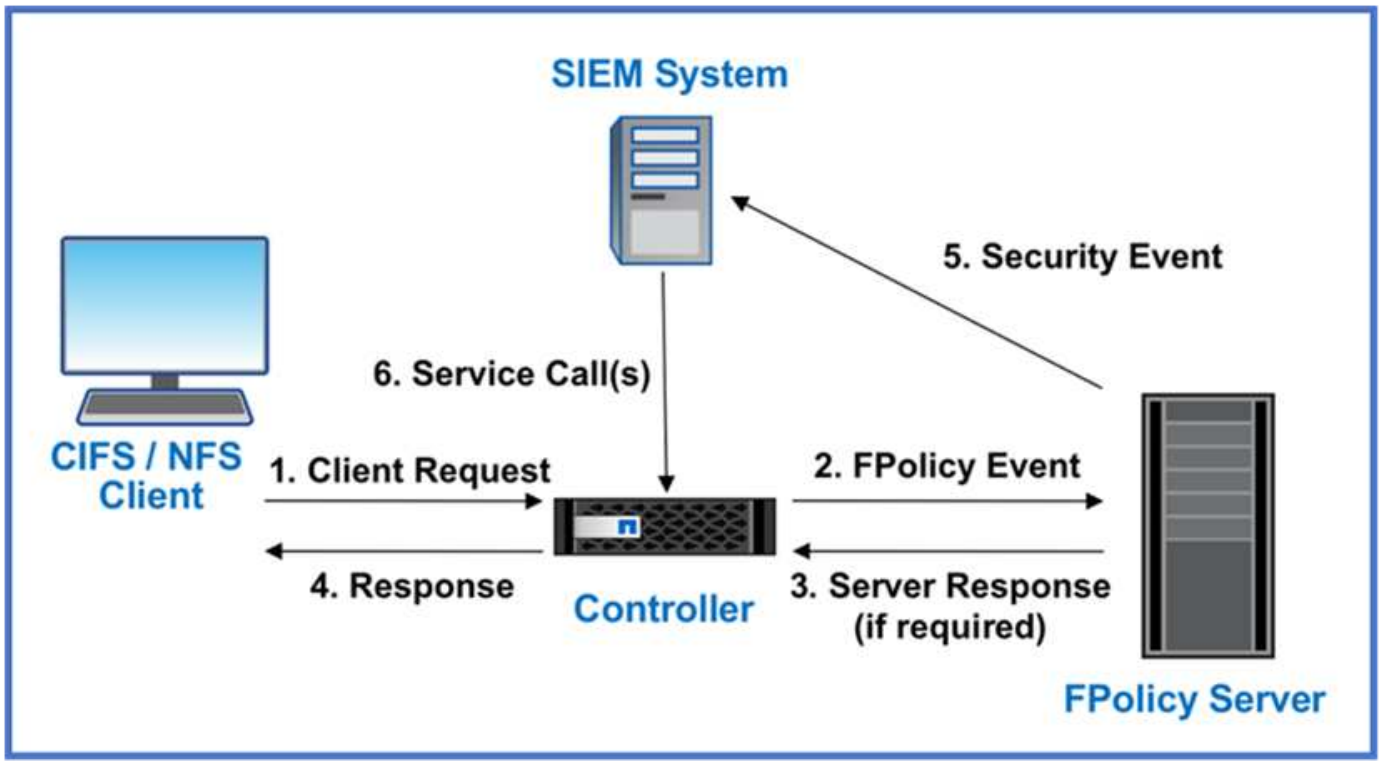
Die ONTAP Verschlüsselung von aktiven Daten sichert den Zugriff auf Benutzerdaten und Zugriff auf Kontrollebene. Der Benutzerdatenzugriff kann durch SMB 3.0-Verschlüsselung für den Zugriff auf Microsoft CIFS-Freigaben oder durch krb5P für NFS Kerberos 5 verschlüsselt werden. Der Zugriff auf Benutzerdaten kann auch mit für CIFS, NFS und iSCSI verschlüsselt werden "IPsec" . Der Zugriff auf die Kontrollebene wird mit Transport Layer Security (TLS) verschlüsselt. ONTAP bietet "FIPS" einen Compliance-Modus für den Zugriff auf die Kontrollebene, mit dem FIPS-genehmigte Algorithmen aktiviert und nicht FIPS-zertifizierte Algorithmen deaktiviert werden. Die Datenreplikation wird mit verschlüsselt "Cluster-Peer-Verschlüsselung". Dadurch wird Verschlüsselung für die ONTAP SnapVault und SnapMirror Technologien bereitgestellt.

Überwachen und protokollieren Sie den gesamten Zugriff

Nachdem die RBAC-Richtlinien festgelegt sind, müssen Sie aktive Monitoring-, Audit- und Warnfunktionen implementieren. Die FPolicy Zero-Trust-Engine von NetApp ONTAP bietet in Kombination mit dem die "Partner-Ecosystem von NetApp FPolicy"erforderlichen Kontrollen für das datenorientierte Zero-Trust-Modell. NetApp ONTAP ist eine sicherheitsrelevante Datenmanagement-Software und "FPolicy" eine branchenführende ONTAP-Funktion, die eine granulare, dateibasierte Ereignisbenachrichtigung bietet. NetApp FPolicy Partner können diese Schnittstelle nutzen, um den Datenzugriff innerhalb von ONTAP besser zu nutzen. Mit der FPolicy Funktion von ONTAP und dem NetApp Alliance Partner Ecosystem von FPolicy Partnern können Sie feststellen, wo sich die Daten Ihres Unternehmens befinden und wer Zugriff auf sie hat. Dies erfolgt mithilfe von Benutzerverhaltensanalysen, die feststellen, ob Datenzugriffsmuster gültig sind.

Mithilfe von Analysen des Benutzerverhaltens lässt sich ein Alarm bei verdächtigem oder irridenem Datenzugriff erstellen, der nicht dem normalen Muster entspricht, und gegebenenfalls Maßnahmen ergreifen, um den Zugriff zu verweigern.

FPolicy-Partner gehen über die Verhaltensanalyse von Benutzern hinaus auf maschinelles Lernen (ML) und künstliche Intelligenz (KI) um, was zu mehr Ereignistreue und weniger, wenn überhaupt, falsche Positives führt. Alle Ereignisse sollten bei einem Syslog-Server oder bei einem SIEM-System (Security Information and Event Management) protokolliert werden, das auch ML und KI einsetzen kann.



NetApps "DII-Speicher-Workload-Sicherheit" nutzt die FPolicy-Schnittstelle und die Benutzerverhaltensanalyse sowohl auf Cloud- als auch auf lokalen ONTAP Speichersystemen, um Sie in Echtzeit vor böswilligem Benutzerverhalten zu warnen. Storage Workload Security schützt Unternehmensdaten durch fortschrittliches maschinelles Lernen und Anomalieerkennung vor Missbrauch durch böswillige oder kompromittierte Benutzer. Storage Workload Security kann Ransomware-Angriffe oder andere schädliche Verhaltensweisen erkennen, Snapshots aufrufen und böswillige Benutzer unter Quarantäne stellen. Storage Workload Security verfügt außerdem über eine forensische Funktion, um Benutzer- und Entitätsaktivitäten detailliert anzuzeigen. Storage Workload Security ist Teil von NetApp Data Infrastructure Insights.

Zusätzlich zur Sicherheit von Storage-Workloads verfügt ONTAP über eine integrierte Funktion zur Erkennung von Ransomware, die als (ARP) bekannt "Autonomer Schutz Durch Ransomware" ist. ARP ermittelt mithilfe von Machine Learning, ob anormale Dateiaktivitäten auf einen Ransomware-Angriff hindeuten, und ruft einen Snapshot auf und warnt Administratoren. Storage Workload Security ist in ONTAP integrierbar, um ARP-Ereignisse zu empfangen und eine zusätzliche Analysemebene und automatische Reaktionen zu ermöglichen.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Kontrollmechanismen für die Sicherheitsautomatisierung und Orchestrierung von NetApp außerhalb von ONTAP

Durch Automatisierung können Sie Prozesse oder Verfahren mit minimaler menschlicher Unterstützung durchführen. Durch Automatisierung sind Unternehmen in der Lage, Zero-

Trust-Implementierungen weit über manuelle Verfahren hinaus zu skalieren und sich so gegen ebenfalls automatisierte Aktivitäten zu wehren, bei denen Fehlkreationen entstehen.

Ansible ist ein Open-Source-Tool für Softwarebereitstellung, Konfigurationsmanagement und Anwendungsdeployment. Es läuft auf vielen Unix-ähnlichen Systemen und kann sowohl diese als auch Microsoft Windows konfigurieren. Es enthält eine eigene deklarative Sprache zur Beschreibung der Systemkonfiguration. Ansible wurde von Michael DeHaan entwickelt und 2015 von Red Hat übernommen. Ansible arbeitet agentenlos, stellt temporär eine Remote-Verbindung über SSH oder Windows Remote Management her (was die Remote PowerShell-Ausführung ermöglicht), um Aufgaben auszuführen. NetApp hat mehr als "150 Ansible-Module für ONTAP-Software" entwickelt, was eine weitere Integration mit dem Ansible Automation Framework ermöglicht. Ansible-Module für NetApp liefern Anweisungen, wie der gewünschte Zustand definiert und an die Zielumgebung von NetApp übermittelt wird. Module unterstützen Aufgaben wie das Einrichten von Lizenzen, das Erstellen von Aggregaten und Storage Virtual Machines, das Erstellen von Volumes und das Wiederherstellen von Snapshots, um nur einige zu nennen. Eine Ansible-Rolle wurde "Veröffentlicht auf GitHub" spezifisch für den NetApp DoD Unified Capabilities (UC) Deployment Guide entwickelt.

Mit der Bibliothek verfügbarer Module können Benutzer auf einfache Weise Ansible-Playbooks entwickeln und für die eigenen Applikationen und geschäftlichen Anforderungen anpassen, um Routineaufgaben zu automatisieren. Nachdem ein Playbook verfasst ist, können Sie es ausführen, um die angegebene Aufgabe auszuführen. Dies spart Zeit und erhöht die Produktivität. NetApp hat Beispiel-Playbooks erstellt und geteilt, die direkt verwendet oder an die eigenen Anforderungen angepasst werden können.

Data Infrastructure Insights ist ein Tool zur Infrastrukturüberwachung, das Ihnen Einblick in Ihre gesamte Infrastruktur gibt. Mit Data Infrastructure Insights können Sie alle Ihre Ressourcen überwachen, Fehler beheben und optimieren, einschließlich Ihrer öffentlichen Cloud-Instanzen und Ihrer privaten Rechenzentren. Data Infrastructure Insights kann die durchschnittliche Zeit bis zur Lösung um 90 % verkürzen und verhindern, dass 80 % der Cloud-Probleme Endbenutzer betreffen. Darüber hinaus können Sie die Kosten für die Cloud-Infrastruktur um durchschnittlich 33 % senken und Ihre Anfälligkeit gegenüber Insider-Bedrohungen verringern, indem Sie Ihre Daten mit verwertbaren Informationen schützen. Die Storage Workload Security-Funktion von Data Infrastructure Insights ermöglicht die Analyse des Benutzerverhaltens mit KI und ML, um zu warnen, wenn aufgrund einer Insider-Bedrohung abweichendes Benutzerverhalten auftritt. Für ONTAP nutzt Storage Workload Security die Zero Trust FPolicy-Engine.

Zero-Trust- und Hybrid-Cloud-Implementierungen

NetApp ist die Datenautorität für die Hybrid Cloud. NetApp bietet eine Vielzahl von Optionen zur Erweiterung lokaler Datenmanagementsysteme auf die Hybrid Cloud mit Amazon Web Services (AWS), Microsoft Azure, Google Cloud und anderen führenden Cloud-Anbietern. NetApp Hybrid-Cloud-Lösungen unterstützen dieselben Zero Trust-Sicherheitskontrollen, die auch für lokale ONTAP -Systeme und softwaredefinierten ONTAP Select Speicher verfügbar sind.

Sie können die Kapazität in öffentlichen Clouds ohne die typischen CAPEX-Einschränkungen problemlos erweitern, indem Sie Cloud-native Dateidienste der Enterprise-Klasse für AWS (FSxN), Google Cloud (GCNV) und Azure NetApp Files für Microsoft Azure verwenden. Diese Cloud-Datendienste eignen sich ideal für datenintensive Workloads wie Analysen und DevOps und kombinieren elastischen On-Demand-Speicher als Service von NetApp mit ONTAP Datenmanagement in einem vollständig verwalteten Angebot.

ONTAP ermöglicht die Datenübertragung zwischen Ihren lokalen ONTAP -Systemen und der AWS-, Google Cloud- oder Azure-Speicherumgebung mit der Datenreplikationssoftware NetApp SnapMirror .

Attributbasierte Zugriffssteuerung

Attributbasierte Zugriffssteuerung mit ONTAP

Ab Version 9.12.1 können Sie ONTAP mit NFSv4.2-Sicherheitsetiketten und erweiterten Attributen (xattrs) konfigurieren, um rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) mit Attributen und attributbasierter Zugriffssteuerung (Attribute Based Access Control, ABAC) zu unterstützen.

ABAC ist eine Autorisierungsstrategie, die Berechtigungen basierend auf Benutzerattributen, Ressourcenattributen und Umgebungsbedingungen definiert. Die Integration von ONTAP mit NFS v4.2 Security Labels und xattrs entspricht den NIST Standards für ABAC Lösungen, wie in NIST Special Publication 800-162.

Sie können NFS v4.2-Sicherheitsetiketten und xattrs verwenden, um Dateien benutzerdefinierte Attribute und Labels zuzuweisen. ONTAP kann in die ABAC-orientierte Identitäts- und Zugriffsmanagement-Software integriert werden, um auf der Grundlage dieser Attribute und Labels granulare Richtlinien zur Zugriffskontrolle von Dateien und Ordnern durchzusetzen.

Verwandte Informationen

- "Ansätze für ABAC mit ONTAP"
- "NFS in NetApp ONTAP: Best Practice und Implementierungsleitfaden"

Ansätze zur attributbasierten Zugriffssteuerung (ABAC) in ONTAP

ONTAP bietet verschiedene Ansätze zur Erzielung einer attributbasierten Zugriffssteuerung (File-Level-Based Access Control, ABAC), einschließlich NFS v4.2 Security Labels und Extended Attributes (xattrs) mithilfe von NFS.

NFS v4.2-Sicherheitslabels

Ab ONTAP 9.9 wird die NFS v4.2-Funktion mit der Bezeichnung NFS unterstützt.

NFS v4.2-Sicherheitsetiketten sind eine Möglichkeit, den granularen Datei- und Ordnerzugriff mithilfe von SELinux-Labels und Mandatory Access Control (MAC) zu verwalten. Diese MAC-Labels werden mit Dateien und Ordnern gespeichert und funktionieren in Verbindung mit UNIX-Berechtigungen und NFS v4.x ACLs.

Durch die Unterstützung von NFS v4.2-Sicherheitsetiketten erkennt ONTAP jetzt die SELinux-Label-Einstellungen des NFS-Clients und versteht sie. Die Sicherheitslabels für NFS v4.2 sind in RFC-7204 abgedeckt.

Zu den Anwendungsfällen für die NFS v4.2-Sicherheitslabels gehören:

- MAC-Beschriftung von Virtual Machine (VM) Images
- Datensicherheitsklassifizierung für den öffentlichen Sektor (geheime, streng geheime und andere Klassifizierungen)
- Sicherheits-Compliance
- Diskless Linux

Aktivieren Sie die NFS v4.2-Sicherheitsetiketten

Sie können die NFS v4.2-Sicherheitsetiketten mit dem folgenden Befehl aktivieren oder deaktivieren (erweiterte Berechtigung erforderlich):

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

Erfahren Sie mehr über `vserver nfs modify` in der "ONTAP-Befehlsreferenz".

Durchsetzungsmodi für NFS v4.2-Sicherheitslabels

Ab ONTAP 9.9 unterstützt ONTAP die folgenden Erzwingungsmodi:

- **Eingeschränkter Servermodus**: ONTAP kann die Labels nicht erzwingen, sondern speichern und übertragen.

  Die Möglichkeit, MAC-Labels zu ändern, liegt bei der Durchsetzung durch den Client.

- **Gastmodus**: Wenn der Client nicht NFS-aware (v4.1 oder niedriger) ist, werden MAC-Labels nicht übertragen.

  ONTAP unterstützt derzeit nicht den Vollmodus (Speichern und Erzwingen von MAC-Etiketten).

Beispiele für Sicherheitsetiketten in NFS v4.2

Die folgende Beispielkonfiguration zeigt Konzepte mit Red hat Enterprise Linux Version 9.3 (Plough).

Der Benutzer `jrsmith`, der basierend auf den Anmeldeinformationen von John R. Smith erstellt wurde, hat das folgende Konto Privileges:

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

Es gibt zwei Rollen: Das Administratorkonto, das ein privilegierter Benutzer und ein Benutzer ist `jrsmith`, wie in der folgenden MLS-Privileges-Tabelle beschrieben:

Benutzer	Rolle	Typ	Stufen
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

In dieser Beispielumgebung hat der Benutzer `jrsmith` Zugriff auf Dateien auf den Ebenen `s0` bis `s3`. Wir können die bestehenden Sicherheitsklassifizierungen wie unten beschrieben verbessern, um sicherzustellen, dass Administratoren keinen Zugriff auf benutzerspezifische Daten haben.

- s0 = Berechtigungsverwaltung Benutzerdaten

- s0 = nicht klassifizierte Daten
- s1 = vertraulich
- s2 = geheime Daten
- s3 = Top-Geheimdaten

Beispiel für NFS v4.2-Sicherheitsetiketten mit MCS

Zusätzlich zu Multi-Level Security (MLS) können Sie mit einer weiteren Funktion namens Multi-Category Security (MCS) Kategorien wie Projekte definieren.

NFS-Sicherheitsetikett	Wert
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Erweiterte Attribute (xattrs)

Ab ONTAP 9.12.1 unterstützt ONTAP xattrs. Xattrs ermöglicht die Zuordnung von Metadaten zu Dateien und Verzeichnissen über das hinaus, was vom System bereitgestellt wird, wie z. B. Zugriffskontrolllisten (ACLs) oder benutzerdefinierte Attribute.

Um xattrs zu implementieren, können Sie und `getfattr` Kommandozeilen-Dienstprogramme in Linux verwenden `setfattr`. Diese Tools bieten eine leistungsstarke Möglichkeit, zusätzliche Metadaten für Dateien und Verzeichnisse zu managen. Sie sollten mit Vorsicht eingesetzt werden, da eine unsachgemäße Verwendung zu unerwartetem Verhalten oder Sicherheitsproblemen führen kann. Detaillierte Anweisungen zur Verwendung finden Sie stets auf den `setfattr` Manpages und `getfattr` in anderen zuverlässigen Dokumentationen.

Wenn xattrs auf einem ONTAP-Dateisystem aktiviert ist, können Benutzer beliebige Attribute auf Dateien festlegen, ändern und abrufen. Diese Attribute können verwendet werden, um zusätzliche Informationen über die Datei zu speichern, die nicht von den standardmäßigen Dateiattributen erfasst werden, z. B. Informationen zur Zugriffssteuerung.

Für die Verwendung von xattrs in ONTAP gibt es mehrere Anforderungen und Grenzen:

- Red hat Enterprise Linux 8.4 oder höher
- Ubuntu 22.04 oder höher
- Jede Datei kann bis zu 128 xattrs haben
- Xattr-Schlüssel sind auf 255 Byte begrenzt
- Die kombinierte Schlüssel- oder Wertgröße beträgt 1,729 Byte pro xattr
- Verzeichnisse und Dateien können xattrs haben
- Zum Festlegen und Abrufen von xattrs `w` oder Schreibmodus müssen Bits für den Benutzer und die Gruppe aktiviert sein

Xattrs werden innerhalb des Benutzer-Namespace verwendet und haben keine intrinsische Bedeutung für ONTAP selbst. Stattdessen werden ihre praktischen Anwendungen ausschließlich von der Client-seitigen Anwendung bestimmt und verwaltet, die mit dem Dateisystem interagiert.

Anwendungsbeispiele für xattr:

- Aufzeichnen des Namens der Anwendung, die für die Erstellung einer Datei verantwortlich ist
- Beibehalten eines Verweises auf die E-Mail-Nachricht, aus der eine Datei abgerufen wurde
- Einrichten eines Kategorisierungsrahmens für die Organisation von Dateiobjekten
- Beschriften von Dateien mit der URL ihrer ursprünglichen Download-Quelle

Befehle zum Verwalten von xattrs

- `setfattr` Legt ein erweitertes Attribut einer Datei oder eines Verzeichnisses fest:

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

  Beispielbefehl:

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

- `getfattr` Ruft den Wert eines bestimmten erweiterten Attributs ab oder listet alle erweiterten Attribute einer Datei oder eines Verzeichnisses auf:

  Spezifisches Attribut:
  `getfattr -n <attribute_name> <file or directory name>`

  Alle Attribute:
  `getfattr <file or directory name>`

  Beispielbefehl:

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

Beispiele für das Schlüsselwertpaar xattr

In der folgenden Tabelle sind zwei Beispiele für das Schlüsselwertpaar xattr aufgeführt:

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

Benutzerberechtigungen mit ACE für xattrs

Ein Access Control Entry (ACE) ist eine Komponente innerhalb einer ACL, die die Zugriffsrechte oder Berechtigungen definiert, die einem einzelnen Benutzer oder einer Benutzergruppe für eine bestimmte Ressource, z. B. eine Datei oder ein Verzeichnis, gewährt werden. Jeder ACE gibt die Art des erlaubten oder abgelehnten Zugriffs an und ist mit einem bestimmten Sicherheitsprinzipal (Benutzer- oder Gruppenidentität) verknüpft.

Access Control Entry (ACE) für xattrs erforderlich

- Abrufen von xattr: Die Berechtigungen, die ein Benutzer benötigt, um die erweiterten Attribute einer Datei oder eines Verzeichnisses zu lesen. Das „R“ bedeutet, dass Leseberechtigung erforderlich ist.
- Xattrs festlegen: Die Berechtigungen, die zum Ändern oder Festlegen der erweiterten Attribute benötigt werden. „A“, „w“ und „T“ stellen verschiedene Beispiele für Berechtigungen wie Append, Write und eine bestimmte Berechtigung in Bezug auf xattrs dar.
- Dateien: Benutzer benötigen Append, Write und möglicherweise eine spezielle Berechtigung im Zusammenhang mit xattrs, um erweiterte Attribute zu setzen.
- Verzeichnisse: Eine bestimmte Berechtigung "T" ist erforderlich, um erweiterte Attribute zu setzen.

Dateityp	Xattr. Abrufen	Xattrs einstellen
Datei	R	A,w,T
Verzeichnis	R	T

Integration mit ABAC Identitäts- und Zugriffskontrollsoftware

Um die Funktionen von ABAC voll auszuschöpfen, kann ONTAP in eine ABAC-orientierte Identitäts- und Zugriffsverwaltungssoftware integriert werden.

In einem ABAC-System spielen der Policy Enforcement Point (PEP) und der Policy Decision Point (PDP) eine entscheidende Rolle. Der PEP ist für die Durchsetzung von Zugriffssteuerungsrichtlinien verantwortlich, während der PDP die Entscheidung darüber trifft, ob der Zugriff auf der Grundlage der Richtlinien gewährt oder verweigert werden soll.

In einer praktischen Umgebung würde ein Unternehmen eine Mischung aus NFS-Sicherheitsetiketten und xattrs einsetzen. Diese werden verwendet, um eine Vielzahl von Metadaten darzustellen, einschließlich Klassifizierung, Sicherheit, Anwendung und Inhalt, die alle entscheidend für ABAC Entscheidungen sind. Xattrs, zum Beispiel, kann verwendet werden, um die Ressourcenattribute zu speichern, die die PDP für seinen Entscheidungsprozess verwendet. Ein Attribut kann definiert werden, um die Klassifizierungsstufe einer Datei darzustellen (z. B. „nicht klassifiziert“, „vertraulich“, „geheim“ oder „streng geheim“). Die PDP könnte dann dieses Attribut nutzen, um eine Richtlinie durchzusetzen, die Benutzern den Zugriff auf Dateien einschränkt, die eine Klassifizierungsstufe haben, die ihrem Sicherheitsniveau entspricht oder kleiner ist.

Dieser Inhalt setzt voraus, dass die Identitäts-, Authentifizierungs- und Zugriffsdienste des Kunden mindestens einen PEP und ein PDP umfassen, die als Vermittler für den Zugriff auf das Dateisystem fungieren.

Beispiel für einen Prozessablauf für ABAC

1. Benutzer stellt Anmeldeinformationen (z. B. PKI, OAuth, SAML) für den Systemzugriff auf PEP bereit und ruft Ergebnisse von PDP ab.

   Die Rolle des PEP besteht darin, die Zugriffsanforderung des Benutzers abzufangen und an das PDP weiterzuleiten.

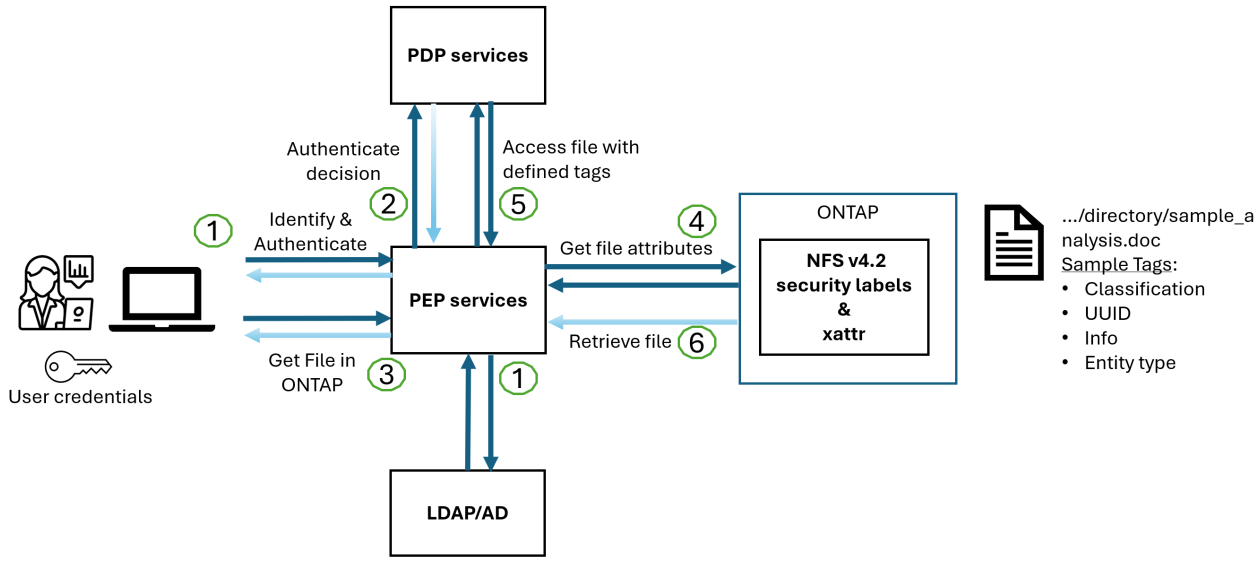
2. Die PDP wertet diese Anforderung dann anhand der festgelegten ABAC-Richtlinien aus.

   In diesen Richtlinien werden verschiedene Attribute berücksichtigt, die sich auf den Benutzer, die betreffende Ressource und die Umgebung beziehen. Auf der Grundlage dieser Richtlinien trifft die PDP eine Zugriffsentscheidung, entweder zuzulassen oder abzulehnen, und teilt diese Entscheidung dann dem PEP zurück.

PDP stellt PEP Richtlinien zur Durchsetzung bereit. Der PEP erzwingt dann diese Entscheidung, indem er die Zugriffsanfrage des Benutzers gemäß der Entscheidung des PDP entweder gewährt oder ablehnt.

3. Nach einer erfolgreichen Anfrage fordert der Benutzer eine in ONTAP gespeicherte Datei an (z. B. AFF, AFF-C).
4. Wenn die Anforderung erfolgreich war, erhält PEP fein abgestufte Zugangskontroll-Tags aus dem Dokument.
5. PEP fordert die Richtlinie für den Benutzer auf Grundlage der Zertifikate dieses Benutzers an.
6. PEP trifft eine Entscheidung auf der Grundlage von Richtlinien und Tags, wenn der Benutzer Zugriff auf die Datei hat, und lässt den Benutzer die Datei abrufen.

Der eigentliche Zugriff kann mit Token erfolgen.



ONTAP Cloning und SnapMirror

Die Klon- und SnapMirror-Technologien von ONTAP bieten effiziente und zuverlässige Datenreplizierungs- und Klonfunktionen und stellen sicher, dass alle Aspekte von Dateidaten, einschließlich xattrs, zusammen mit der Datei erhalten und übertragen werden. Xattrs sind wichtig, da sie zusätzliche Metadaten, die einer Datei zugeordnet sind, wie z. B. Sicherheitslabels, Zugriffskontrollinformationen und benutzerdefinierte Daten, speichern. Diese sind für die Aufrechterhaltung des Kontexts und der Integrität dieser Datei von wesentlicher Bedeutung.

Wenn ein Volume mit der FlexClone-Technologie von ONTAP geklont wird, wird ein exaktes, beschreibbares Replikat des Volumes erstellt. Dieser Klonprozess ist sofort und platzsparend und umfasst alle Dateidaten und Metadaten, um sicherzustellen, dass xattrs vollständig repliziert werden. SnapMirror sorgt auf ähnliche Weise dafür, dass Daten originalgetreu auf ein sekundäres System gespiegelt werden. Dazu gehört xattrs, die entscheidend sind für Anwendungen, die auf diese Metadaten angewiesen sind, um korrekt zu funktionieren.

Durch die Einbeziehung von xattrs sowohl beim Klonen als auch bei der Replizierung stellt NetApp ONTAP sicher, dass der vollständige Datensatz mit allen seinen Merkmalen verfügbar und konsistent über primäre und sekundäre Storage-Systeme hinweg ist. Dieser umfassende Datenmanagementansatz ist für Unternehmen unerlässlich, die eine konsistente Datensicherung, schnelle Wiederherstellung und die Einhaltung von Compliance- und gesetzlichen Standards benötigen. Zudem vereinfacht sie das Management von Daten in verschiedenen Umgebungen, sowohl vor Ort als auch in der Cloud. Benutzer können sich darauf verlassen,

dass ihre Daten während dieser Prozesse vollständig und unverändert sind.

> Für NFS v4.2-Sicherheits-Labels sind die Einschränkungen definiert inNFS v4.2-Sicherheitslabels.

Prüfen von Änderungen an Beschriftungen

Das Auditing von Änderungen an xattrs oder NFS-Sicherheitsetiketten ist ein wichtiger Aspekt der Verwaltung und Sicherheit von Dateisystemen. Standard-Dateisystemauditing-Tools ermöglichen die Überwachung und Protokollierung aller Änderungen an einem Dateisystem, einschließlich Änderungen an xattrs und Sicherheitsetiketten.

In Linux-Umgebungen wird der `auditd` Daemon häufig verwendet, um Auditing für Dateisystemereignisse einzurichten. Es ermöglicht Administratoren, Regeln zu konfigurieren, um auf bestimmte Systemaufrufe im Zusammenhang mit xattr-Änderungen zu achten, wie `setxattr`,, `lsetxattr` und `fsetxattr` um Attribute und, `lremovexattr` zu setzen `removexattr` und `fremovexattr` Attribute zu entfernen.

ONTAP FPolicy erweitert diese Funktionen durch ein robustes Framework für das Monitoring und die Kontrolle von Dateivorgängen in Echtzeit. FPolicy kann zur Unterstützung verschiedener xattr-Ereignisse konfiguriert werden. Dies ermöglicht eine granulare Kontrolle über Dateivorgänge und die Durchsetzung umfassender Datenmanagement-Richtlinien.

Für Benutzer, die xattrs verwenden, insbesondere in NFS v3- und NFS v4-Umgebungen, werden nur bestimmte Kombinationen von Dateioperationen und -Filtern für die Überwachung unterstützt. Die Liste der unterstützten Dateioperationen und Filterkombinationen für das FPolicy Monitoring von NFS v3- und NFS v4-Dateizugriffsereignissen ist unten detailliert:

Unterstützte Dateivorgänge	Unterstützte Filter
`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`

Beispiel eines auditd-Protokollausschlags für eine setattr-Operation:

```
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"
```

Die Aktivierung "ONTAP FPolicy" für Benutzer, die mit xattrs arbeiten, bietet eine Ebene der Sichtbarkeit und Kontrolle, die für die Aufrechterhaltung der Integrität und Sicherheit des Dateisystems unerlässlich ist. Mithilfe

der erweiterten Monitoring-Funktionen von FPolicy können Unternehmen sicherstellen, dass alle Änderungen an xattrs nachverfolgt, geprüft und an ihren Sicherheits- und Compliance-Standards ausgerichtet werden. Dieser proaktive Ansatz beim Filesystem-Management ist daher die Aktivierung von ONTAP FPolicy nur für Unternehmen empfehlenswert, die ihre Daten-Governance- und Sicherungsstrategien verbessern möchten.

Beispiele für die Kontrolle des Zugriffs auf Daten

Der folgende Beispieleintrag für Daten, die in John R. Smiths PKI-Zertifikat gespeichert sind, zeigt, wie der Ansatz von NetApp auf eine Datei angewendet werden kann und eine feingranulare Zugriffskontrolle bietet.

> Diese Beispiele dienen zur Veranschaulichung, und es liegt in der Verantwortung des Kunden, die mit den NFS v4.2-Sicherheitslabels und xattrs verbundenen Metadaten zu ermitteln. Details zur Aktualisierung und Aufbewahrung von Etiketten werden aus einfachen Grund weggelassen.

Beispiel PKI-Zertifikatwerte

Taste	Wert
EntitySecurityMark	t:s01 = NICHT KLASSIFIZIERT

Info	{
	"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"
	}
	}

Taste	Wert
Spezifikation	„DoD“
uuid	B4111349-7875-4115-ad30-0928565f2e15

AdminOrganisation	{
	"value": "DoD"
	}

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

Bürgerstatus	{
	"value": "US"
	}

Taste	Wert
Abstände	`[ { "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" } ]`
LänderOfMitgliedschaften	`[ { "value": "USA" } ]`
DigitalIdentifier	`{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }`
DissTos	`{ "value": "DoD" }`
DytOrganisation	`{ "value": "DoD" }`

Taste	Wert

EntityType	<pre>{
	"value": "GOV"
	}</pre>

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

Diese PKI-Berechtigungen zeigen die Zugangsdaten von John R. Smith, einschließlich des Zugriffs nach Datentyp und Zuordnung.

In Szenarien, in denen IC-TDF-Metadaten getrennt von der Datei gespeichert werden, empfiehlt NetApp eine zusätzliche Ebene feingranularer Zugriffskontrolle. Dabei werden Informationen zur Zugriffssteuerung sowohl auf Verzeichnisebene als auch in Verbindung mit jeder Datei gespeichert. Betrachten Sie als Beispiel die folgenden Tags, die mit einer Datei verknüpft sind:

- Sicherheitslabels für NFS v4.2: Werden für Sicherheitsentscheidungen verwendet
- Xattrs: Geben Sie ergänzende Informationen, die für die Datei und die Anforderungen an das organisatorische Programm relevant sind

Die folgenden Schlüssel-Wert-Paare sind Beispiele für Metadaten, die als xattrs gespeichert werden können und detaillierte Informationen über den Ersteller der Datei und die zugehörigen Sicherheitsklassifizierungen bieten. Diese Metadaten können von den Client-Applikationen genutzt werden, um fundierte Zugriffsentscheidungen zu treffen und Dateien gemäß den Standards und Anforderungen des Unternehmens zu organisieren.

Beispiel für xattr Schlüssel-Wert-Paare

Taste	Wert
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`

Taste	Wert
`user.specification`	`"INFO"`

Taste	Wert

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"
	},

Taste	Wert
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Verwandte Informationen

- "NFS in NetApp ONTAP: Best Practice und Implementierungsleitfaden"
- "ONTAP-Befehlsreferenz"
- Anforderung von Kommentaren (RFC)
  - "RFC 7204: Anforderungen für gekennzeichnetes NFS"
  - "RFC 2203: RPCSEC_GSS-Protokollspezifikation"
  - "RFC 3530: Network File System (NFS) Version 4 Protocol"

Verstärkte Sicherheit

Leitfäden zur ONTAP-Erhöhung der Sicherheit

Diese technischen Berichte enthalten Anleitungen zum Härten von NetApp ONTAP sowie anderen NetApp Produkten.

Diese technischen Berichte erweitern die "ONTAP Sicherheit und Datenverschlüsselung"Produktdokumentation.

Härteführungen

"TR-4569: Handbuch zur Erhöhung der Sicherheit für NetApp ONTAP" Erfahren Sie, wie Sie NetApp ONTAP so konfigurieren, dass Unternehmen vorgeschriebene Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen.

"Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere" Erfahren Sie, wie Sie ONTAP Tools für VMware vSphere konfigurieren, um Unternehmen dabei zu unterstützen, die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu erfüllen.

"TR-4957: Handbuch zur Erhöhung der Sicherheit für NetApp SnapCenter"
Erfahren Sie, wie Sie die NetApp SnapCenter Software so konfigurieren, dass Unternehmen die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen können.

"TR-4963: Leitfaden zur Sicherheitshärtung: NetApp Backup and Recovery für Anwendungen"Erfahren Sie, wie Sie NetApp Cloud Backup for Applications konfigurieren, um Unternehmen dabei zu helfen, vorgeschriebene Sicherheitsziele hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu erreichen.

"TR-4943: Handbuch zur Erhöhung der Sicherheit für NetApp Active IQ Unified Manager"
Erfahren Sie, wie Sie NetApp Active IQ Unified Manager so konfigurieren, dass Unternehmen vorgeschriebene Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen.

"TR-4945: Leitfaden zur Erhöhung der Sicherheit für NetApp Manageability SDK"
Erfahren Sie, wie Sie das NetApp Manageability SDK (NMSDK) konfigurieren, damit Unternehmen die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen können.

"Leitfaden zur Erhöhung der Sicherheit für MetroCluster Tiebreaker Host und Datenbank" Erfahren Sie, wie Sie den NetApp MetroCluster Tiebreaker Host und die Datenbank konfigurieren, um Unternehmen dabei zu unterstützen, die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit des Informationssystems zu erfüllen.

Richtlinien zur Erhöhung der Sicherheit durch ONTAP

Übersicht über die Erhöhung der Sicherheit durch ONTAP

ONTAP bietet eine Reihe von Kontrollmechanismen, mit denen Sie das Storage-Betriebssystem ONTAP, die branchenführende Datenmanagement-Software, absichern können. Mithilfe der Richtlinien- und Konfigurationseinstellungen für ONTAP kann Ihr

Unternehmen die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen.

Die Entwicklung der aktuellen Bedrohungslandschaft stellt Unternehmen vor besondere Herausforderungen beim Schutz ihrer wertvollsten Ressourcen: Daten und Informationen. Die fortschrittlichen und dynamischen Bedrohungen und Schwachstellen, mit denen wir konfrontiert sind, werden immer raffinierter. Zusammen mit einer Steigerung der Effektivität von Verschleiss- und Aufklärungstechniken durch potenzielle Eindringlinge müssen sich die Systemmanager proaktiv mit der Sicherheit von Daten und Informationen befassen.

Ab Juli 2024 ist der Inhalt des technischen Berichts *TR-4569: Security Hardening Guide for ONTAP*, der zuvor als PDF veröffentlicht wurde, auf docs.netapp.com verfügbar.

Validierung von ONTAP-Images

ONTAP stellt Mechanismen bereit, die sicherstellen, dass das ONTAP-Image beim Upgrade und beim Booten gültig ist.

Validierung von Upgrade Images

Mithilfe von Code-Signing kann sichergestellt werden, dass ONTAP Images über unterbrechungsfreie Image-Updates oder automatisierte unterbrechungsfreie Image-Updates, CLIs oder ONTAP APIs authentisch von NetApp erstellt und nicht manipuliert wurden. Die Validierung des Upgrade-Images wurde in ONTAP 9.3 eingeführt.

Diese Funktion ist eine automatische Sicherheitserweiterung für ONTAP-Upgrades oder -Reverversionen. Es wird nicht erwartet, dass der Benutzer etwas anderes tut, außer dass er optional die Signatur der obersten Ebene überprüft `image.tgz` .

Image-Validierung beim Booten

Ab ONTAP 9.4 ist sicheres Boot mit Unified Extensible Firmware Interface (UEFI) für NetApp AFF A800, AFF A220, FAS2750 und FAS2720 Systeme und nachfolgende Systeme der nächsten Generation mit UEFI BIOS aktiviert.

Während des Einschaltvorgangs validiert der Bootloader die Whitelist-Datenbank der sicheren Startschlüssel mit der Signatur, die jedem geladenen Modul zugeordnet ist. Nachdem jedes Modul validiert und geladen wurde, wird der Startvorgang mit der ONTAP-Initialisierung fortgesetzt. Wenn die Signaturüberprüfung für ein Modul fehlschlägt, wird das System neu gestartet.

Diese Optionen gelten für ONTAP-Images und das Plattform-BIOS.

Lokale Storage-Administratorkonten

ONTAP-Rollen, -Applikationen und -Authentifizierung

ONTAP bietet sicherheitsbewussten Unternehmen die Möglichkeit, verschiedenen Administratoren anhand verschiedener Anmeldeanwendungen und -Methoden granularen Zugriff zu gewähren. So können Kunden ein datenorientiertes Zero-Trust-Modell aufbauen.

Dies sind die Rollen, die Administratoren von Administratoren und Storage Virtual Machines zur Verfügung

stehen. Die Methoden der Anmeldeanwendung und die Methoden der Anmeldeauthentifizierung werden angegeben.

Rollen

Dank rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) haben Benutzer nur Zugriff auf die Systeme und Optionen, die für ihre Rollen und Funktionen erforderlich sind. Die RBAC-Lösung in ONTAP beschränkt den administrativen Zugriff der Benutzer auf das Niveau, das für ihre Rolle festgelegt wurde. Administratoren können so Benutzer anhand der zugewiesenen Rolle managen. ONTAP bietet mehrere vordefinierte Rollen. Operatoren und Administratoren können benutzerdefinierte Zugriffskontrollrollen erstellen, ändern oder löschen und Kontobeschränkungen für bestimmte Rollen festlegen.

Vordefinierte Rollen für Cluster-Administratoren

Diese Rolle…	Verfügt über diese Zugriffsebene…	Zu den folgenden Befehlen oder Befehlsverzeichnissen
`admin`	Alle	Alle Befehlsverzeichnisse (`DEFAULT`)
`admin-no-fsa` (Verfügbar ab ONTAP 9.12.1)	Lese-/Schreibzugriff	• Alle Befehlsverzeichnisse (`DEFAULT`) • `security login rest-role` • `security login role`

Schreibgeschützt	• `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`	Keine
`volume file show-disk-usage`	`autosupport`	Alle
• `set` • `system node autosupport`	Keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
`backup`	Alle	`vserver services ndmp`
Schreibgeschützt	`volume`	Keine
Alle anderen Befehlsverzeichnisse (`DEFAULT`)	`readonly`	Alle

• `security login password` Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • `set`	Keine	`security`
Schreibgeschützt	Alle anderen Befehlsverzeichnisse (`DEFAULT`)	`none`

Die `autosupport` Rolle wird dem vordefinierten `autosupport` Konto zugewiesen, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert `autosupport`, dass Sie das Konto ändern oder löschen. ONTAP hindert Sie auch daran, die `autosupport` Rolle anderen Benutzerkonten zuzuweisen.

Vordefinierte Rollen für SVM-Administratoren (Storage Virtual Machine

Rollenname	Sorgen
`vsadmin`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen • Managen von Kontingenten, qtrees, Snapshots und Dateien • LUNs managen • Führen Sie SnapLock-Vorgänge aus, mit Ausnahme von privilegiertem Löschen • Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Services konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen • Monitoring des Systemzustands der SVM

`vsadmin-volume`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen • Managen von Kontingenten, qtrees, Snapshots und Dateien • LUNs managen • Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Services konfigurieren: DNS, LDAP und NIS • Überwachung der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
`vsadmin-protocol`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Services konfigurieren: DNS, LDAP und NIS • LUNs managen • Überwachung der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
`vsadmin-backup`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Management von NDMP-Vorgängen • Lese-/Schreibzugriff auf ein wiederhergestelltes Volume erstellen • Management von SnapMirror Beziehungen und Snapshots • Anzeigen von Volumes und Netzwerkinformationen

`vsadmin-snaplock`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen • Managen von Kontingenten, qtrees, Snapshots und Dateien • Führen Sie SnapLock-Vorgänge durch, einschließlich privilegiertem Löschen • Protokolle konfigurieren: NFS und SMB • Services konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen
`vsadmin-readonly`	• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen • Monitoring des Systemzustands der SVM • Überwachung der Netzwerkschnittstelle • Zeigen Sie Volumes und LUNs an • Services und Protokolle anzeigen

Anwendungsmethoden

Die Anwendungsmethode gibt den Zugriffstyp der Anmeldemethode an. Mögliche Werte sind `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, und `telnet`.

Durch Festlegen dieses Parameters wird `service-processor` dem Benutzer Zugriff auf den Service-Prozessor gewährt. Wenn dieser Parameter auf festgelegt `service-processor`ist, muss der `-authentication-method` Parameter auf festgelegt werden `password` , da der Service Processor nur die Authentifizierung unterstützt `password` . SVM-Benutzerkonten können nicht auf den Service-Prozessor zugreifen. Daher können Operatoren und Administratoren den Parameter nicht verwenden `-vserver` , wenn dieser Parameter auf eingestellt ist `service-processor`.

Um den Zugriff auf das weiter einzuschränken `service-processor` , verwenden Sie den Befehl `system service-processor ssh add-allowed-addresses`. Mit dem Befehl `system service-processor api-service` können die Konfigurationen und Zertifikate aktualisiert werden.

Aus Sicherheitsgründen sind Telnet und Remote Shell (RSH) standardmäßig deaktiviert, da NetApp Secure Shell (SSH) für sicheren Remote-Zugriff empfiehlt. Wenn Telnet oder RSH erforderlich ist oder nur einmalig benötigt wird, müssen diese aktiviert sein.

Mit dem `security protocol modify` Befehl wird die vorhandene Cluster-weite Konfiguration von RSH und Telnet geändert. Aktivieren Sie RSH und Telnet im Cluster, indem Sie das Feld aktiviert auf einstellen `true`.

Authentifizierungsmethoden

Der Parameter für die Authentifizierungsmethode gibt die Authentifizierungsmethode an, die für Anmeldungen verwendet wird.

Authentifizierungsmethode	Beschreibung
`cert`	SSL-Zertifikatauthentifizierung
`community`	SNMP-Community-Zeichenfolgen
`domain`	Active Directory-Authentifizierung
`nsswitch`	LDAP- oder NIS-Authentifizierung
`password`	Passwort
`publickey`	Authentifizierung über öffentlichen Schlüssel
`usm`	SNMP-Benutzersicherheitsmodell

Die Verwendung von NIS wird aufgrund von Schwachstellen bei der Protokollsicherheit nicht empfohlen.

Ab ONTAP 9.3 steht für lokale SSH-Konten verkettete zwei-Faktor-Authentifizierung mit und als die beiden Authentifizierungsmethoden zur Verfügung `admin` `publickey` `password` . Zusätzlich zum Feld im Befehl wurde ein neues Feld mit dem `-authentication-method` `security login` Namen `-second -authentication-method` hinzugefügt. Entweder `publickey` oder `password` kann als oder als angegeben werden `-authentication-method` `-second-authentication-method`. Während der SSH-Authentifizierung erfolgt die Reihenfolge jedoch immer `publickey` mit teilweiser Authentifizierung, gefolgt von der Passwortaufforderung zur vollständigen Authentifizierung.

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

Ab ONTAP 9.4 `nsswitch` kann als zweite Authentifizierungsmethode mit verwendet werden `publickey`.

Ab ONTAP 9.12.1 kann FIDO2 auch für die SSH-Authentifizierung über ein YubiKey oder andere mit FIDO2 kompatible Geräte genutzt werden.

Ab ONTAP 9.13.1:

- `domain` Konten können als zweite Authentifizierungsmethode mit verwendet werden `publickey`.
- Time-Based One-time password (`totp`) ist ein temporärer Passcode, der von einem Algorithmus generiert wird, der die aktuelle Tageszeit als einen seiner Authentifizierungsfaktoren für die zweite Authentifizierungsmethode verwendet.
- Public Key Revocation wird mit SSH publickeys sowie Zertifikaten unterstützt, die während SSH auf Ablauf/Widerruf überprüft werden.

Weitere Informationen zur Multifaktor-Authentifizierung (MFA) für ONTAP System Manager, Active IQ Unified Manager und SSH sind unter "TR-4647: Multifaktor-Authentifizierung in ONTAP 9" zu finden.

Standard-Administratorkonten

Das Administratorkonto sollte eingeschränkt sein, da die Rolle des Administrators Zugriff über alle Anwendungen erhält. Das Diagnose-Konto gewährt Zugriff auf die System-Shell und sollte nur für den technischen Support reserviert werden, um Fehlerbehebungsaufgaben durchzuführen.

Es gibt zwei standardmäßige Administratorkonten: `admin` Und `diag`.

Verwaiste Konten sind ein wichtiger Sicherheitsvektor und führen oft zu Schwachstellen, einschließlich der Eskalation von Berechtigungen. Dabei handelt es sich um unnötige und nicht genutzte Konten, die im Benutzerkonto-Repository verbleiben. Dabei handelt es sich in erster Linie um Standardkonten, die nie verwendet wurden oder für die Passwörter nie aktualisiert oder geändert wurden. Um dieses Problem zu beheben, unterstützt ONTAP das Entfernen und Umbenennen von Konten.

Sie können integrierte Konten nicht entfernen oder umbenennen. Wenn ein Administrator das Konto entfernt, wird das integrierte Konto beim Neustart wiederhergestellt. **NetApp empfiehlt**, nicht benötigte integrierte Konten mit dem Befehl `lock` zu sperren.

Obwohl verwaiste Konten ein erhebliches Sicherheitsrisiko darstellen, **NetApp empfiehlt dringend**, die Auswirkungen des Entfernens von Konten aus dem lokalen Kontenspeicher zu testen.

Lokale Konten auflisten

Führen Sie zum Auflisten der lokalen Konten den Befehl aus `security login show .`

```
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.
```

Legen Sie das Kennwort für das Diagnosekonto (diag) fest

Ein Diagnosekonto mit dem Namen `diag` wird im Lieferumfang des Speichersystems angegeben. Sie können das Konto verwenden `diag` , um Fehlerbehebungsaufgaben im durchzuführen `systemshell`. Das `diag` Konto ist das einzige Konto, mit dem über den privilegierten Befehl auf die Systemshell zugegriffen werden kann `diag systemshell`.

Die Systemshell und das zugehörige `diag` Konto sind für Low-Level-Diagnosezwecke vorgesehen. Ihr Zugriff erfordert die Berechtigungsebene für die Diagnose und darf nur unter Anleitung des technischen Supports verwendet werden, um Fehlerbehebungsaufgaben durchzuführen. Weder `diag` das Konto noch das `systemshell` sind für allgemeine administrative Zwecke bestimmt.

Bevor Sie beginnen

Bevor Sie auf den zugreifen `systemshell`, müssen Sie das Kontokennwort mit dem Befehl festlegen `diag security login password`. Verwenden Sie strenge Passwort-Prinzipien und ändern Sie das `diag` Passwort in regelmäßigen Abständen.

Schritte

1. Legen Sie das Kennwort für den Kontobenutzer fest `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%
```

Überprüfung durch mehrere Administratoren

Ab ONTAP 9.11.1 können Sie mithilfe von MAV (Multi-Admin Verification) bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshots, nur nach Genehmigungen von designierten Administratoren ausführen lassen. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der MAV besteht aus folgenden Komponenten:

- "Erstellen einer oder mehrerer Administratorgenehmigungsgruppen".
- "Aktivieren der Funktion zur Verifizierung durch mehrere Administratoren".
- "Hinzufügen oder Ändern von Regeln".

Nach der Erstkonfiguration können nur Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) diese Elemente ändern.

Wenn MAV aktiviert ist, sind für jeden geschützten Vorgang drei Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, wird ein "Die Anforderung wird generiert".
2. Bevor es ausgeführt werden kann, die erforderliche Anzahl von "MAV-Administratoren müssen genehmigen".
3. Nach der Genehmigung schließt der Benutzer den Vorgang ab.

MAV ist nicht für den Einsatz bei Volumes oder Workflows mit hoher Automatisierung vorgesehen, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automatisierung und MAV gemeinsam nutzen möchten, empfiehlt NetApp, Abfragen für bestimmte MAV-Vorgänge zu verwenden. Sie können beispielsweise MAV-Regeln nur auf Volumes anwenden `volume delete` , auf die keine Automatisierung involviert ist. Sie können diese Volumes einem bestimmten Benennungsschema zuweisen.

Weitere Informationen zum MAV finden Sie im "Dokumentation zur Verifizierung durch mehrere ONTAP Administratoren".

Snapshot wird gesperrt

Beim Snapshot-Sperren handelt es sich um eine SnapLock-Funktion, bei der Snapshots manuell oder automatisch mit einer Aufbewahrungsfrist auf der Snapshot-Richtlinie des Volumes unlöschbar gemacht werden. Mit dem Zweck der Snapshot-Sperrung können Sie verhindern, dass abnormale oder nicht vertrauenswürdige Administratoren Snapshots auf dem primären oder sekundären ONTAP System löschen.

Die Snapshot-Sperrung wurde im ONTAP 9.12.1 eingeführt. Snapshot-Sperrung wird auch als manipulationssichere Snapshot Sperrung bezeichnet. Obwohl es die SnapLock-Lizenz und die Initialisierung der Compliance-Uhr erfordert, ist die Snapshot-Sperrung nicht mit SnapLock Compliance oder SnapLock Enterprise verbunden. Es gibt keinen vertrauenswürdigen Storage-Administrator, wie bei SnapLock Enterprise und er schützt nicht die zugrunde liegende physische Storage-Infrastruktur, wie bei der SnapLock Compliance. Dies ist eine Verbesserung gegenüber der SnapVaulting Snapshots auf ein sekundäres System. Die schnelle Recovery von gesperrten Snapshots auf Primärsystemen kann ermöglicht werden, um Volumes wiederherzustellen, die durch Ransomware beschädigt sind.

Weitere Informationen finden Sie im "Dokumentation zum Sperren von snapshots".

Richten Sie den zertifikatbasierten API-Zugriff ein

Statt der Benutzer-ID- und Kennwortauthentifizierung für den REST-API- oder NetApp Manageability SDK-Zugriff auf ONTAP muss die zertifikatbasierte Authentifizierung verwendet werden.

> Als Alternative zur zertifikatbasierten Authentifizierung für REST-API verwenden Sie "OAuth 2.0 Token-basierte Authentifizierung".)

Sie können ein selbstsigniertes Zertifikat auf ONTAP erstellen und installieren, wie in den folgenden Schritten beschrieben.

Schritte

1. Erstellen Sie mithilfe von OpenSSL ein Zertifikat, indem Sie den folgenden Befehl ausführen:

```
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'
```

Dieser Befehl erzeugt ein öffentliches Zertifikat mit dem Namen `test.pem` und einen privaten Schlüssel mit dem Namen `key.out`. Der allgemeine Name CN entspricht der ONTAP-Benutzer-ID.

2. Installieren Sie den Inhalt des öffentlichen Zertifikats im Format Privacy Enhanced Mail (pem) in ONTAP, indem Sie den folgenden Befehl ausführen und den Inhalt des Zertifikats einfügen, wenn Sie dazu aufgefordert werden:

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

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

3. Aktivieren Sie ONTAP, um den Clientzugriff über SSL zu erlauben, und definieren Sie die Benutzer-ID für den API-Zugriff.

```
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
```

Im folgenden Beispiel ist die Benutzer-ID `cert_user` nun für die Verwendung des zertifikatauthentifizierten API-Zugriffs aktiviert. Ein einfaches Manageability SDK Python-Skript, das zur Anzeige der ONTAP-Version verwendet `cert_user` wird, wird wie folgt angezeigt:

```
#!/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)
```

Die Ausgabe des Skripts zeigt die ONTAP-Version an.

```
./version.py

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

4. Führen Sie folgende Schritte durch, um eine zertifikatbasierte Authentifizierung mit der ONTAP REST API durchzuführen:
   a. Definieren Sie in ONTAP die Benutzer-ID für HTTP-Zugriff:

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

b. Führen Sie auf Ihrem Linux-Client den folgenden Befehl aus, der die ONTAP-Version als Ausgabe erzeugt:

```
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"
        }
    }
}
```

Weitere Informationen

- "Zertifikatbasierte Authentifizierung mit dem NetApp Manageability SDK für ONTAP".

ONTAP OAuth 2.0 Token-basierte Authentifizierung für REST-API

Als Alternative zur zertifikatbasierten Authentifizierung können Sie die auf OAuth 2.0 Token-basierte Authentifizierung für REST-API verwenden.

Ab ONTAP 9.14.1 haben Sie die Möglichkeit, den Zugriff auf Ihre ONTAP-Cluster über das Open Authorization (OAuth 2.0)-Framework zu steuern. Sie können diese Funktion über jede der ONTAP-Administrationsschnittstellen konfigurieren, einschließlich der ONTAP-CLI, System Manager und REST-API. Die OAuth 2.0-Autorisierungs- und Zugriffskontrollentscheidungen können jedoch nur angewendet werden, wenn ein Client über die REST-API auf ONTAP zugreift.

OAuth 2.0-Token ersetzen Passwörter für die Benutzerkontoauthentifizierung.

Weitere Informationen zur Verwendung von OAuth 2.0 finden Sie im "ONTAP-Dokumentation zur Authentifizierung und Autorisierung mit OAuth 2.0".

Anmelde- und Kennwortparameter

Eine effektive Sicherheitslage hält die festgelegten Unternehmensrichtlinien, Richtlinien und alle Governance- oder Standards ein, die für das Unternehmen gelten. Beispiele für diese Anforderungen sind die Lebensdauer des Benutzernamens, Anforderungen an die Länge des Passworts, Zeichenanforderungen und die Speicherung solcher Konten. Die ONTAP-Lösung bietet Funktionen für diese Sicherheitsstrukturen.

Neue lokale Kontofunktionen

Zur Unterstützung der Richtlinien, Richtlinien oder Standards für Benutzerkonten eines Unternehmens, einschließlich Governance, wird in ONTAP die folgende Funktionalität unterstützt:

- Konfigurieren von Passwortrichtlinien zur Durchsetzung einer Mindestanzahl von Ziffern, Kleinbuchstaben oder Großbuchstaben
- Nach einem fehlgeschlagenen Anmeldeversuch ist eine Verzögerung erforderlich
- Definition des inaktiven Kontonormienlimits
- Ablaufen eines Benutzerkontos
- Eine Warnmeldung zum Ablauf des Kennworts wird angezeigt
- Benachrichtigung über eine ungültige Anmeldung

Konfigurierbare Einstellungen werden über den Befehl Security Login role config modify verwaltet.

SHA-512-Unterstützung

Um die Passwortsicherheit zu verbessern, unterstützt ONTAP 9 die SHA-2-Passwort-Hash-Funktion und verwendet standardmäßig SHA-512, um neu erstellte oder geänderte Passwörter zu hashen. Operatoren und Administratoren können Konten auch nach Bedarf ablaufen lassen oder sperren.

Bereits vorhandene ONTAP 9-Benutzerkonten mit unveränderten Kennwörtern verwenden nach dem Upgrade auf ONTAP 9.0 oder höher weiterhin die MD5-Hash-Funktion. NetApp empfiehlt jedoch dringend, dass diese Benutzerkonten auf die sicherere SHA-512-Lösung migriert werden, indem Benutzer ihre Passwörter ändern müssen.

Mit der Passwort-Hash-Funktion können Sie die folgenden Aufgaben ausführen:

- Benutzerkonten anzeigen, die mit der angegebenen Hash-Funktion übereinstimmen:

```
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
```

- Konten ablaufen lassen, die eine bestimmte Hash-Funktion (z. B. MD5) verwenden, wodurch Benutzer bei der nächsten Anmeldung gezwungen werden, ihr Passwort zu ändern:

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

- Sperren Sie Konten mit Kennwörtern, die die angegebene Hash-Funktion verwenden.

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

Die Passwort-Hash-Funktion ist für den internen Benutzer in der Administrations-SVM des Clusters unbekannt `autosupport` . Dieses Problem ist kosmetisch. Die Hash-Funktion ist unbekannt, da dieser interne Benutzer standardmäßig kein konfiguriertes Passwort hat.

  - Um die Passwort-Hash-Funktion für den Benutzer anzuzeigen `autosupport` , führen Sie die folgenden Befehle aus:

```
::> 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
```

  - Um die Passwort-Hash-Funktion (Standard: sha512) einzustellen, führen Sie den folgenden Befehl aus:

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

Es spielt keine Rolle, auf welche Art das Passwort eingestellt ist.

```
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
```

Kennwortparameter

Die ONTAP Lösung unterstützt Kennwortparameter, die die Anforderungen und Richtlinien des Unternehmens erfüllen und unterstützen.

Ab 9.14.1 gibt es eine erhöhte Komplexität und Sperrregeln für Passwörter, die nur für Neuinstallationen von ONTAP gelten.

Alle Passwörter müssen vom Benutzernamen abweichen.

Attribut	Beschreibung	Standard	Bereich
`username-minlength`	Mindestlänge des Benutzernamens erforderlich	3	3-16
`username-alphanum`	Benutzername alphanumerisch	Deaktiviert	Aktiviert/deaktiviert
`passwd-minlength`	Mindestlänge des Passworts erforderlich	8	3-64
`passwd-alphanum`	Alphanumerisches Passwort	Aktiviert	Aktiviert/deaktiviert
`passwd-min-special-chars`	Mindestanzahl an Sonderzeichen im Passwort erforderlich	0	0-64
`passwd-expiry-time`	Passwortablaufzeit (in Tagen)	Unbegrenzt, d. h. die Passwörter laufen nie ab	0-unbegrenzt 0 == Jetzt ablaufen lassen

Attribut	Beschreibung	Standard	Bereich
`require-initial-passwd-update`	Erste Kennwortaktualisierung bei der ersten Anmeldung erforderlich	Deaktiviert	Aktiviert/deaktiviert Änderungen sind über Konsole oder SSH zulässig
`max-failed-login-attempts`	Maximale Anzahl fehlgeschlagener Versuche	0, Konto nicht sperren	-
`lockout-duration`	Maximale Sperrzeit (in Tagen)	Der Standardwert ist 0, was bedeutet, dass das Konto für einen Tag gesperrt ist	-
`disallowed-reuse`	Letzte N-Kennwörter nicht zulassen	6	Der Mindestwert beträgt 6
`change-delay`	Verzögerung zwischen Passwortänderungen (in Tagen)	0	-
`delay-after-failed-login`	Verzögerung nach jedem fehlgeschlagenen Anmeldeversuch (in Sekunden)	4	-
`passwd-min-lowercase-chars`	Mindestanzahl an Kleinbuchstaben im Passwort erforderlich	0. Dies erfordert keine Kleinbuchstaben	0-64
`passwd-min-uppercase-chars`	Mindestanzahl an alphabetischen Großbuchstaben erforderlich	0. Dies erfordert keine Großbuchstaben	0-64
`passwd-min-digits`	Mindestanzahl an Ziffern im Passwort erforderlich	0, die keine Ziffern erfordert	0-64
`passwd-expiry-warn-time`	Warnmeldung vor Ablauf des Passworts anzeigen (in Tagen)	Unbegrenzt, was bedeutet, dass Sie nie vor Ablauf des Passworts warnen	0. Dies bedeutet, dass der Benutzer bei jeder erfolgreichen Anmeldung über den Ablauf des Passworts informiert wird
`account-expiry-time`	Konto läuft in N Tagen ab	Unbegrenzt, d. h. die Konten laufen nie ab	Die Verfallszeit des Kontos muss größer sein als das Limit für inaktive Konten
`account-inactive-limit`	Maximale Dauer der Inaktivität vor Ablauf des Kontos (in Tagen)	Unbegrenzt. Das bedeutet, dass die inaktiven Konten nie ablaufen	Das Limit für inaktive Konten muss kleiner als die Ablaufdatum des Kontos sein

Beispiel

```
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
```

Methoden für die

Dies sind wichtige Parameter zur Stärkung der ONTAP-Systemadministration.

Zugriff über die Befehlszeile

Die Einrichtung eines sicheren Zugriffs auf Systeme ist ein wichtiger Bestandteil der Aufrechterhaltung einer sicheren Lösung. Die häufigsten Optionen für den Zugriff auf die Befehlszeile sind SSH, Telnet und RSH. Davon ist SSH die sicherste, dem Branchenstandard entsprechende Best Practice für den Remote-Zugriff auf die Befehlszeile. NetApp empfiehlt die Verwendung von SSH für den Zugriff über die Befehlszeile auf die ONTAP-Lösung.

SSH-Konfigurationen

Der `security ssh show` Befehl zeigt die Konfigurationen der SSH Schlüsselaustauschalgorithmen, Chiffren und MAC-Algorithmen für das Cluster und SVMs an. Die Schlüsselaustauschmethode verwendet diese Algorithmen und Chiffren, um festzulegen, wie die einmaligen Sitzungsschlüssel für die Verschlüsselung und Authentifizierung generiert werden und wie die Serverauthentifizierung stattfindet.

```
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.
```

Anmeldebanner

Mithilfe von Anmeldebannern kann ein Unternehmen Bedienern, Administratoren und auch Benutzern mit eingeschränkten Berechtigungen die Bedingungen für eine akzeptable Nutzung anzeigen. Die Banner zeigen an, wer berechtigt ist, auf das System zuzugreifen. Dieser Ansatz ist hilfreich, um Erwartungen an den Zugriff und die Nutzung des Systems zu ermitteln. Mit dem `security login banner modify` Befehl wird das Anmeldebanner geändert. Das Anmeldebanner wird kurz vor dem Authentifizierungsschritt während der SSH- und Konsolengeräteanmeldung angezeigt. Der Bannertext muss in doppelten Anführungszeichen („ “) stehen, wie im folgenden Beispiel gezeigt.

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

Anmeldebannerparameter

Parameter	Beschreibung
`vserver`	Verwenden Sie diesen Parameter, um die SVM mit dem geänderten Banner anzugeben. Verwenden Sie den Namen der Administrator-SVM des Clusters, um die Meldung auf Cluster-Ebene zu ändern. Meldung auf Cluster-Ebene wird als Standard für Daten-SVMs verwendet, für die keine Meldung definiert wurde.

Parameter	Beschreibung
`message`	Mit diesem optionalen Parameter kann eine Login-Banner-Meldung angegeben werden. Wenn auf dem Cluster eine Meldung zum Anmeldebanner gesetzt ist, wird das Cluster-Anmeldebanner-Banner von allen Daten-SVMs ebenfalls verwendet. Das Festlegen des Anmeldebanners einer Daten-SVM überschreibt die Anzeige des Cluster-Anmeldebanners. Verwenden Sie diesen Parameter mit dem Wert „-“, um ein Daten-SVM-Anmeldebanner zur Verwendung des Cluster-Anmeldebanners zurückzusetzen. Wenn Sie diesen Parameter verwenden, darf das Anmeldebanner keine Zeilenumbrüche (auch als Zeilenende [EOLs] oder Zeilenumbrüche bezeichnet) enthalten. Geben Sie keine Parameter an, um eine Login-Banner-Nachricht mit Zeilenumbrüche einzugeben. Sie werden aufgefordert, die Nachricht interaktiv einzugeben. Interaktiv eingegebene Nachrichten können Zeilenumbrüche enthalten. Nicht-ASCII-Zeichen müssen Unicode UTF-8 verwenden.
`uri`	`(ftp
http):///(hostname	IPv4` Verwenden Sie diesen Parameter, um den URI anzugeben, von dem das Anmeldebanner heruntergeladen wird. Die Länge der Nachricht darf 2048 Byte nicht überschreiten. Nicht-ASCII-Zeichen müssen als Unicode UTF-8 angegeben werden.

Nachricht des Tages

Der `security login motd modify` Befehl aktualisiert die Nachricht des Tages (MOTD).

Es gibt zwei Kategorien von MOTD: Die Cluster-Level-MOTD und die Daten-SVM-Level-MOTD. Ein Benutzer, der sich bei der Clustershell einer Daten-SVM anmeldet, kann zwei Meldungen sehen: Die MOTD auf Cluster-Ebene gefolgt von der MOTD auf SVM-Ebene für diese SVM.

Der Clusteradministrator kann bei Bedarf die Clusterebene-MOTD auf jeder SVM einzeln aktivieren oder deaktivieren. Wenn der Clusteradministrator die MOTD auf Cluster-Ebene für eine SVM deaktiviert, kann ein Benutzer, der sich bei der SVM anmeldet, die Meldung auf Cluster-Ebene nicht sehen. Nur ein Clusteradministrator kann die Meldung auf Cluster-Ebene aktivieren oder deaktivieren.

MOTD-Parameter	Beschreibung
Vserver	Verwenden Sie diesen Parameter, um die SVM anzugeben, für die die MOTD geändert wird. Verwenden Sie den Namen der Administrator-SVM des Clusters, um die Meldung auf Cluster-Ebene zu ändern.

MOTD-Parameter	Beschreibung
Nachricht	Mit diesem optionalen Parameter kann eine Meldung angegeben werden. Wenn Sie diesen Parameter verwenden, kann die MOTD keine Zeilenumbrüche enthalten. Wenn Sie außer dem Parameter keinen anderen Parameter angeben `-vserver` , werden Sie aufgefordert, die Meldung interaktiv einzugeben. Interaktiv eingegebene Nachrichten können Zeilenumbrüche enthalten. Nicht-ASCII-Zeichen müssen als Unicode UTF-8 angegeben werden. Die Nachricht kann dynamisch generierten Inhalt mit den folgenden Escape-Sequenzen enthalten: • `\\` - Ein einziger Gegenspielcharakter • `\b` - Keine Ausgabe (nur zur Kompatibilität mit Linux unterstützt) • `\C` - Cluster-Name • `\d` - Aktuelles Datum wie auf dem Login-Knoten eingestellt • `\t` - Aktuelle Zeit wie auf dem Login-Knoten eingestellt • `\I` - Eingehende LIF IP-Adresse (druckt Konsole für einen `console` Login) • `\l` - Login-Gerätename (druckt Konsole für einen `console` Login) • `\L` - Letzte Anmeldung für den Benutzer auf einem beliebigen Knoten im Cluster • `\m` - Maschinenarchitektur • `\n` - Knoten oder Daten-SVM-Name • `\N` - Name des Benutzers, der sich anmeldet • `\o` - Wie \O. Für Linux-Kompatibilität bereitgestellt. • `\O` - DNS-Domain-Name des Knotens. Beachten Sie, dass die Ausgabe von der Netzwerkkonfiguration abhängt und möglicherweise leer ist. • `\r` - Software-Release-Nummer • `\s` - Name des Betriebssystems • `\u` - Anzahl der aktiven Clustershell-Sitzungen auf dem lokalen Knoten. Für den Cluster-Admin: Alle clustershell-Benutzer. Für den Daten-SVM-Administrator: Nur aktive Sitzungen für diese Daten-SVM • `\U` - Wie `\u`, aber hat `user` oder `users` angehängt • `\v` - Effektive Cluster Version String • `\W` - Aktive Sitzungen im Cluster für die Anmeldung des Benutzers (`who`)

Weitere Informationen zum Konfigurieren der Tagesnachricht in ONTAP finden Sie im "ONTAP-Dokumentation über die Botschaft des Tages".

Zeitüberschreitung für CLI-Sitzung

Das standardmäßige Timeout für die CLI-Sitzung beträgt 30 Minuten. Das Timeout ist wichtig, um veraltete Sitzungen und Session Huckepack zu verhindern.

Verwenden Sie den `system timeout show` Befehl, um das aktuelle Timeout für die CLI-Sitzung anzuzeigen.

Verwenden Sie den Befehl, um den Zeitüberschreitungswert festzulegen `system timeout modify -timeout <minutes>`.

Webzugriff mit NetApp ONTAP System Manager

Wenn ein ONTAP Administrator für den Zugriff und das Management eines Clusters eine grafische Benutzeroberfläche anstelle der CLI verwenden möchte, verwenden Sie NetApp ONTAP System Manager. Sie ist in ONTAP als Webdienst enthalten, standardmäßig aktiviert und über einen Browser zugänglich. Zeigen Sie im Browser auf den Hostnamen, wenn Sie DNS oder die IPv4- oder IPv6-Adresse über verwenden `https://cluster-management-LIF`.

Wenn das Cluster ein selbstsigniertes digitales Zertifikat verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, den Zugriff fortzusetzen, oder ein digitales Zertifikat (CA) für die Serverauthentifizierung auf dem Cluster installieren.

Ab ONTAP 9.3 ist die SAML-Authentifizierung (Security Assertion Markup Language) eine Option für den ONTAP-System-Manager.

SAML-Authentifizierung für ONTAP System Manager

SAML 2.0 ist ein weit verbreiteter Industriestandard, der es jedem SAML-konformen Identitätsanbieter (IdP) von Drittanbietern ermöglicht, MFA mithilfe von Mechanismen durchzuführen, die für das IdP der Unternehmenswahl einzigartig sind, und als Single Sign-On (SSO)-Quelle.

In der SAML-Spezifikation sind drei Rollen definiert: Der Principal, der IdP und der Service Provider. Bei der ONTAP-Implementierung ist der Clusteradministrator, der über ONTAP System Manager oder NetApp Active IQ Unified Manager auf ONTAP zugreifen kann. Das IdP ist eine IdP-Software von Drittanbietern. Ab ONTAP 9.3 werden Microsoft Active Directory Federated Services (ADFS) und das Open-Source-Shibboleth-IdP unterstützt. Ab ONTAP 9.12.1 wird Cisco DUO als IdP unterstützt. Bei dem Service-Provider handelt es sich um die in ONTAP integrierte SAML-Funktion, die vom ONTAP-System-Manager oder der Active IQ Unified Manager-Web-Applikation verwendet wird.

Im Gegensatz zum SSH-Zweifaktor-Konfigurationsprozess müssen sich nach Aktivierung der SAML-Authentifizierung alle vorhandenen Administratoren für den Zugriff auf ONTAP-System-Manager oder ONTAP-Serviceprozessor über das SAML-IdP authentifizieren. Es sind keine Änderungen an den Cluster-Benutzerkonten erforderlich. Wenn die SAML-Authentifizierung aktiviert ist, wird vorhandenen Benutzern mit Administratorrollen für und -Anwendungen eine neue Authentifizierungsmethode von `saml` hinzugefügt `http ontapi`.

Nachdem die SAML-Authentifizierung aktiviert ist, sollten in ONTAP weitere neue Konten definiert werden, die SAML-IdP-Zugriff erfordern, mit der Administratorrolle und der saml-Authentifizierungsmethode für `http` und-`ontapi` Anwendungen. Wenn die SAML-Authentifizierung zu einem bestimmten Zeitpunkt deaktiviert ist, muss für diese neuen Konten die `password` Authentifizierungsmethode mit der Administratorrolle für und-Anwendungen definiert werden `http` `ontapi` und die Anwendung für die lokale ONTAP-Authentifizierung in ONTAP System Manager hinzugefügt `console` werden.

Nachdem das SAML-IdP aktiviert wurde, führt das IdP eine Authentifizierung für den Zugriff auf ONTAP-System-Manager durch, indem es Methoden verwendet, die dem IdP zur Verfügung stehen, z. B. LDAP (Lightweight Directory Access Protocol), AD (Active Directory), Kerberos, Passwort usw. Die verfügbaren Methoden sind einzigartig für die IdP. Es ist wichtig, dass die in ONTAP konfigurierten Konten über Benutzer-IDs verfügen, die den IdP-Authentifizierungsmethoden zugeordnet sind.

Von NetApp validierte IDPs sind Microsoft ADFS, Cisco DUO und Open Source Shibboleth IdP.

Ab ONTAP 9.14.1 kann Cisco DUO als zweiter Authentifizierungsfaktor für SSH verwendet werden.

Weitere Informationen zur Multi-Faktor-Authentifizierung (MFA) für ONTAP System Manager, Active IQ Unified Manager und SSH sind unter "TR-4647: Multifaktor-Authentifizierung in ONTAP 9" zu finden.

Einblicke in ONTAP System Manager

Ab ONTAP 9.11.1 bietet ONTAP System Manager Einblicke, die Cluster-Administratoren bei der Optimierung ihrer täglichen Aufgaben unterstützen. Die Erkenntnisse zur Sicherheit basieren auf den Empfehlungen dieses technischen Berichts.

Security Insight	Entschlossenheit
Telnet ist aktiviert	NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff.
Remote Shell (RSH) ist aktiviert	NetApp empfiehlt SSH für sicheren Remote-Zugriff.
AutoSupport verwendet ein unsicheres Protokoll	AutoSupport ist nicht für den Versand über Link:HTTPS konfiguriert.
Der Anmeldebanner ist auf Cluster-Ebene nicht konfiguriert	Warnung, wenn das Anmeldebanner für das Cluster nicht konfiguriert ist.
SSH verwendet unsichere Chiffren	Warnung, wenn SSH unsichere Chiffren verwendet.
Es sind zu wenige NTP-Server konfiguriert	Warnung, wenn die Anzahl der konfigurierten NTP-Server kleiner als drei ist.
Standard-Admin-Benutzer nicht gesperrt	Wenn Sie keine Standard-Administratorkonten (admin oder diag) für die Anmeldung bei System Manager verwenden und diese Konten nicht gesperrt sind, sollten Sie sie sperren.
Ransomware-Verteidigung: Volumes verfügen nicht über Snapshot-Richtlinien	An ein oder mehrere Volumes ist keine angemessene Snapshot-Richtlinie gebunden.
Ransomware-Verteidigung: Deaktivieren Sie das automatische Löschen von Snapshot	Die automatische Löschung von Snapshots ist für ein oder mehrere Volumes festgelegt.
Volumes werden nicht auf Ransomware-Angriffe überwacht	Autonomer Ransomware-Schutz wird auf mehreren Volumes unterstützt, aber noch nicht konfiguriert.
SVMs sind nicht für den autonomen Ransomware-Schutz konfiguriert	Autonomer Ransomware-Schutz wird auf mehreren SVMs unterstützt, aber noch nicht konfiguriert.
Native FPolicy ist nicht konfiguriert	FPolicy ist nicht für NAS SVMs festgelegt.
Autonomer Ransomware-Schutz, aktiv-Modus	Mehrere Volumes haben ihren Lernmodus abgeschlossen, und Sie können den aktiven Modus einschalten
Die globale FIPS 140-2-2-Compliance ist deaktiviert	Die globale FIPS 140-2-Compliance ist nicht aktiviert.
Das Cluster ist nicht für Benachrichtigungen konfiguriert	E-Mails, Webhooks oder SNMP-Traphosts sind nicht für den Empfang von Benachrichtigungen konfiguriert.

Weitere Informationen zu den Einblicken in ONTAP System Manager finden Sie in der "ONTAP System Manager – Dokumentation zu den Einblicken".

Zeitüberschreitung bei System Manager-Sitzung

Sie können das Zeitlimit für die Inaktivität der System Manager Sitzung ändern. Das standardmäßige Zeitlimit für Inaktivität beträgt 30 Minuten. Ein Timeout ist wichtig, um veraltete Sitzungen und Session Huckepack zu verhindern.

Wenn SAML konfiguriert ist, wird das Inaktivitäts-Timeout durch Einstellungen auf dem IdP gesteuert.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **UI settings** .
3. Geben Sie im Feld **Inaktivität Timeout** einen Minutenwert zwischen 2 und 180 ein oder geben Sie „0“ ein, um das Timeout zu deaktivieren.
4. Wählen Sie **Speichern**.

Autonomer Ransomware-Schutz von ONTAP

Als Ergänzung zur Analyse des Benutzerverhaltens für die Sicherheit von Storage-Workloads analysiert der autonome Ransomware-Schutz von ONTAP Volume-Workloads und Entropie, um Ransomware zu erkennen. Er erstellt einen Snapshot und benachrichtigt den Administrator, wenn der Verdacht eines Angriffs besteht.

Zusätzlich zur Ransomware-Erkennung und -Prävention durch externe FPolicy-Benutzerverhaltensanalysen (UBA) mit NetApp Data Infrastructure Insights Storage Workload Security und dem NetApp FPolicy-Partner-Ökosystem führt ONTAP 9.10.1 einen autonomen Ransomware-Schutz ein. Der autonome Ransomware-Schutz von ONTAP nutzt eine integrierte On-Box-Funktion für maschinelles Lernen (ML), die die Workload-Aktivität des Volumens sowie die Datenentropie berücksichtigt, um Ransomware automatisch zu erkennen. Es überwacht Aktivitäten, die sich von UBA unterscheiden, sodass es Angriffe erkennen kann, die UBA nicht erkennt.

Weitere Informationen zu dieser Funktion finden Sie unter "NetApp Lösungen für Ransomware" oder "Dokumentation zum autonomen Ransomware-Schutz von ONTAP".

Prüfung von Storage-Verwaltungssystemen

Stellen Sie die Integrität der Ereignisüberwachung sicher, indem Sie ONTAP-Ereignisse auf einen Remote-Syslog-Server laden. Bei diesem Server könnte es sich um ein Sicherheitsinformationsereignismanagementsystem wie Splunk handelt.

Senden Sie Syslog

Protokoll- und Audit-Informationen sind für ein Unternehmen im Hinblick auf Support und Verfügbarkeit von unschätzbarem Wert. Zudem handelt es sich bei den in Protokollen (Syslog) und Audit-Berichten enthaltenen Informationen und Details in der Regel um sensible Daten. Um die Sicherheitskontrollen und das Sicherheitsniveau aufrechtzuerhalten, müssen Unternehmen die Protokoll- und Audit-Daten unbedingt sicher managen.

Das verlagern von Syslog-Informationen ist nötig, um den Umfang oder die Auswirkungen einer Sicherheitsverletzung auf ein einzelnes System oder eine einzelne Lösung zu beschränken. Daher empfiehlt NetApp, Syslog-Informationen sicher an einen sicheren Storage- oder Aufbewahrungsort zu verlagern.

Erstellen Sie ein Ziel für die Protokollweiterleitung

Verwenden Sie den `cluster log-forwarding create` Befehl, um Protokollweiterleitungsziele für die Remote-Protokollierung zu erstellen.

Parameter

Verwenden Sie die folgenden Parameter, um den Befehl zu konfigurieren `cluster log-forwarding create`:

- **Ziel-Host.** Dieser Name ist der Hostname oder die IPv4- oder IPv6-Adresse des Servers, an den die Protokolle weitergeleitet werden sollen.

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

- **Zielport.** Dies ist der Port, an dem der Zielserver abhört.

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

- **Protokoll zur Protokollweiterleitung.** Dieses Protokoll wird zum Senden von Meldungen an das Ziel verwendet.

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

  Das Protokoll für die Protokollweiterleitung kann einen der folgenden Werte verwenden:

  - `udp-unencrypted`. Benutzer-Datagram-Protokoll ohne Sicherheit.
  - `tcp-unencrypted`. TCP ohne Sicherheit.
  - `tcp-encrypted`. TCP mit Transport Layer Security (TLS).
- * Überprüfen Sie die Identität des Zielservers.* Wenn dieser Parameter auf true gesetzt ist, wird die Identität des Protokollweiterleitungsziels durch Validierung des Zertifikats überprüft. Der Wert kann nur dann auf TRUE gesetzt werden, wenn der `tcpencrypted` Wert im Protokollfeld ausgewählt ist.

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

- **Syslog-Funktion.** Dieser Wert ist die Syslog-Funktion, die für die weitergeleiteten Protokolle verwendet werden soll.

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

- **Überspringen Sie den Verbindungstest.** Normalerweise überprüft der `cluster log-forwarding create` Befehl, ob das Ziel durch Senden eines ICMP-Ping (Internet Control Message Protocol) erreichbar ist, und schlägt fehl, wenn es nicht erreichbar ist. Wenn Sie diesen Wert so einstellen, `true` dass die Ping-Prüfung umgangen wird, können Sie das Ziel konfigurieren, wenn es nicht erreichbar ist.

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

NetApp empfiehlt, die Verbindung zu einem Typ mit dem `cluster log-forwarding` Befehl zu erzwingen `-tcp-encrypted`.

Ereignisbenachrichtigung

Der Schutz der Informationen und Daten, die ein System verlassen, ist für die Aufrechterhaltung und das Management der Sicherheit des Systems von entscheidender Bedeutung. Die durch die ONTAP Lösung generierten Ereignisse bieten eine Fülle von Informationen über die Lösung, die verarbeiteten Informationen und vieles mehr. Die Vitalität dieser Daten macht deutlich, dass sie sicher gemanagt und migriert werden müssen.

Der `event notification create` Befehl sendet eine neue Benachrichtigung über eine Reihe von Ereignissen, die durch einen Ereignisfilter definiert wurden, an ein oder mehrere Benachrichtigungsziele. In den folgenden Beispielen werden die Konfiguration für Ereignisbenachrichtigungen und der `event notification show` Befehl dargestellt, mit dem die konfigurierten Filter und Ziele für Ereignisbenachrichtigungen angezeigt werden.

```
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
```

Storage-Verschlüsselung in ONTAP

Verwenden Sie zur Sicherung sensibler Daten im Falle einer gestohlenen, zurückgegebenen oder umgewandten Festplatte die hardwarebasierte Storage-Verschlüsselung von NetApp oder die softwarebasierte Volume-Verschlüsselung/NetApp Aggregatverschlüsselung. Beide Mechanismen sind nach FIPS-140-2 validiert. Wenn hardwarebasierte Mechanismen mit softwarebasierten Mechanismen verwendet werden, ist die Lösung für das Commercial Solutions for Classified (CSfC)-Programm qualifiziert. Die Lösung bietet erweiterten Schutz für geheime und streng geheime Daten im Ruhezustand sowohl auf der Hardware- als auch auf der Softwareebene.

Die Verschlüsselung ruhender Daten ist wichtig, um sensible Daten bei Diebstahl, Rückgabe oder neuer Verwendung einer Festplatte zu schützen.

ONTAP 9 bietet drei FIPS 140-2-konforme Verschlüsselungslösungen für Daten im Ruhezustand:

- NetApp Storage Encryption (NSE) ist eine Hardwarelösung, die Self-Encrypting Drives verwendet.
- NetApp Volume Encryption (NVE) ist eine Softwarelösung, die die Verschlüsselung beliebiger Daten-Volumes auf jedem Laufwerkstyp ermöglicht, bei dem sie aktiviert wird, mit einem eindeutigen Schlüssel für

jedes Volume.

- NetApp Aggregate Encryption (NAE) ist eine Softwarelösung, die die Verschlüsselung beliebiger Daten-Volumes auf beliebigen Laufwerken ermöglicht, wobei sie mit eindeutigen Schlüsseln für jedes Aggregat aktiviert wird.

NSE, NVE und NAE können entweder externes Verschlüsselungsmanagement oder den Onboard Key Manager (OKM) verwenden. Die Verwendung von NSE, NVE und NAE wirkt sich nicht auf die ONTAP Storage-Effizienzfunktionen aus. NVE Volumes sind jedoch von der Aggregatdeduplizierung ausgeschlossen. NAE Volumes werden in die Aggregatdeduplizierung einbezogen und profitieren von ihnen.

OKM bietet eine eigenständige Verschlüsselungslösung für Daten im Ruhezustand mit NSE, NVE oder NAE.

NVE, NAE und OKM verwenden den ONTAP CryptoMod. CryptoMod ist in der nach FIPS 140-2 validierten CMVP-Modulliste aufgeführt. Siehe "FIPS 140-2 Cert# 4144".

Verwenden Sie zum Starten der OKM-Konfiguration den `security key-manager onboard enable` Befehl. Um externe KMIP-Schlüsselmanager (Key Management Interoperability Protocol) zu konfigurieren, verwenden Sie den `security key-manager external enable` Befehl. Ab ONTAP 9.6 wird die Mandantenfähigkeit für externe Schlüsselmanager unterstützt. Verwenden Sie den `-vserver <vserver name>` Parameter, um das externe Verschlüsselungsmanagement für eine bestimmte SVM zu aktivieren. Vor 9.6 wurde der `security key-manager setup` Befehl verwendet, um sowohl OKM als auch externe Schlüsselmanager zu konfigurieren. Für das Onboard-Verschlüsselungsmanagement leitet diese Konfiguration den Bediener oder Administrator durch die Passphrase-Einrichtung und zusätzliche Parameter für die Konfiguration von OKM.

Ein Teil der Konfiguration wird im folgenden Beispiel dargestellt:

```
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.
```

Ab ONTAP 9.4 können Sie die Option true mit verwenden `-enable-cc-mode` `security key-manager setup` , um die Eingabe der Passphrase nach einem Neustart durch Benutzer zu verlangen. Für ONTAP 9.6 und höher lautet die Befehlssyntax `security key-manager onboard enable -cc-mode-enabled yes`.

Ab ONTAP 9.4 können Sie die Funktion mit erweiterten Berechtigungen verwenden `secure-purge` , um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu „Scrub“. Durch das Scrubbing von Daten auf einem verschlüsselten Volume wird sichergestellt, dass sie nicht von den physischen Medien wiederhergestellt werden können. Mit dem folgenden Befehl werden die gelöschten Dateien auf vol1 auf SVM vs1 sicher gelöscht:

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

Ab ONTAP 9.7 sind NAE und NVE standardmäßig aktiviert, wenn die VE-Lizenz vorhanden ist, OKM- oder externe Schlüsselmanager konfiguriert werden und NSE nicht verwendet wird. NAE-Volumes werden auf NAE-Aggregaten standardmäßig erstellt und NVE-Volumes werden standardmäßig auf nicht-NAE-Aggregaten erstellt. Sie können diesen umgehen, indem Sie den folgenden Befehl eingeben:

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

Ab ONTAP 9.6 können Sie mithilfe eines SVM-Umfangs externes Verschlüsselungsmanagement für eine Daten-SVM im Cluster konfigurieren. Dies ist insbesondere für mandantenfähige Umgebungen geeignet, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten. Weitere Informationen finden Sie unter "Aktivieren Sie das externe Schlüsselmanagement in ONTAP 9.6 und höher" in der ONTAP-Dokumentation.

Ab ONTAP 9.11.1 können Sie die Konnektivität zu geclusterten externen Schlüsselmanagementservern konfigurieren, indem Sie primäre und sekundäre Schlüsselserver auf einer SVM festlegen. Weitere Informationen finden Sie unter "Konfiguration von geclusterten externen Schlüsselservern" in der ONTAP-Dokumentation.

Ab ONTAP 9.13.1 können Sie externe Schlüsselmanager-Server im System Manager konfigurieren. Weitere Informationen finden Sie unter "Management externer Schlüsselmanager" in der ONTAP-Dokumentation.

Datenreplizierung Verschlüsselung

Zur Ergänzung der Daten im Ruhezustand-Verschlüsselung können Sie den ONTAP-Datenreplizierungsverkehr zwischen Clustern mithilfe von TLS mit einem vorab vereinbarten Schlüssel für SnapMirror, SnapVault oder FlexCache verschlüsseln.

Bei der Replizierung von Daten für Disaster Recovery, Caching oder Backup müssen die Daten während der Übertragung über das Netzwerk von einem ONTAP Cluster zum anderen gesichert werden. Auf diese Weise werden böswillige man-in-the-Middle-Angriffe auf sensible Daten während der Übertragung verhindert.

Ab ONTAP 9.6 bietet die Cluster-Peering-Verschlüsselung TLS 1.2 AES-256 GCM-Verschlüsselungsunterstützung für ONTAP Datenreplizierungsfunktionen wie SnapMirror, SnapVault und FlexCache. Die Verschlüsselung wird mittels eines vorab vereinbarten Schlüssels (PSK) zwischen zwei Cluster-Peers eingerichtet.

Ab ONTAP 9.15.1 bietet die Cluster-Peering-Verschlüsselung Unterstützung für TLS 1.3 AES-256 GCM-Verschlüsselung für ONTAP Datenreplizierungsfunktionen wie SnapMirror, SnapVault und FlexCache. Die Verschlüsselung wird mittels eines vorab vereinbarten Schlüssels (PSK) zwischen zwei Cluster-Peers eingerichtet.

Kunden, die Technologien wie NSE, NVE und NAE zum Schutz von Daten im Ruhezustand verwenden, können auch eine Ende-zu-Ende-Datenverschlüsselung nutzen, indem sie auf ONTAP 9.6 oder höher upgraden, um Cluster-Peering-Verschlüsselung zu verwenden.

Cluster-Peering verschlüsselt alle Daten zwischen den Cluster-Peers. Beispielsweise werden bei Verwendung von SnapMirror sowohl alle Peering-Informationen als auch alle SnapMirror-Beziehungen zwischen dem Quell- und Ziel-Cluster-Peer verschlüsselt. Sie können keine Klartextdaten zwischen Cluster-Peers übertragen, wenn die Cluster-Peering-Verschlüsselung aktiviert ist.

Ab ONTAP 9.6 ist die Verschlüsselung neuer Cluster-Peer-Beziehungen standardmäßig aktiviert. Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, müssen Sie sowohl den Quell- als auch den Ziel-Cluster auf 9.6 aktualisieren. Außerdem müssen Sie den `cluster peer modify` Befehl verwenden, um sowohl die Quell- als auch die Ziel-Cluster-Peers so zu ändern, dass sie die Cluster-Peering-Verschlüsselung verwenden.

Sie können eine bestehende Peer-Beziehung so umwandeln, dass sie Cluster-Peering-Verschlüsselung in ONTAP 9.6 verwendet, wie im folgenden Beispiel gezeigt:

```
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.
```

IPsec-Verschlüsselung von aktiven Daten

Unternehmen, die Verschlüsselungstechnologien für ruhende Daten wie NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) und Cluster Peering Encryption (CPE) für den Datenreplizierungsverkehr verwenden, können jetzt durch ein Upgrade auf ONTAP 9.8 oder höher die End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud-Data Fabric nutzen IPsec: IPsec bietet eine Alternative zur NFS- oder SMB/CIFS-Verschlüsselung und ist die einzige Option für die Verschlüsselung bei iSCSI-Datenverkehr.

In manchen Situationen müssen möglicherweise alle Client-Daten geschützt werden, die über das Netzwerk (oder bei der Übertragung) zu der ONTAP SVM übertragen werden. Dadurch werden Replay- und böswillige man-in-the-Middle-Angriffe auf sensible Daten während der Übertragung verhindert.

Ab ONTAP 9.8 bietet die Internetprotokollsicherheit (IPsec) End-to-End-Verschlüsselungsunterstützung für den gesamten IP-Datenverkehr zwischen einem Client und einer ONTAP SVM. Die IPsec-Datenverschlüsselung für den gesamten IP-Datenverkehr umfasst NFS-, iSCSI- und SMB/CIFS-Protokolle. IPsec bietet die einzige Verschlüsselung im Flug für iSCSI-Datenverkehr.

Die Bereitstellung von NFS-Verschlüsselung über das Netzwerk ist einer der wichtigsten Anwendungsfälle für IPsec. Vor ONTAP 9.8 war für die NFS-Verschlüsselung über das Netzwerk die Einrichtung und Konfiguration von Kerberos erforderlich, damit NFS-Daten bei der Übertragung mit krb5p verschlüsselt werden. Dies ist nicht immer einfach oder leicht in jeder Kundenumgebung zu erreichen.

Unternehmen, die Verschlüsselungstechnologien für ruhende Daten wie NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) und Cluster Peering Encryption (CPE) für den Datenreplizierungsverkehr verwenden, können jetzt durch ein Upgrade auf ONTAP 9.8 oder höher die End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud-Data Fabric nutzen IPsec:

IPsec ist ein IETF-Standard. ONTAP verwendet IPsec im Transportmodus. Es nutzt auch das IKE-Protokoll (Internet Key Exchange) Version 2, das einen Pre-Shared Key (PSK) verwendet, um Schlüsselmaterial zwischen dem Client und ONTAP entweder mit IPv4 oder IPv6 auszuhandeln. Standardmäßig verwendet

IPsec Suite-B AES-GCM 256-Bit-Verschlüsselung. Suite-B AES-GMAC256 und AES-CBC256 mit 256-Bit-Verschlüsselung werden ebenfalls unterstützt.

Obwohl die IPsec-Funktion auf dem Cluster aktiviert werden muss, wird sie durch Verwendung eines SPD-Eintrags (Security Policy Database) auf einzelne SVM-IP-Adressen angewendet. Der Richtlinieneintrag (SPD) enthält die Client-IP-Adresse (Remote-IP-Subnetz), die SVM-IP-Adresse (lokales IP-Subnetz), die zu verwendende Verschlüsselungssuite und den Pre-Shared-Schlüssel (PSK), der für die Authentifizierung über IKEv2 und den Aufbau der IPsec-Verbindung benötigt wird. Zusätzlich zum IPsec-Richtlinieneintrag muss der Client mit denselben Informationen (lokale und Remote-IP, PSK und Chiffre-Suite) konfiguriert werden, bevor der Datenverkehr über die IPsec-Verbindung fließen kann. Ab ONTAP 9.10.1 wird die IPsec-Zertifikatauthentifizierung unterstützt. Dadurch werden IPsec-Richtlinienbeschränkungen entfernt und Windows-Betriebssystemunterstützung für IPsec aktiviert.

Wenn zwischen dem Client und der SVM-IP-Adresse eine Firewall vorhanden ist, muss die ESP- und UDP-Protokolle (Port 500 und 4500) sowohl Inbound (Ingress) als auch Outbound (Egress) zugelassen werden, damit die IKEv2-Verhandlung erfolgreich ist und damit IPsec-Datenverkehr ermöglicht wird.

Für die Verkehrsverschlüsselung mit NetApp SnapMirror und Cluster-Peering wird die Cluster-Peering-Verschlüsselung (CPE) für die sichere Übertragung über das Netzwerk weiterhin über IPsec empfohlen. CPE bietet für diese Workloads eine bessere Performance als IPsec. Sie benötigen keine Lizenz für IPsec und es gibt keine Import- oder Exportbeschränkungen.

Sie können IPsec auf dem Cluster aktivieren und einen SPD-Eintrag für einen einzelnen Client und eine einzelne SVM-IP-Adresse erstellen, wie im folgenden Beispiel gezeigt:

```
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).
```

Verwandte Informationen

"Bereiten Sie die Verwendung der IP-Sicherheit im ONTAP-Netzwerk vor"

FIPS-Modus und TLS- und SSL-Management in ONTAP

Der FIPS 140-2-Standard legt Sicherheitsanforderungen für kryptografische Module in Sicherheitssystemen fest, die sensible Informationen in Computer- und Telekommunikationssystemen schützen. Der FIPS 140-2-Standard gilt *speziell* für das kryptografische Modul und nicht für das Produkt, die Architektur, die Daten oder das Ökosystem. Das kryptografische Modul ist die spezifische Komponente (Hardware, Software, Firmware oder eine Kombination der drei), die von NIST zugelassene Sicherheitsfunktionen implementiert.

Die Aktivierung der FIPS 140-2-2-Konformität hat Auswirkungen auf andere interne und externe Systeme und die Kommunikation mit ONTAP 9. NetApp empfiehlt dringend, diese Einstellungen auf einem nicht-produktiven System mit Konsolenzugriff zu testen.

Ab ONTAP 9.11.1 und TLS 1.3-Unterstützung können Sie FIPS 140-3 validieren.

Die FIPS-Konfiguration gilt für ONTAP und die Plattform BMC.

NetApp ONTAP FIPS-Mode-Konfiguration

NetApp ONTAP verfügt über eine FIPS-Modus-Konfiguration, die eine zusätzliche Sicherheitsstufe der Kontrollebene instanziiert:

- Ab ONTAP 9.11.1 sind bei aktiviertem FIPS 140-2-Compliance-Modus TLSv1, TLSv1.1 und SSLv3 deaktiviert, und nur TSLv1.2 und TSLv1.3 bleiben aktiviert. Sie wirkt sich auf andere interne und externe Systeme und Kommunikation mit ONTAP 9 aus. Wenn Sie den FIPS 140-2 Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1, TLSv1.1 und SSLv3 deaktiviert. Je nach vorheriger Konfiguration bleibt entweder TLSv1.2 oder TLSv1.3 aktiviert.
- Bei Versionen von ONTAP vor 9.11.1, wenn der FIPS 140-2-Compliance-Modus aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn der Compliance-Modus nach FIPS 140-2 aktiviert ist. Wenn Sie den FIPS 140-2-Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1 und SSLv3 deaktiviert, jedoch sind je nach vorheriger Konfiguration entweder TLSv1.2 oder TLSv1.1 und TLSv1.2 aktiviert.
- "Cryptographic Security Module (NCSM) von NetApp", Das nach FIPS 140-2 Level 1 validiert ist, bietet softwarebasierte Compliance.

NIST hat einen FIPS-140-3-Standard eingereicht und NCSM verfügt über FIPS-140-2- und FIPS-140-3-Validierungen. Alle FIPS 140-2-Validierungen werden am 21. September 2026, also fünf Jahre nach dem letzten Tag für neue Zertifikatsübermittlungen, in den historischen Status versetzt.

Ermöglichen Sie den Compliance-Modus nach FIPS-140-2 und FIPS-140-3

Ab ONTAP 9 können die Compliance-Modi FIPS-140-2 und FIPS-140-3 für Cluster-weite Kontrollebene-Schnittstellen aktiviert werden.

- "Aktivieren Sie FIPS"
- "Anzeigen des FIPS-Status"

FIPS-Enablement und -Protokolle

`security config modify`Mit dem Befehl können Sie die vorhandene Cluster-weite Sicherheitskonfiguration ändern. Wenn Sie den FIPS-konformen Modus aktivieren, wählt das Cluster automatisch nur TLS-Protokolle aus.

- Verwenden Sie den `-supported-protocols` Parameter, um TLS-Protokolle unabhängig vom FIPS-Modus ein- oder auszuschließen. Standardmäßig ist der FIPS-Modus deaktiviert und die Protokolle TLSv1.3 (beginnend mit ONTAP 9.11.1) und TLSv1.2 sind aktiviert.
- In früheren ONTAP-Versionen waren standardmäßig die folgenden TLS-Protokolle aktiviert:
  - TLSv1.1 (standardmäßig deaktiviert ab ONTAP 9.12.1)
  - TLSv1 (standardmäßig deaktiviert, beginnend mit ONTAP 9.8)
- Zur Rückwärtskompatibilität unterstützt ONTAP das Hinzufügen von SSLv3 zur Liste der unterstützten

Protokolle, wenn der FIPS-Modus deaktiviert ist.

FIPS-Enablement und Verschlüsselung

- Verwenden Sie den `-supported-cipher-suites` Parameter, um nur den Advanced Encryption Standard (AES) oder AES und 3DES zu konfigurieren.
- Sie können schwache Chiffren wie RC4 deaktivieren `!RC4`, indem Sie angeben. Standardmäßig ist die unterstützte Chiffre-Einstellung `ALL:!LOW:!aNULL:!EXP:!eNULL`. Diese Einstellung bedeutet, dass alle unterstützten Cipher-Suites für die Protokolle aktiviert sind, mit Ausnahme der 64-Bit- oder 56-Bit-Verschlüsselungsalgorithmen ohne Authentifizierung, keine Verschlüsselung, keine Exporte und Verschlüsselungssuites mit geringer Verschlüsselung.
- Wählen Sie eine Verschlüsselungssuite aus, die mit dem entsprechenden ausgewählten Protokoll verfügbar ist. Eine ungültige Konfiguration kann dazu führen, dass einige Funktionen nicht ordnungsgemäß funktionieren.
- Die korrekte Syntax für die Chiffrierzeichenfolge finden Sie im "Seite „Chiffren“" auf OpenSSL (veröffentlicht von OpenSSL Software Foundation). Ab ONTAP 9.9.1 und neueren Versionen müssen Sie nach Änderung der Sicherheitskonfiguration nicht mehr alle Nodes manuell neu booten.

Erhöhung der SSH- und TLS-Sicherheit

Für die SSH-Administration von ONTAP 9 ist ein OpenSSH-Client 5.7 oder höher erforderlich. SSH-Clients müssen mit dem öffentlichen Schlüsselalgorithmus Elliptic Curve Digital Signature Algorithm (ECDSA) verhandeln, damit die Verbindung erfolgreich hergestellt werden kann.

Um TLS-Sicherheit zu erhärten, aktivieren Sie nur TLS 1.2 und verwenden Sie Cipher Suites, die Perfect Forward Secrecy (PFS) bieten. PFS ist eine Methode des Schlüsselaustauschs, die in Kombination mit Verschlüsselungsprotokollen wie TLS 1.2 einen Angreifer daran hindert, alle Netzwerksitzungen zwischen einem Client und einem Server zu entschlüsseln.

Aktivieren Sie TLSv1.2- und PFS-fähige Chiffre-Suites

Um nur TLS 1.2- und PFS-fähige Cipher-Suites `security config modify` zu aktivieren, verwenden Sie den Befehl von der erweiterten Berechtigungsebene aus.

> Bevor Sie die Konfiguration der SSL-Schnittstelle ändern, stellen Sie sicher, dass der Client die Chiffren DHE und ECDHE unterstützt, wenn eine Verbindung zu ONTAP hergestellt wird, um die Verbindung mit ONTAP aufrechtzuerhalten.

Beispiel

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

Bestätigen Sie `y` für jede Eingabeaufforderung. Weitere Informationen zu PFS finden Sie in diesem "NetApp Blog".

Verwandte Informationen

"Federal Information Processing Standard (FIPS) Publication 140"

Erstellen Sie ein CA-signiertes digitales Zertifikat

Für viele Unternehmen ist das selbstsignierte digitale Zertifikat für den ONTAP-Webzugriff nicht mit den InfoSec-Richtlinien kompatibel. Auf Produktionssystemen ist es eine NetApp Best Practice, ein CA-signiertes digitales Zertifikat zu installieren, das zur Authentifizierung des Clusters oder der SVM als SSL-Server verwendet wird.

Sie können den Befehl verwenden `security certificate generate-csr` , um eine Zertifikatsignierungsanforderung (CSR) zu generieren, und den `security certificate install` Befehl, um das Zertifikat zu installieren, das Sie von der Zertifizierungsstelle zurückerhalten.

Schritte

1. Gehen Sie wie folgt vor, um ein digitales Zertifikat zu erstellen, das von der Zertifizierungsstelle des Unternehmens signiert wurde:
   a. CSR erstellen.
   b. Befolgen Sie die Anweisungen Ihres Unternehmens, um ein digitales Zertifikat über die CSR von der Zertifizierungsstelle Ihres Unternehmens anzufordern. Gehen Sie beispielsweise über die Microsoft Active Directory-Zertifikatdienste-Webschnittstelle zu `<CA_server_name>/certsrv` und fordern Sie ein Zertifikat an.
   c. Installieren Sie das digitale Zertifikat in ONTAP.

Online-Protokoll für den Zertifikatsstatus

Mit dem Online Certificate Status Protocol (OCSP) können ONTAP-Applikationen, die TLS-Kommunikation wie LDAP oder TLS verwenden, einen digitalen Zertifikatsstatus erhalten, wenn OCSP aktiviert ist. Die Applikation erhält eine signierte Antwort, die angibt, ob das angeforderte Zertifikat in Ordnung, annulliert oder unbekannt ist.

OCSP ermöglicht die Ermittlung des aktuellen Status eines digitalen Zertifikats, ohne dass Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) erforderlich sind.

Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert. Es kann mit dem Befehl eingeschaltet werden `security config ocsp enable -app name`, wo der App-Name sein kann `autosupport`, , `audit_log` `fabricpool` `ems`, , , `kmip`, `ldap_ad` `ldap_nis_namemap`, oder `all`. Für den Befehl ist eine erweiterte Berechtigungsebene erforderlich.

SSHv2-Management

Mit dem `security ssh modify` Befehl werden die vorhandenen Konfigurationen der SSH-Schlüsselaustauschalgorithmen, Chiffren oder MAC-Algorithmen für das Cluster oder eine SVM durch die von Ihnen angegebenen Konfigurationseinstellungen ersetzt.

NetApp empfiehlt Folgendes:

- Verwenden Sie Passwörter für Benutzersitzungen.
- Verwenden Sie einen öffentlichen Schlüssel für den Maschinenzugriff.

Unterstützte Chiffren und Schlüsselaustausch

Verschlüsselung	Schlüsselaustausch
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-gcm	-
aes256-gcm	-
3des-cbc	-

Unterstützte symmetrische AES- und 3DES-Verschlüsselungen

ONTAP unterstützt auch die folgenden Arten von symmetrischen AES- und 3DES-Verschlüsselungen (auch als Chiffren bezeichnet):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- 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-etm
- hmac-md5-96-etm
- hmac-Ripemd160-etm
- umac-64-etm
- umac-128-etm

Die SSH-Verwaltungskonfiguration gilt für ONTAP und die Plattform BMC.

NetApp AutoSupport

Mit der AutoSupport Funktion von ONTAP überwachen Sie proaktiv den Zustand Ihres Systems und senden automatisch Nachrichten und Details an den technischen Support von NetApp, das interne Support-Team Ihres Unternehmens oder einen Support-Partner. Standardmäßig sind AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn das Storage-System zum ersten Mal konfiguriert wird. Darüber hinaus sendet AutoSupport 24 Stunden nach Aktivierung Nachrichten an den technischen Support von NetApp. Dieser Zeitraum von 24 Stunden ist konfigurierbar. Um die Kommunikation mit dem internen Support-Team eines Unternehmens nutzen zu können, muss die Konfiguration des Mail-Hosts abgeschlossen sein.

Das AutoSupport-Management (Konfiguration) kann nur vom Clusteradministrator durchgeführt werden. Der SVM-Administrator hat keinen Zugriff auf AutoSupport. Die AutoSupport-Funktion kann deaktiviert werden. NetApp empfiehlt jedoch die Aktivierung, da mit AutoSupport Probleme schneller identifiziert und gelöst werden können, sollte auf dem Storage-System ein Problem auftreten. Standardmäßig erfasst das System AutoSupport-Informationen und speichert diese lokal, selbst wenn Sie AutoSupport deaktivieren.

Weitere Details zu AutoSupport Meldungen, einschließlich der Inhalte in den verschiedenen Meldungen und wo verschiedene Meldungstypen gesendet werden, finden Sie in der "Digitaler Berater von NetApp" Dokumentation.

AutoSupport-Meldungen enthalten sensible Daten, wie z. B. die folgenden Elemente:

- Log-Dateien
- Kontextsensitive Daten zu spezifischen Subsystemen
- Konfigurations- und Statusdaten
- Performance-Daten

AutoSupport unterstützt HTTPS und SMTP für Transportprotokolle. Aufgrund der sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.

Zusätzlich sollten Sie den Befehl nutzen `system node autosupport modify` , um die Ziele von AutoSupport-Daten anzugeben (z. B. technischer Support von NetApp, interne Vorgänge eines Unternehmens oder Partner). Mit diesem Befehl können Sie auch angeben, welche spezifischen AutoSupport-Details gesendet werden sollen (z. B. Performance-Daten, Log-Dateien usw.).

Um AutoSupport vollständig zu deaktivieren, verwenden Sie den `system node autosupport modify -state disable` Befehl.

Network Time Protocol

Obwohl Sie mit ONTAP die Zeitzone, das Datum und die Uhrzeit auf dem Cluster manuell festlegen können, müssen Sie die NTP-Server (Network Time Protocol) konfigurieren, damit die Cluster-Zeit mit mindestens drei externen NTP-Servern synchronisiert wird.

Wenn die Cluster-Zeit nicht stimmt, können Probleme auftreten. ONTAP ermöglicht Ihnen zwar das manuelle Einstellen der Zeitzone, des Datums und der Uhrzeit auf dem Cluster, Sie müssen jedoch die NTP-Server (Network Time Protocol) konfigurieren, damit die Cluster-Zeit mit externen NTP-Servern synchronisiert wird.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung konfigurieren.

Mit dem Befehl können Sie maximal 10 externe NTP-Server verknüpfen `cluster time-service ntp server create` . Um Redundanz und Qualität des Zeitdienstes zu gewährleisten, sollten Sie mindestens drei externe NTP-Server mit dem Cluster verbinden.

Details zur Konfiguration von NTP in ONTAP finden Sie unter "Verwalten der Cluster-Zeit (nur Cluster-Administratoren)".

Lokale NAS-Dateisystemkonten (CIFS-Arbeitsgruppe)

Die Workgroup-Client-Authentifizierung bietet eine zusätzliche Sicherheitsebene für die ONTAP-Lösung, die mit der herkömmlichen Domänenauthentifizierung konsistent ist. Verwenden Sie den `vserver cifs session show` Befehl, um zahlreiche Details zu den Positionen anzuzeigen, einschließlich IP-Informationen, des Authentifizierungsmechanismus, der Protokollversion und des Authentifizierungstyps.

Ab ONTAP 9 können Sie einen CIFS-Server in einer Arbeitsgruppe mit CIFS-Clients konfigurieren, die sich mithilfe lokal definierter Benutzer und Gruppen beim Server authentifizieren. Die Workgroup-Client-Authentifizierung bietet eine zusätzliche Sicherheitsebene für die ONTAP-Lösung, die mit der herkömmlichen Domänenauthentifizierung konsistent ist. Verwenden Sie zum Konfigurieren des CIFS-Servers den `vserver cifs create` Befehl. Nachdem der CIFS-Server erstellt wurde, können Sie ihn einer CIFS-Domäne hinzufügen oder einer Arbeitsgruppe beitreten. Um einer Arbeitsgruppe beizutreten, verwenden Sie den `-workgroup` Parameter. Hier ist eine Beispielkonfiguration:

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

Ein CIFS-Server im Arbeitsgruppenmodus unterstützt nur die NTLM-Authentifizierung (Windows NT LAN Manager) und unterstützt keine Kerberos-Authentifizierung.

NetApp empfiehlt die Verwendung der NTLM-Authentifizierungsfunktion mit CIFS-Arbeitsgruppen, um die Sicherheit Ihres Unternehmens aufrechtzuerhalten. Zum Validieren der CIFS-Sicherheitslage empfiehlt NetApp, mithilfe des `vserver cifs session show` Befehls zahlreiche Details zum Thema Haltung anzuzeigen, einschließlich IP-Informationen, des Authentifizierungsmechanismus, der Protokollversion und des Authentifizierungstyps.

NAS-Filesystem-Auditing

NAS-Dateisysteme nehmen in der heutigen Bedrohungslandschaft einen größeren Platz ein, Audit-Funktionen sind für die Transparenz von entscheidender Bedeutung.

Sicherheit erfordert Validierung. ONTAP bietet erweiterte Auditing-Ereignisse und -details für die gesamte Lösung. Da NAS-Dateisysteme in der heutigen Bedrohungslandschaft eine immer größere Rolle spielen, sind Audit-Funktionen entscheidend, um Transparenz zu unterstützen. Aufgrund der verbesserten Audit-Fähigkeit in ONTAP sind CIFS-Audit-Details umfangreicher denn je. Wichtige Details, einschließlich der folgenden, werden mit den erstellten Ereignissen protokolliert:

- Datei-, Ordner- und Freigabezugriff

- Erstellte, bearbeitete oder gelöschte Dateien
- Erfolgreicher Lesezugriff auf die Datei
- Fehlgeschlagene Versuche, Dateien zu lesen oder zu schreiben
- Geänderte Ordnerrechte

Erstellen Sie eine Überwachungskonfiguration

Sie müssen CIFS-Überwachung aktivieren, um Auditing-Ereignisse zu generieren. Erstellen Sie mit dem `vserver audit create` Befehl eine Überwachungskonfiguration. Standardmäßig verwendet das Audit-Protokoll eine auf Größe basierende Rotationsmethode. Sie können eine zeitbasierte Rotationsoption verwenden, wenn sie im Feld Rotationsparameter angegeben ist. Weitere Konfigurationsdetails für die Protokollaudit-Rotation sind der Rotationszeitplan, die Rotationsgrenzen, die Rotationstage der Woche und die Rotationsgröße. Der folgende Text enthält eine Beispielkonfiguration, die eine Überwachungskonfiguration mit einer monatlichen, zeitbasierten Rotation darstellt, die für alle Wochentage um 12:30 Uhr geplant ist.

```
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-Audit-Ereignisse

CIFS-Audit-Ereignisse sind wie folgt:

- **Dateifreigabe**: Erzeugt ein Audit-Ereignis, wenn eine CIFS-Netzwerkfreigabe mit den zugehörigen Befehlen hinzugefügt, geändert oder gelöscht wird `vserver cifs share`.
- **Änderung der Überwachungsrichtlinie**: Erzeugt ein Audit-Ereignis, wenn die Überwachungsrichtlinie mit den zugehörigen Befehlen deaktiviert, aktiviert oder geändert wird `vserver audit`.
- **Benutzerkonto**: Erzeugt ein Audit-Ereignis, wenn ein lokaler CIFS- oder UNIX-Benutzer erstellt oder gelöscht wird; ein lokales Benutzerkonto aktiviert, deaktiviert oder geändert wird; oder ein Passwort zurückgesetzt oder geändert wird. Dieses Ereignis verwendet den `vserver cifs users-and-groups local-group` Befehl oder den entsprechenden `vserver services name-service unix-user` Befehl.
- **Sicherheitsgruppe**: Erzeugt ein Auditereignis, wenn eine lokale CIFS- oder UNIX-Sicherheitsgruppe mit dem Befehl oder dem entsprechenden Befehl erstellt oder gelöscht wird `vserver cifs users-and-groups local-group` `vserver services name-service unix-group`.
- **Änderung der Autorisierungsrichtlinie**: Erzeugt ein Auditereignis, wenn Rechte für einen CIFS-Benutzer oder eine CIFS-Gruppe mit dem Befehl gewährt oder aufgehoben werden `vserver cifs users-and-groups privilege`.

> Diese Funktion basiert auf der Systemaudit-Funktion, mit der ein Administrator aus Sicht eines Datenbenutzers überprüfen kann, was das System erlaubt und was es ausführt.

Auswirkungen von REST-APIs auf NAS-Auditing

ONTAP bietet Administratorkonten die Möglichkeit, über REST-APIs auf SMB/CIFS- oder NFS-Dateien zuzugreifen und diese zu bearbeiten. Obwohl REST-APIs nur von ONTAP Administratoren ausgeführt werden können, umgehen REST-API-Befehle das NAS-Revisionsprotokoll des Systems. Darüber hinaus können Dateiberechtigungen von ONTAP-Administratoren bei Verwendung von REST-APIs ignoriert werden. Die

Aktionen des Administrators mit REST-APIs für Dateien werden jedoch im Verlaufsprotokoll des Systembefehls erfasst.

REST-API-Rolle ohne Zugriff erstellen

Sie können verhindern, dass ONTAP-Administratoren REST-APIs für den Dateizugriff verwenden, indem Sie eine REST-API-Rolle erstellen, die über REST keinen Zugriff auf ONTAP Volumes hat. Führen Sie die folgenden Schritte aus, um diese Rolle bereitzustellen.

> Die REST-API /api/storage/volumes wird für mehr als nur den Dateizugriff verwendet. Sie wird vom System Manager und anderen grafischen Benutzeroberflächen zum Erstellen, Anzeigen und Ändern von Volumes verwendet.

Schritte

1. Erstellen einer neuen REST-Rolle, die keinen Zugriff auf Storage-Volumes hat, aber über alle anderen REST-API-Zugriff verfügt

```
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. Weisen Sie das Administratorkonto der neuen REST-API-Rolle zu, die Sie im vorherigen Schritt erstellt haben.

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

> Wenn Sie verhindern möchten, dass das integrierte ONTAP-Cluster-Administratorkonto REST-APIs für den Dateizugriff verwendet, müssen Sie zuerst "Erstellen Sie ein neues Administratorkonto, und deaktivieren oder löschen Sie das integrierte Konto".

Konfigurieren und aktivieren Sie das CIFS-SMB-Signing and Sealing

Sie können SMB-Signaturen konfigurieren und aktivieren, die die Sicherheit der Data-Fabric-Architektur schützen, indem dafür gesorgt wird, dass der Datenverkehr zwischen den Storage-Systemen und den Clients nicht durch Replay- oder man-in-the-Middle-Angriffe beeinträchtigt wird. SMB-Signaturen schützen durch Überprüfung, ob SMB-Nachrichten über gültige Signaturen verfügen.

Über diese Aufgabe

Ein gängiger Bedrohungsvektor für Filesysteme und Architekturen ist das SMB-Protokoll. Um diesen Vektor anzugehen, verwendet die ONTAP 9 Lösung das branchenübliche SMB-Signing and Sealing. SMB-Signaturen schützen die Sicherheit der Data-Fabric-Architektur, indem sichergestellt wird, dass der Datenverkehr zwischen den Storage-Systemen und den Clients nicht durch Replay- oder man-in-the-Middle-Angriffe beeinträchtigt wird. Dazu wird sichergestellt, dass SMB-Nachrichten über gültige Signaturen verfügen.

Obwohl die SMB-Signatur im Hinblick auf die Performance standardmäßig deaktiviert ist, empfiehlt NetApp dringend, sie zu aktivieren. Zudem unterstützt die ONTAP Lösung SMB-Verschlüsselung, die auch als Sealing bezeichnet wird. Dieser Ansatz ermöglicht einen sicheren Share-by-Share-Transport der Daten. Die SMB-Verschlüsselung ist standardmäßig deaktiviert. NetApp empfiehlt jedoch, die SMB-Verschlüsselung zu aktivieren.

LDAP-Signing und Sealing werden jetzt in SMB 2.0 und höher unterstützt. Das Signieren (Schutz vor Manipulation) und Sealing (Verschlüsselung) ermöglichen eine sichere Kommunikation zwischen SVMs und Active Directory-Servern. Beschleunigte AES New Instructions (Intel AES NI)-Verschlüsselung wird jetzt in SMB 3.0 und höher unterstützt. Intel AES NI verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien.

Schritte

1. Verwenden Sie zum Konfigurieren und Aktivieren von SMB-Signaturen den `vserver cifs security modify` Befehl und überprüfen Sie, ob der `-is-signing-required` Parameter auf festgelegt ist `true`. Siehe folgendes Beispiel:

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

2. Verwenden Sie zum Konfigurieren und Aktivieren von SMB-Sealing und -Verschlüsselung den `vserver cifs security modify` Befehl und überprüfen Sie, ob der `-is-smb-encryption-required` Parameter auf festgelegt ist `true`. Siehe folgendes Beispiel:

```
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-Sicherung

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Die Exportregeln richten sich nach Client-Zugriffsanforderungen für ein Volume anhand bestimmter Parameter, die Sie konfigurieren, um zu bestimmen, wie mit den Clientzugriffsanfragen umzugehen ist. Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden.

Zugriffssteuerung ist ein zentraler Bestandteil des Sicherheitsstatus. Daher verwendet ONTAP die Funktion für die Exportrichtlinie, um den Zugriff auf NFS-Volumes auf Clients zu beschränken, die mit bestimmten Parametern übereinstimmen. Exportrichtlinien enthalten mindestens eine Exportregel, die jede Clientzugriffsanforderung verarbeitet. Jedem Volume ist eine Exportrichtlinie zugeordnet, um den Client-Zugriff

auf das Volume zu konfigurieren. Das Ergebnis dieses Prozesses legt fest, ob dem Client (mit einer Meldung, dass ihm die Berechtigung verweigert wird) der Zugriff auf das Volume gewährt oder verweigert wird. Dieser Prozess bestimmt auch, welche Zugriffsebene auf das Volume bereitgestellt wird.

> Für den Zugriff auf Daten durch Clients muss auf einer SVM eine Exportrichtlinie mit Exportrichtlinien vorhanden sein. Eine SVM kann mehrere Exportrichtlinien enthalten.

Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Wenn eine Regel mit einem Client übereinstimmt, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Exportregeln bestimmen Clientzugriffsberechtigungen, indem die folgenden Kriterien angewendet werden:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet (z. B. NFSv4 oder SMB)
- Eine Client-Kennung (z. B. Hostname oder IP-Adresse)
- Der vom Client zur Authentifizierung verwendete Sicherheitstyp (z. B. Kerberos v5, NTLM oder AUTH_SYS)

Wenn in einer Regel mehrere Kriterien angegeben sind und der Client einem oder mehreren Kriterien nicht entspricht, gilt die Regel nicht.

Eine Beispielrichtlinie für den Export enthält eine Exportregel mit den folgenden Parametern:

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

Der Sicherheitstyp legt fest, welche Zugriffsebene ein Client erhält. Die drei Zugriffsebenen sind schreibgeschützt, Lesen/Schreiben und Superuser (für Clients mit der Benutzer-ID `0`). Da die vom Sicherheitstyp festgelegte Zugriffsebene in dieser Reihenfolge bewertet wird, müssen Sie die folgenden Regeln beachten:

Regeln für Parameter auf Zugriffsebene in Exportregeln

Für einen Client, um die folgenden Zugriffsebenen zu erhalten	Diese Zugriffsparameter müssen mit dem Sicherheitstyp des Clients übereinstimmen
Normaler Benutzer schreibgeschützt	Schreibgeschützt (`-rorule`)
Normaler Benutzer Lese-/Schreibzugriff	Read-only(`-rorule`) und read-write (`-rwrule`)
Schreibgeschützt für Superuser	Read-only (`-rorule`) und `-superuser`
Superuser lesen und schreiben	Read-only (`-rorule`) und read-write (`-rwrule`) und `-superuser`

Die folgenden Sicherheitstypen sind für jeden der folgenden drei Zugriffsparameter gültig:

- Alle
- Keine
- Nie

Diese Sicherheitstypen sind für die Verwendung mit dem `-superuser` Parameter:

- krb5
- ntlm
- Sys

Regeln für Zugriffsparameter-Ergebnisse

Wenn der Sicherheitstyp des Clients …	Dann …
Stimmt mit einem Sicherheitstyp überein, der im Zugriffsparameter angegeben wurde.	Der Client erhält Zugriff auf diese Ebene mit seiner eigenen Benutzer-ID.
Stimmt nicht mit einem angegebenen Sicherheitstyp überein, aber der Zugriffsparameter enthält die Option `none`.	Der Client erhält Zugriff auf diese Ebene und erhält den anonymen Benutzer mit der vom Parameter angegebenen Benutzer-ID `-anon` .
Stimmt nicht mit einem angegebenen Sicherheitstyp überein, und der Zugriffsparameter enthält nicht die Option `none`.	Der Client erhält keinen Zugriff auf diese Ebene. Diese Einschränkung gilt nicht für den `-superuser` Parameter, da dieser Parameter auch dann keine enthält, wenn er nicht angegeben ist.

Kerberos 5 und Krb5p

Ab ONTAP 9 wird die Kerberos 5-Authentifizierung mit dem Datenschutzdienst (krb5p) unterstützt. Der krbp5-Authentifizierungsmodus ist sicher und schützt mithilfe von Prüfsummen vor Datenmanipulation und -Ausspähung, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln. Die ONTAP-Lösung unterstützt 128-Bit- und 256-Bit-AES-Verschlüsselung für Kerberos. Der Datenschutzservice umfasst die Überprüfung der Integrität der empfangenen Daten, die Authentifizierung von Benutzern und die Verschlüsselung von Daten vor der Übertragung.

Die krb5p-Option ist am häufigsten in der Exportrichtlinie vorhanden, wo sie als Verschlüsselungsoption festgelegt ist. Die krb5p-Authentifizierungsmethode kann als Authentifizierungsparameter verwendet werden, wie im folgenden Beispiel gezeigt:

```
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
```

Aktivieren Sie Lightweight Directory Access Protocol Signing and Sealing

Das Signieren und Versiegeln wird unterstützt, um die Sitzungssicherheit bei Anfragen an einen LDAP-Server zu ermöglichen. Dieser Ansatz bietet eine Alternative zur LDAP-über-

TLS-Sitzungssicherheit.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Sitzungssicherheitseinstellungen auf einer SVM entsprechen denen auf dem LDAP-Server. Standardmäßig sind LDAP-Signing und Sealing deaktiviert.

Schritte

1. Um diese Funktion zu aktivieren, führen Sie den `vserver cifs security modify` Befehl mit dem `session-security-for-ad-ldap` Parameter aus.

   Optionen für LDAP-Sicherheitsfunktionen:

   - **None**: Standard, keine Signatur oder Versiegelung
   - **Zeichen**: LDAP-Verkehr signieren
   - **Seal**: LDAP-Verkehr signieren und verschlüsseln

   > Die Parameter für Zeichen und Siegel sind kumulativ, d. h. wenn die Option Zeichen verwendet wird, ist das Ergebnis LDAP mit Signing. Wenn jedoch die Option „Siegel“ verwendet wird, ist das Ergebnis sowohl Zeichen als auch Siegel. Wenn für diesen Befehl kein Parameter angegeben wird, ist der Standardwert „none“.

   Im Folgenden finden Sie eine Beispielkonfiguration:

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

NetApp FPolicy erstellen und verwenden

Sie können eine FPolicy erstellen und verwenden, eine Infrastrukturkomponente der ONTAP-Lösung, mit der Partnerapplikationen Dateizugriffsberechtigungen überwachen und festlegen können. Eine der leistungsstärksten Anwendungen ist Storage Workload Security, eine NetApp-SaaS-Anwendung, die über Hybrid-Cloud-Umgebungen hinweg einen zentralen Überblick und eine zentrale Kontrolle über den Zugriff auf alle Unternehmensdaten bietet und so die Einhaltung von Sicherheits- und Compliance-Zielen sicherstellt.

Die Zugriffssteuerung ist ein zentrales Sicherheitskonzept. Sichtbarkeit und die Fähigkeit, auf Dateizugriff und Dateivorgänge zu reagieren, sind wichtig, um die Sicherheit aufrechtzuerhalten. Um Sichtbarkeit und Zugriffssteuerung für Dateien zu ermöglichen, verwendet die ONTAP Lösung die Funktion NetApp FPolicy.

Dateirichtlinien können basierend auf dem Dateityp festgelegt werden. FPolicy legt fest, wie das Storage-System Anfragen von einzelnen Client-Systemen für Vorgänge wie Erstellen, Öffnen, Umbenennen und Löschen verarbeitet. Mit ONTAP 9 wurde das FPolicy Dateizugriffs-Benachrichtigungs-Framework durch Filterkontrollen und Ausfallsicherheit bei kurzen Netzwerkausfällen verbessert.

Schritte

1. Um die FPolicy Funktion nutzen zu können, müssen Sie zunächst die FPolicy Richtlinie mit dem Befehl

erstellen `vserver fpolicy policy create`.

> Verwenden Sie außerdem den `-events` Parameter, wenn Sie FPolicy für die Sichtbarkeit und das Sammeln von Ereignissen verwenden. Die zusätzliche Granularität durch ONTAP ermöglicht Filterung und Zugriff bis hinunter auf die Kontrollebene für Benutzernamen. Um Berechtigungen und Zugriff mit Benutzernamen zu steuern, geben Sie den Parameter an `-privilege-user-name`.

Der folgende Text zeigt ein Beispiel für die FPolicy-Erstellung:

```
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. Nachdem Sie die FPolicy-Richtlinie erstellt haben, müssen Sie sie mit dem Befehl aktivieren `vserver fpolicy enable`. Mit diesem Befehl wird auch die Priorität oder Sequenz des FPolicy-Eintrags festgelegt.

> Die FPolicy-Sequenz ist wichtig, da, wenn mehrere Richtlinien dasselbe Dateizugriffsereignis abonniert haben, die Sequenz die Reihenfolge vorgibt, in der der Zugriff gewährt oder verweigert wird.

Der folgende Text enthält eine Beispielkonfiguration zum Aktivieren der FPolicy-Richtlinie und zum Validieren der Konfiguration mit dem `vserver fpolicy show` Befehl:

```
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.
```

Verbesserungen von FPolicy

ONTAP 9 umfasst die in den folgenden Abschnitten beschriebenen Verbesserungen von FPolicy.

Filterkontrollen

Für und zum Entfernen von Benachrichtigungen zu Verzeichnisaktivitäten stehen neue Filter zur Verfügung `SetAttr`.

Asynchrone Ausfallsicherheit

Wenn bei einem FPolicy-Server im asynchronen Modus ein Netzwerkausfall auftritt, werden FPolicy Benachrichtigungen, die während des Ausfalls generiert wurden, auf dem Storage-Node gespeichert. Wenn der FPolicy-Server wieder online geschaltet wird, wird er über die gespeicherten Benachrichtigungen benachrichtigt und kann sie vom Speicher-Node abrufen. Die Länge der Speicherung der Benachrichtigungen während eines Ausfalls kann so bis zu 10 Minuten betragen.

Sicherheitsmerkmale von LIF-Rollen in ONTAP

Eine LIF ist eine IP-Adresse oder ein WWPN (Worldwide Port Name) mit zugehörigen Merkmalen, beispielsweise eine Rolle, einen Home Port, einen Home Node, eine Liste der Failover-Ports sowie eine Firewallrichtlinie. Sie können LIFs an Ports konfigurieren, über die das Cluster Kommunikation über das Netzwerk sendet und empfängt. Es ist wichtig, die Sicherheitsmerkmale der einzelnen LIF-Rollen zu kennen.

LIF-Rollen

Dies sind die folgenden LIF-Rollen:

- **Data LIF**: Eine mit einer SVM verknüpfte LIF, die zur Kommunikation mit Clients verwendet wird.
- **Cluster LIF**: Eine LIF zur Durchführung von Intracluster-Datenverkehr zwischen Knoten in einem Cluster.
- **Node Management LIF**: Eine LIF, die eine dedizierte IP-Adresse zur Verwaltung eines bestimmten Knotens in einem Cluster bereitstellt.
- **Cluster-Management-LIF**: Eine LIF, die eine einzige Managementoberfläche für den gesamten Cluster bereitstellt.
- **Intercluster LIF**: Eine LIF, die für Cluster-übergreifende Kommunikation, Backup und Replikation verwendet wird.

Sicherheitsmerkmale der einzelnen LIF-Rolle

	Data LIF	Cluster-LIF	Node Management-LIF	Cluster-Management-LIF	Intercluster LIF
Privates IP-Subnetz erforderlich?	Nein	Ja.	Nein	Nein	Nein
Erfordert ein sicheres Netzwerk?	Nein	Ja.	Nein	Nein	Ja.
Standardmäßige Firewallrichtlinie	Sehr restriktiv	Vollständig geöffnet	Mittel	Mittel	Sehr restriktiv
Ist die Firewall anpassbar?	Ja.	Nein	Ja.	Ja.	Ja.

- Da die Cluster-LIF vollständig geöffnet ist und keine konfigurierbare Firewall-Richtlinie enthält, muss sie sich in einem privaten IP-Subnetz in einem sicheren, isolierten Netzwerk befinden.
- LIF-Rollen sollten niemals über das Internet zugänglich sein.

Weitere Informationen zur Sicherung von LIFs finden Sie unter "Konfigurieren Sie Firewallrichtlinien für

LIFs"Die Auf dieser Seite finden Sie außerdem Details zu den LIF-Servicerichtlinien, beginnend mit ONTAP 9.10.1.

Weitere Informationen zum Erstellen einer neuen Servicerichtlinie finden Sie unter `network interface service-policy create` Befehl im "Befehlsreferenz."

Protokoll- und Portsicherheit

Neben der Durchführung von integrierten Sicherheitsvorgängen und -Funktionen muss die Härtung einer Lösung auch Off-Box-Sicherheitsmechanismen beinhalten. Die Nutzung zusätzlicher Infrastrukturgeräte wie Firewalls, Intrusion Prevention-Systeme (IPSs) und andere Sicherheitsgeräte zum Filtern und Einschränken des Zugriffs auf ONTAP ist eine effiziente Möglichkeit, ein strenges Sicherheitsniveau zu definieren und aufrechtzuerhalten. Diese Informationen sind eine wichtige Komponente zum Filtern und Einschränken des Zugriffs auf die Umgebung und ihre Ressourcen.

Häufig verwendete Protokolle und Ports

Service	Port/Protokoll	Beschreibung
`SSH`	22/TCP	SSH-Anmeldung
`telnet`	23/TCP	Remote-Anmeldung
`Domain`	53/TCP	Domain Name Server
`HTTP`	80/TCP 80/UDP	HTTP
`rpcbind`	111/TCP 111/UDP	Remote-Prozeduraufruf
`NTP`	123/UDP	Network Time Protocol
`msrpc`	135/TCP	Microsoft Remote Procedure Call
`Netbios-name`	137/TCP 137/UDP	NetBIOS-Namensdienst
`netbios-ssn`	139/TCP	Sitzung für den NETBIOS-Dienst
`SNMP`	161/UDP	SNMP
`HTTPS`	443/TCP	Sicherer Link:http
`microsoft-ds`	445/TCP	Microsoft Verzeichnisdienste
`IPsec`	500/UDP	Sicherheit Des Internetprotokolls
`mount`	635/UDP	NFS-Mount
`named`	953/UDP	Name Daemon
`NFS`	2049/UDP 2049/TCP	NFS-Server-Daemon
`nrv`	2050/TCP	NetApp Remote Volume-Protokoll

Service	Port/Protokoll	Beschreibung
iscsi	3260/TCP	ISCSI-Zielport
Lockd	4045/TCP 4045/UDP	NFS-Sperr-Daemon
NFS	4046/TCP	NFS-Mountd-Protokoll
acp-proto	4046/UDP	Buchhaltungsprotokoll
rquotad	4049/UDP	NFS rquotad-Protokoll
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Sicherheit Des Internetprotokolls
acp	5125/UDP 5133/UDP 5144/TCP	Alternativer Kontrollport für Festplatte
Mdns	5353/UDP	Multicast-DNS
HTTPS	5986/UDP	HTTPS-Port: Hören binäres Protokoll
TELNET	8023/TCP	Node-Scope-Telnet
HTTPS	8443/TCP	7MTT GUI-Tool über Link:HTTPS
RSH	8514/TCP	Knoten-Umfang RSH
KMIP	9877/TCP	KMIP-Client-Port (nur interner lokaler Host)
ndmp	10000/TCP	NDMP
cifs Witness-Port	40001/TCP	CIFS-Witness-Port
TLS	50000/TCP	Sicherheit der Datenübertragungsschicht
Iscsi	65200/TCP	ISCSI-Port
SSH	65502/TCP	Sichere Shell
vsun	65503/TCP	Vsun

Interne NetApp-Ports

Port/Protokoll	Beschreibung
900	NetApp-Cluster-RPC
902	NetApp-Cluster-RPC
904	NetApp-Cluster-RPC
905	NetApp-Cluster-RPC
910	NetApp-Cluster-RPC
911	NetApp-Cluster-RPC
913	NetApp-Cluster-RPC
914	NetApp-Cluster-RPC

Port/Protokoll	Beschreibung
915	NetApp-Cluster-RPC
918	NetApp-Cluster-RPC
920	NetApp-Cluster-RPC
921	NetApp-Cluster-RPC
924	NetApp-Cluster-RPC
925	NetApp-Cluster-RPC
927	NetApp-Cluster-RPC
928	NetApp-Cluster-RPC
929	NetApp-Cluster-RPC
931	NetApp-Cluster-RPC
932	NetApp-Cluster-RPC
933	NetApp-Cluster-RPC
934	NetApp-Cluster-RPC
935	NetApp-Cluster-RPC
936	NetApp-Cluster-RPC
937	NetApp-Cluster-RPC
939	NetApp-Cluster-RPC
940	NetApp-Cluster-RPC
951	NetApp-Cluster-RPC
954	NetApp-Cluster-RPC
955	NetApp-Cluster-RPC
956	NetApp-Cluster-RPC
958	NetApp-Cluster-RPC
961	NetApp-Cluster-RPC
963	NetApp-Cluster-RPC
964	NetApp-Cluster-RPC
966	NetApp-Cluster-RPC
967	NetApp-Cluster-RPC
7810	NetApp-Cluster-RPC
7811	NetApp-Cluster-RPC
7812	NetApp-Cluster-RPC
7813	NetApp-Cluster-RPC
7814	NetApp-Cluster-RPC

Port/Protokoll	Beschreibung
7815	NetApp-Cluster-RPC
7816	NetApp-Cluster-RPC
7817	NetApp-Cluster-RPC
7818	NetApp-Cluster-RPC
7819	NetApp-Cluster-RPC
7820	NetApp-Cluster-RPC
7821	NetApp-Cluster-RPC
7822	NetApp-Cluster-RPC
7823	NetApp-Cluster-RPC
7824	NetApp-Cluster-RPC

Technische Berichte zu ONTAP NAS

NetApp NAS-Lösungen vereinfachen die Datenverwaltung und helfen Ihnen, mit dem Wachstum Schritt zu halten und gleichzeitig die Kosten zu optimieren.

ONTAP S3

"TR-4814: S3 in ONTAP Best Practices" Lernen Sie empfohlene Vorgehensweisen für die Verwendung des Amazon Simple Storage Service (S3) mit ONTAP Software kennen. Darüber hinaus erhalten Sie Funktionen und Konfigurationen für die Verwendung von ONTAP als Objektspeicher mit nativen S3-Applikationen oder als Tiering-Ziel für FabricPool.

ONTAP SMB Technical Reports

NetApp NAS-Lösungen vereinfachen die Datenverwaltung und helfen Ihnen, mit dem Wachstum Schritt zu halten und gleichzeitig die Kosten zu optimieren.

SMB

"TR-4740: SMB 3.0 Multichannel"
Microsoft hat Multichannel im SMB 3.0-Protokoll eingeführt, um das SMB3-Protokoll zu verbessern, indem es die Leistungs- und Zuverlässigkeitseinschränkungen von SMB1 und SMB2 berücksichtigt. Erfahren Sie mehr über die Multichannel-Funktion in ONTAP, einschließlich seiner Funktionen, empfohlenen Vorgehensweisen und Ergebnisse von Leistungstests.

Multi-Protokoll

"TR-4887: Übersicht über Multiprotokoll-NAS in ONTAP und Best Practices"
Erfahren Sie, wie der Multiprotokoll-NAS-Zugriff in ONTAP funktioniert und welche empfohlenen Praktiken für Multi-Protokoll-Umgebungen kommen.

Speichersysteme

AFX

NetApp AFX-Übersicht: Erfahren Sie mehr über NetApp AFX

NetApp AFX ist nach wie vor ONTAP — es ist einfach eine andere Möglichkeit, die Vorteile von ONTAP zu nutzen. NetApp AFX liefert eine disaggregierte Architektur für NAS- und Objekt-Workloads und stellt gleichzeitig die funktionsreiche ONTAP-Software bereit, die Sie kennen und schätzen.

Eine Evolution der Innovation: NetApp ONTAP

NetApp ONTAP wurde 1992 als neue Methode zur Bereitstellung von NFS-Workloads für mehrere Clients entwickelt und revolutionierte dabei Leistung, Datenresilienz, zeitpunktgenaue Kopien und mehr. Ursprünglich unterstützte es nur NFSv2, aber mit der steigenden Nachfrage nach neueren NFS-Versionen, anderen Datenprotokollen und mehr Funktionen zum Datenschutz musste NetApp ONTAP sich weiterentwickeln.

Nachfolgend eine verkürzte Zeitleiste einiger der wichtigsten ONTAP-Entwicklungen, die in den letzten 30+ Jahren stattgefunden haben.

Die Entwicklung von NetApp ONTAP

Jahrzehnt	Features
1990s	NFSv2, NFSv3, CIFS, Snapshots, WAFL Dateisystem, AutoSupport, SnapMirror
2000s	SnapVault, SnapLock, NFSv4, Blockprotokolle, FlexVols, FlexClone, GX/Scale-out, Deduplizierung, Dateiklone
2010s	Clustered ONTAP, Inline-Speichereffizienz, NFSv4.1/pNFS, NVMe, RAID-TEC, FlexGroup Volumes, Volume-Verschlüsselung, 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, Autonomer Ransomware-Schutz, SnapMirror in und out of ANF und GCNV, Amazon FSxN, ASAr2, NetApp AFX – Sie sind hier

NetApp ONTAP-Persönlichkeiten

Jahrelang lief ONTAP als einheitliche Plattform, die Datei-, Block- und Objektverarbeitung in einem einzigen System vereinte. Dadurch positionierte sich ONTAP als das Schweizer Taschenmesser des Rechenzentrums – eine Plattform, die alles tun konnte, was Sie von ihr verlangten.

Da sich Anwendungen weiterentwickelten und sich die Anforderungen an Rechenzentren durch eine Reihe von Veränderungen in der IT-Branche wandelten, stieg die Nachfrage nach Plattformen mit spezifischen Funktionen. Daher gibt es heute verschiedene Möglichkeiten, ONTAP zu nutzen.

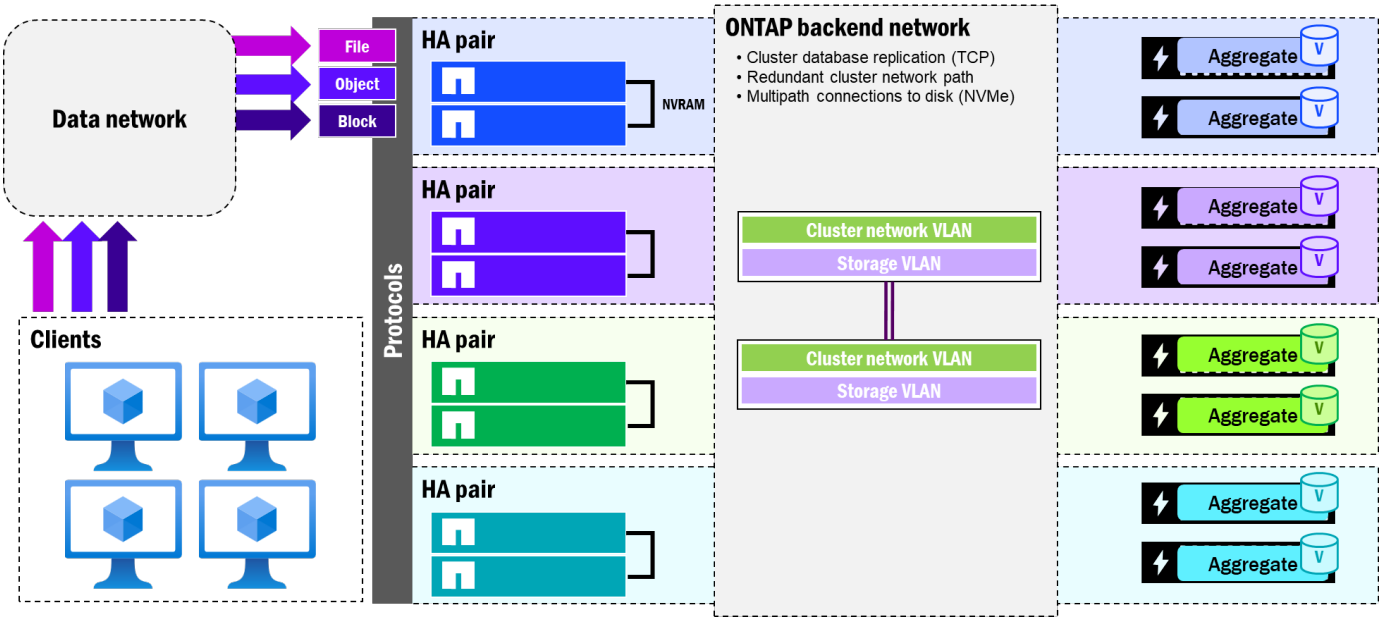
NetApp ONTAP-Persönlichkeiten

ONTAP Personality	Beschreibung
Einheitliches ONTAP	Das gleiche ONTAP, das Sie schon immer kannten, wird weiterhin aktiv weiterentwickelt und verbessert.
Alle SAN-Arrays	ONTAP unterstützt ausschließlich iSCSI, FCP und NVMe über FC/TCP und bietet Aktiv/Aktiv-Controller-Funktionalität sowie disaggregierte Konzepte in ASAr2.
Cloud-basiertes ONTAP	ONTAP, das in der Cloud läuft; entweder auf Bare-Metal-Systemen in einem Cloud-Rechenzentrum oder auf virtualisierten ONTAP Instanzen.
Disaggregiertes ONTAP/AFX	ONTAP nutzt eine disaggregierte Architektur für leistungsstarke NAS- und Objekt-Workloads.

Überblick über die einheitliche ONTAP-Architektur

Das folgende Diagramm zeigt die allgemeine Architektur von unified ONTAP, darunter wird beschrieben, wie alles zusammenpasst.

Allgemeine ONTAP Architektur



Einige wichtige Aspekte der ONTAP Architektur:

- Unterstützung für Dateien, Objekte und Blöcke
- Die Protokolle werden über ein Frontend-Client-Datennetzwerk bereitgestellt.
- Mehrere unabhängige Knoten können zu einem Cluster zusammengefasst werden
- Jeder Knoten kann unabhängige Floating-IP-Adressen für Daten- und Verwaltungsanwendungen bereitstellen
- Cluster-Knoten verbinden sich über ein von NetApp bereitgestelltes Backend-Switch über ein Cluster-VLAN.

- Die Knoten werden als HA-Paare dargestellt, um Ausfallsicherheit im Falle von Hardware- oder Stromausfällen zu gewährleisten.
- HA-Paare verfügen über direkt verbundene NVRAM-Karten, die replizieren, um Schreibvorgänge zu schützen
- Jedem Knoten ist mindestens ein Aggregat zugewiesen und er besitzt eine Teilmenge der Gesamtzahl der Festplatten
- Bei einem Failover werden die Festplatten eines Knotens dem HA-Partner (und nur dem HA-Partner) neu zugewiesen.
- Festplattengehäuse werden üblicherweise über Multipath-Verkabelung direkt mit den Knoten verbunden, aber höherwertige Systeme führen das Konzept von Speichernetzwerken auf demselben Backend-Cluster-Switch ein.
- Volumes (FlexVols und FlexGroup volumes) bieten die Einstiegspunkte zum Speicher für den Datenzugriff

Was ist NetApp AFX?

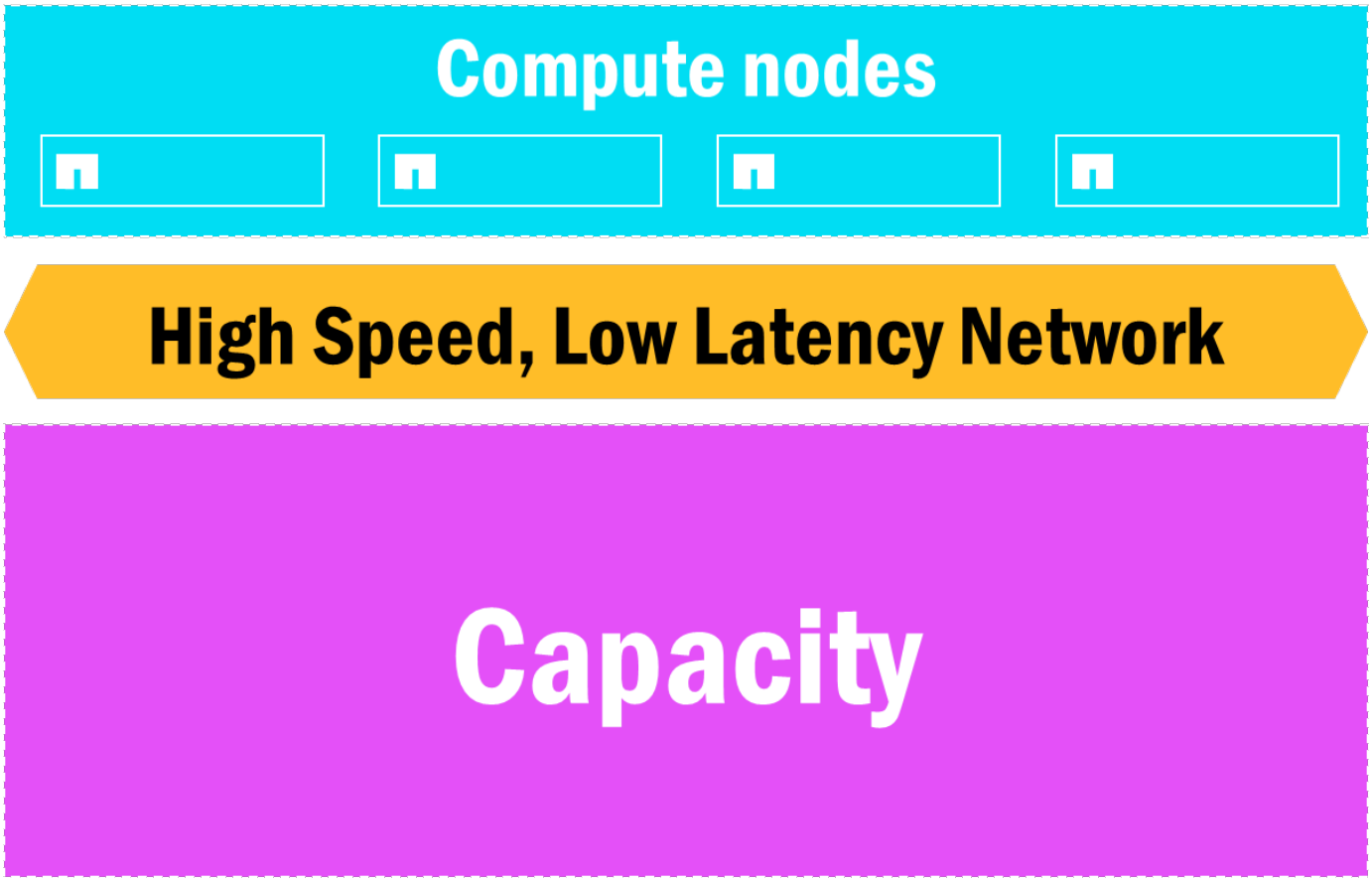
Eines sollte man dabei beachten: NetApp AFX ist immer noch ONTAP.

Es handelt sich lediglich um eine andere Methode, die Vorteile von ONTAP zu nutzen. Das gleiche Image, das Sie für Ihre Unified ONTAP oder All SAN Array Systeme installieren würden, ist das gleiche Image, das mit NetApp AFX verwendet wird. Die Codebasis ist identisch, aber die Art, wie die Systeme starten, bestimmt, welcher Codepfad ausgeführt wird, wie der Backend-Speicher präsentiert wird und welche Funktionen und Protokolle unterstützt werden.

NetApp AFX bietet eine disaggregierte Architektur für NAS- und Objekt-Workloads und gleichzeitig die funktionsreiche ONTAP-Software, die Sie kennen und schätzen. Disaggregiertes ONTAP bezeichnet eine Speicherarchitektur, bei der jeder NetApp Controller-Knoten dank redundanter Netzwerk-Switches und eines schnellen Netzwerks mit geringer Latenz dieselbe Kapazität sieht. Dieser Ansatz ermöglicht es, dass Controller-Knoten und Speicherkapazität unabhängig voneinander skaliert werden können, um die Anforderungen verschiedener Hochleistungs-Workloads besser zu erfüllen. Anders ausgedrückt: Wenn Sie zusätzliche Leistung benötigen, fügen Sie einfach Controller-Knoten hinzu. Wenn Sie zusätzliche Kapazität benötigen, fügen Sie Shelf-Gehäuse hinzu. Dies gibt Speicheradministratoren die Flexibilität, ihren Endbenutzern eine kostengünstigere Speicherlösung bereitzustellen.

Da kein Controller-Knoten eigenständig Festplatten besitzt, gibt es auch keine physischen Aggregate mit eigenen Kapazitäts- und Leistungsbeschränkungen. Stattdessen wird die Kapazität als gemeinsames Modell dargestellt, mit dem alle Knoten interagieren können und das ONTAP automatisch verwalten kann.

Disaggregiertes ONTAP



Schlüsselbegriffe und Konzepte

Nachfolgend finden Sie Begriffe, die sich direkt auf AFX beziehen. Für ONTAP-spezifische Terminologie siehe die Produktdokumentation.

"ONTAP Produktdokumentation".

Disaggregiertes ONTAP

Bezeichnet die neue Architektur, die von ONTAP unterstützt wird und die Möglichkeit bietet, Rechenleistung und Kapazität unabhängig voneinander zu skalieren. Der Begriff „Disaggregated ONTAP“ ist keine Produktbezeichnung, sondern dient der Unterscheidung zwischen Unified ONTAP und NetApp AFX-Architekturen.

NetApp AFX

NetApp AFX ist die offizielle Produktbezeichnung für die disaggregierte ONTAP Architektur und wurde auf NetApp Insight 2025 angekündigt.

Rechenknoten

Ein Compute-Knoten in NetApp AFX bezeichnet den Storage-Controller-Knoten (und wird in der Dokumentation oft synonym verwendet). Diese Knoten verfügen über keine integrierte Festplatte und sind vollständig modular aufgebaut, um die unabhängige Skalierbarkeit zu ermöglichen, die die disaggregierte ONTAP Architektur bietet.

Speicherverfügbarkeitszone

Eine Storage Availability Zone (SAZ) ist der zentrale Speicherpool in einem NetApp AFX-Cluster, in dem alle Festplatten von allen Knoten gemeinsam genutzt werden. Die SAZ ermöglicht Funktionen wie gemeinsam genutzte Kapazität, verbesserte Leistung, globale Deduplizierung und vieles mehr.

Was ist neu in NetApp AFX

Dieser Abschnitt enthält die neuesten Updates für NetApp AFX und wird mit jeder neuen Version aktualisiert. Schauen Sie regelmäßig hier vorbei, um neue Informationen zu erhalten, und lesen Sie auch die Versionshinweise.

Was ist neu in der neuesten Version von NetApp ONTAP für AFX?

Neueste Version:

ONTAP 9.19.1RC1 (Stand: Mai 2026)

Neue Funktionen in NetApp AFX:

- Globale Deduplizierung
- Dynamische Speichereffizienz
- Erweiterte Lesevorschau
- Unterstützung für 32 Knoten
- 32PB-Unterstützung
- 512 Bestandteilvolumina pro FlexGroup volume

Versionsverlauf

Version	Datum	Dokumentversionsverlauf
Version 1.0	Juni 2026	Erstveröffentlichung

Wie sich die NetApp AFX-Architektur von Unified ONTAP unterscheidet

NetApp AFX führt im Vergleich zu unified ONTAP bedeutende architektonische Unterschiede ein, wie Speicher präsentiert wird, wie Knoten mit Festplatten interagieren und wie Kapazität verwaltet wird.

Wir haben zuvor einen allgemeinen Überblick darüber gegeben, wie die Unified ONTAP-Architektur Datei-, Objekt- und Blockdatenspeicherung über direkt verbundene HA-Paare bereitstellt, die jeweils über eigene Festplatten verfügen und physische Kapazität über Festplattenaggregate bereitstellen. In diesem Abschnitt werden wir einige der wichtigsten Unterschiede zwischen Unified ONTAP und NetApp AFX-Architekturen detaillierter erläutern.

Wie man erkennt, ob auf einem System NetApp AFX ausgeführt wird

Die wichtigste Methode, um festzustellen, ob auf Ihrem System NetApp AFX ausgeführt wird, besteht darin, den folgenden Befehl auszuführen:

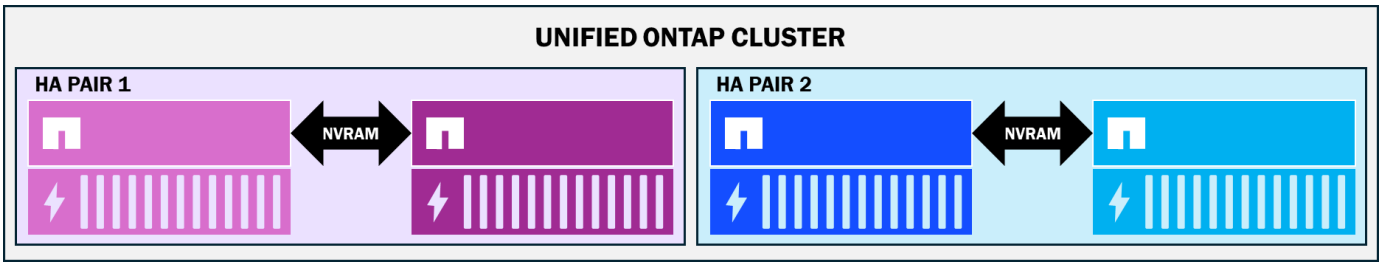
```
AFX::> node show -fields personality
node             personality
---------------- -----------
afx-01           AFX
afx-02           AFX
```

Ein weiterer Hinweis ist die neue Storage Availability Zone, die jedoch auch für NetApp All-SAN Arrays (ASA) verfügbar ist. Ihre Kapazität können Sie über diesen Befehl anzeigen.

```
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%
```

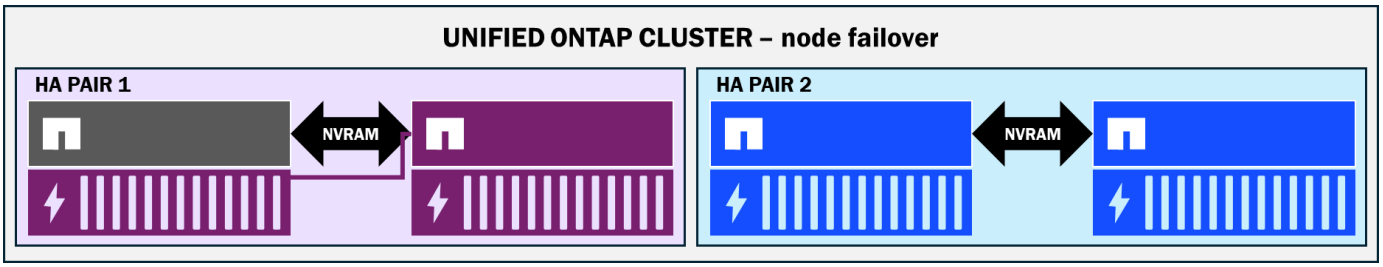
Knoten-zu-Festplatte-Beziehungen

In der einheitlichen ONTAP-Architektur werden Lese- und Schreibvorgänge an eine bestimmte Teilmenge von Festplatten gerichtet. Selbst wenn Sie 24 Festplattengehäuse in einem 24-Knoten-Cluster haben (ein Gehäuse pro Knoten), kann jeder Knoten zu jedem Zeitpunkt nur direkt auf ein Festplattengehäuse zugreifen, was die im Cluster verfügbare Kapazität und Leistung begrenzt.



Da NVRAM zwischen HA-Paaren direkt verbunden ist, müssen die Knoten physisch nebeneinander liegen und sind als Failover-Ziele enger gekoppelt. Wenn beispielsweise ein Knoten auf seinen Partnerknoten ausfällt, hat er physisch nur Zugriff auf die Festplatten im HA-Paar-Domäne.

Vereinheitlichter ONTAP Cluster während eines HA-Failovers

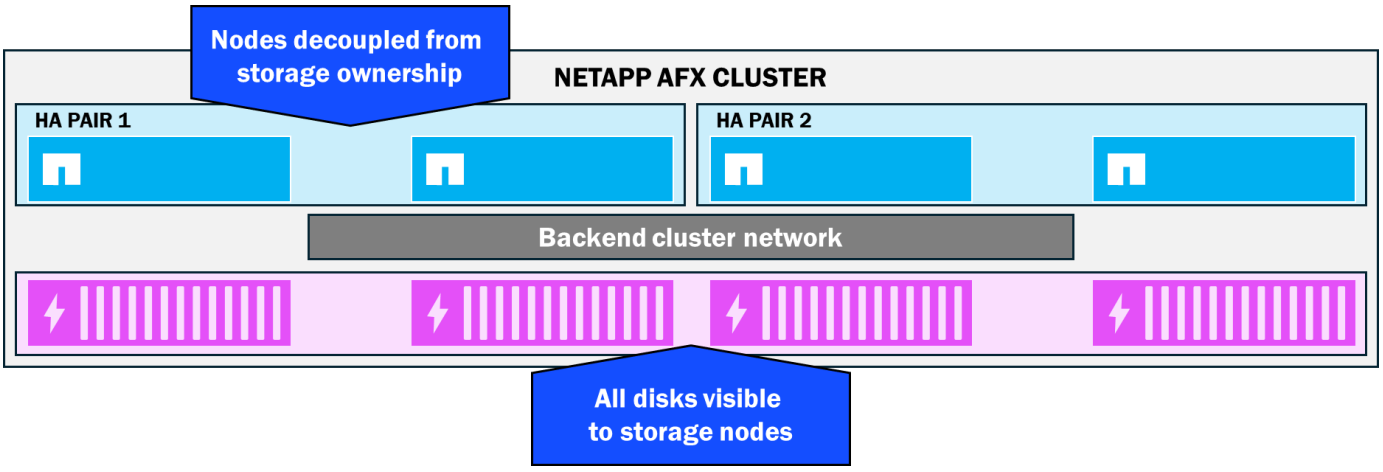


In NetApp AFX gibt es einige wesentliche Änderungen in der Art und Weise, wie Festplatten den Rechenknoten präsentiert werden.

Alle Datenträger sind für alle Speicherknoten sichtbar – keine Datenträgerzugehörigkeit

In NetApp AFX sind alle Nodes und Shelfs an denselben Backend-Switch angeschlossen, was es ONTAP ermöglicht, den gesamten Sichtbarkeitsbereich für Festplatten auf den gesamten Stack auszudehnen. Folglich besitzt kein Node bestimmte Festplatten. Stattdessen nehmen alle Festplatten an einem einzigen Kapazitätspool teil, der als Storage Availability Zone bezeichnet wird und einfacheres Kapazitätsmanagement sowie ein erhöhtes Leistungspotenzial bietet (mehr verfügbare Festplatten bedeuten mehr verfügbare Leistung).

NetApp AFX-Speicherverfügbarkeitszone

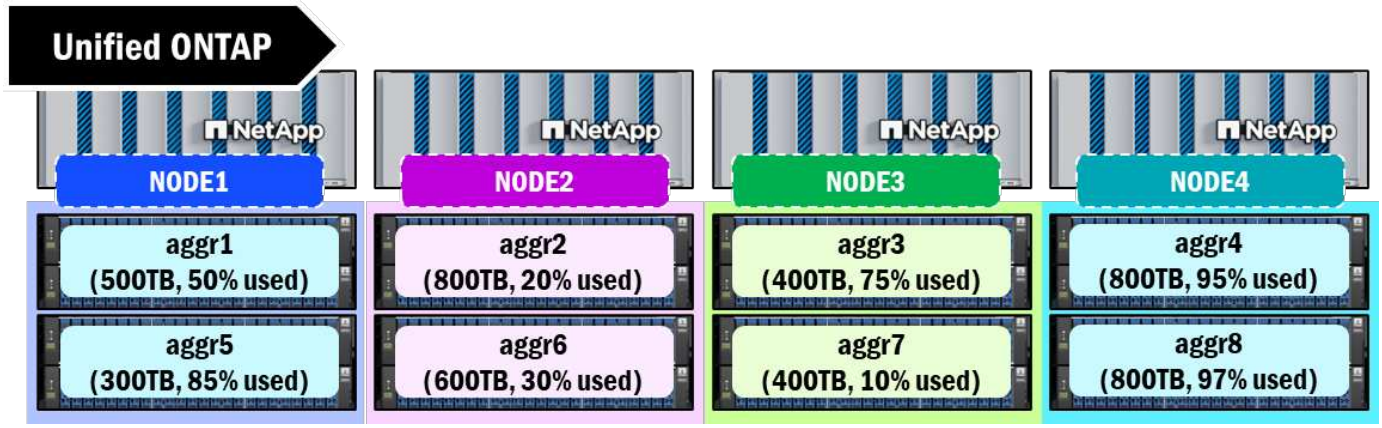


Keine physischen Aggregate mehr

Unified ONTAP fasst Festplatten in RAID-Gruppen zusammen und kombiniert diese zu einem Kapazitätskonstrukt, dem sogenannten Aggregat. Dieses Aggregat stellt die physische Kapazität dar und ist die Grenze des Speicherplatzes, der für die Erstellung von Volumes zur Bereitstellung von Daten für Endbenutzer zur Verfügung steht. Jedem Knoten muss mindestens ein Aggregat zugewiesen sein und diese Aggregate haben derzeit ein Limit von 800TB. Sobald dieses Limit erreicht ist, steht kein Speicherplatz mehr für zusätzliche Schreibvorgänge zur Verfügung.

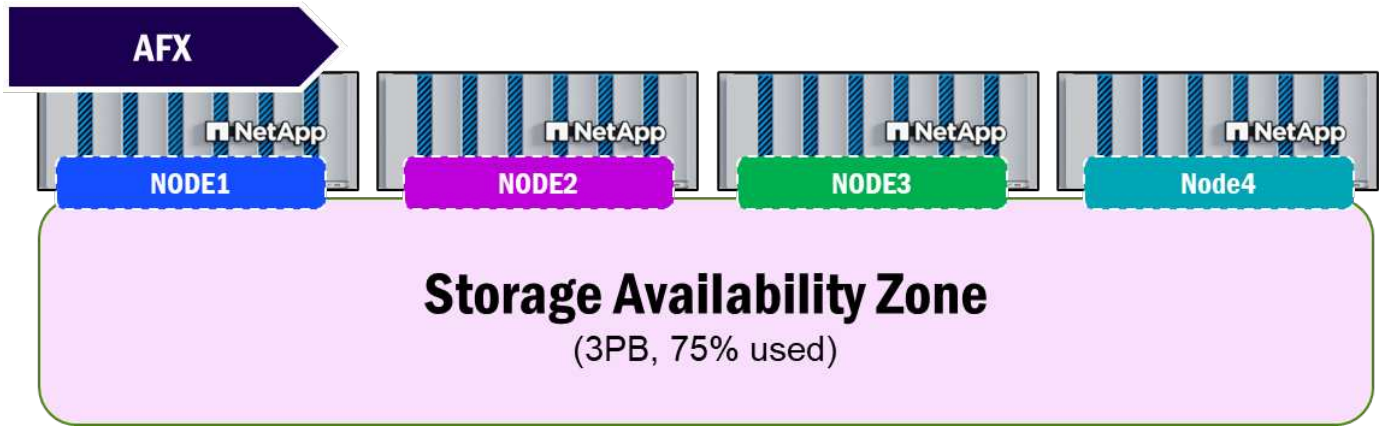
Physische Aggregate können auch Kapazitätsmanagement-Herausforderungen mit sich bringen, da Speicheradministratoren Volumes mitunter manuell verschieben müssen, um eine ausgewogene Kapazitätsverteilung zwischen den Clusterknoten zu gewährleisten. Diese Herausforderungen können sich bei Verwendung einer Scale-Out-Volume-Architektur (z. B. eines FlexGroup-Volumes) noch verstärken. Aggregate können zudem hinsichtlich Größe, Anzahl und Typ der Festplatten usw. variieren, was beim Wechsel zwischen den Knoten ebenfalls zu Leistungsunterschieden führen kann.

Aggregate in Unified ONTAP



NetApp AFX virtualisiert das Konzept eines physischen Aggregats, macht es ONTAP-verwaltet und verlagert das physische Kapazitätsmanagement von einer knotenbasierten auf eine clusterbasierte Verwaltung über die neue Storage Availability Zone. Dieser zentrale Kapazitätspool bietet einen „What you see is what you get“-Ansatz für das Speicherplatzmanagement.

NetApp AFX-Speicherverfügbarkeitszone



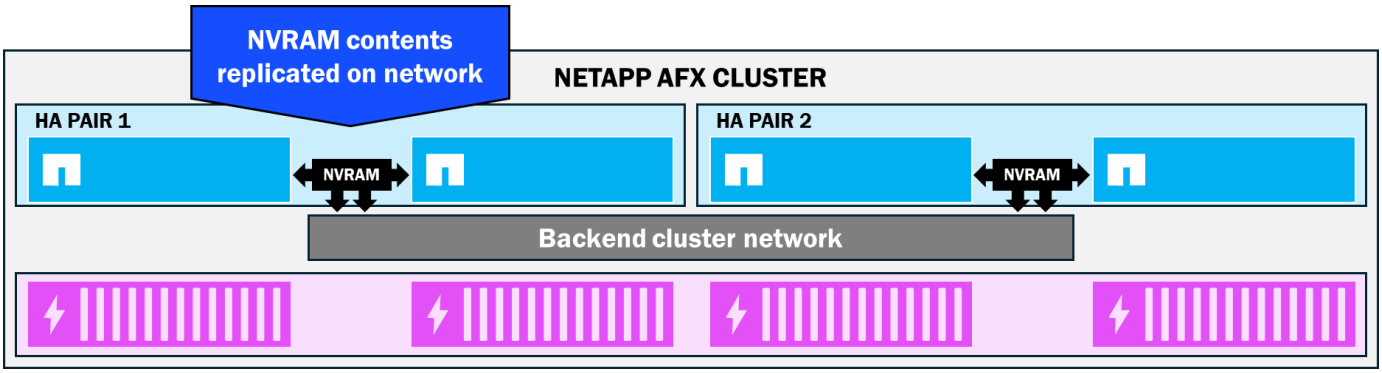
NVRAM wurde von direkter Verbindung auf geschaltete Replikation umgestellt

ONTAP verwendet NVRAM als Zwischenspeicher, um eingehende Schreibvorgänge in einem Cluster zu schützen. Jeder Knoten in einem ONTAP Cluster verfügt über eine mit Akku ausgestattete NVRAM-Karte. Wenn ein Schreibvorgang von einem Client an ein Volume gesendet wird, wird dieser zuerst im NVRAM gespeichert. Der NVRAM-Inhalt wird dann auf die Festplatte geschrieben, sobald der NVRAM voll ist oder ein 10-Sekunden-Timer abläuft (je nachdem, was zuerst eintritt). Dies wird als Konsistenzpunkt bezeichnet.

Der NVRAM-Inhalt wird zudem ständig zwischen den HA-Paaren repliziert, was zusätzlich zur Sicherung der Datenkonsistenz beiträgt, da im Falle eines Knotenausfalls der NVRAM-Inhalt auf dem verbleibenden Knoten erhalten bleibt und auf die Festplatte geschrieben wird.

In Unified ONTAP-Clustern sind die NVRAM-Karten zwischen HA-Paaren direkt miteinander verbunden. NetApp AFX verlagert die NVRAM-Replikation in das Backend-Clusternetzwerk. Dadurch entfällt die strenge Abstandsanforderung für HA-Partnerknoten. Stattdessen können HA-Paare bis zur maximalen Entfernung von Ethernet voneinander getrennt sein.

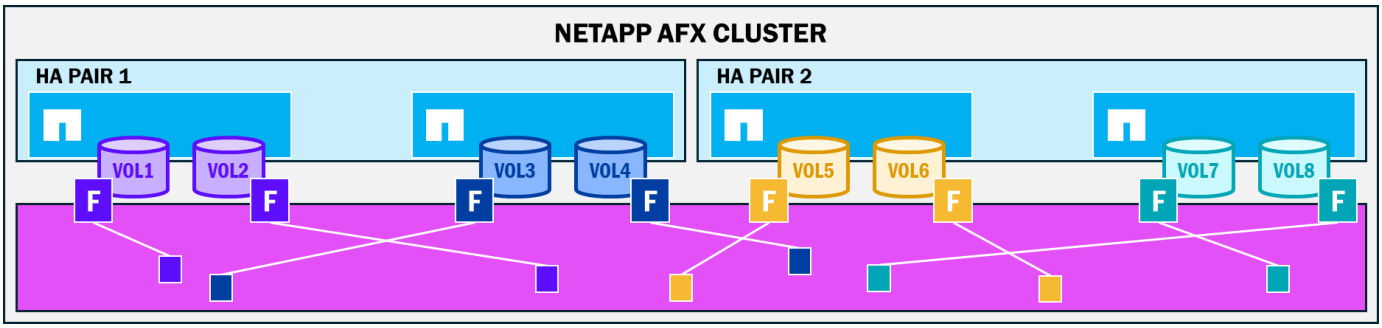
NetApp AFX NVRAM Replikation



Daten, die auf beliebige (und alle) Datenträger in der Verfügbarkeitszone geschrieben werden

NetApp AFX beseitigt das Konzept des Festplattenbesitzes und verlagert die physische Aggregatstruktur auf einen virtualisierten Ansatz, der von ONTAP verwaltet wird, wobei die für den Cluster erworbene Kapazität allen an den Cluster angeschlossenen Knoten zur Verfügung steht. Mit AFX können alle Knoten unabhängig von der Knoten:Volume-Zugehörigkeit auf alle Festplatten in der Storage Availability Zone schreiben. Knoten besitzen weiterhin ein Konzept des Volume-Besitzes, da Schreibvorgänge nach wie vor über den NVRAM laufen, aber diese Daten können an beliebiger Stelle innerhalb der verfügbaren Kapazität abgelegt werden. Dies bedeutet, dass eine größere Anzahl von Festplatten an einer einzelnen Arbeitslast teilnehmen kann, was Leistungssteigerungen bietet.

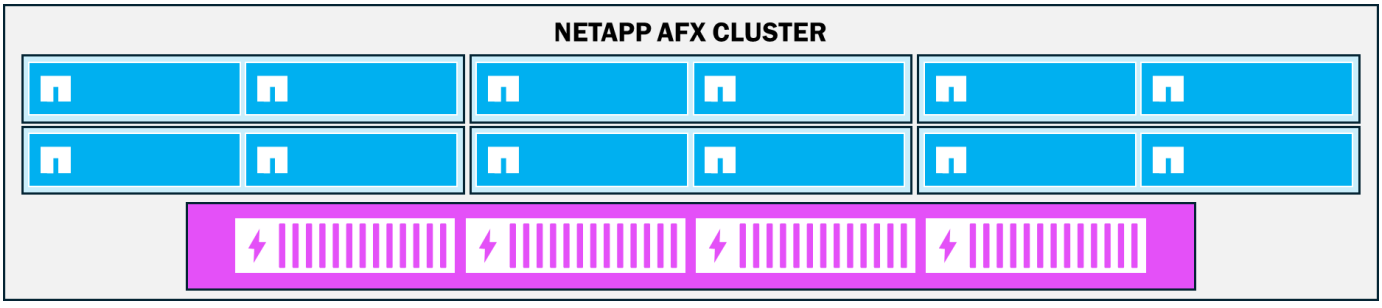
Wie Daten in einer Storage Availability Zone landen



Unabhängige Skalierung der Kapazität und der Rechenknoten

Da die Hardware-Ressourcen in der NetApp AFX-Architektur entkoppelt sind, müssen Knoten nicht mehr mit zugehörigen Festplatten kombiniert werden. Wenn einem Cluster Leistungsressourcen wie RAM, CPU oder Netzwerkdurchsatz fehlen, müssen lediglich Speicherknoten hinzugefügt werden, die die bestehende Storage Availability Zone nutzen können. Wird hingegen mehr Kapazität benötigt, müssen nur zusätzliche Shelves hinzugefügt werden. Diese Flexibilität stellt sicher, dass Sie nur die Ressourcen erwerben, die Sie benötigen, und somit Überprovisionierung vermeiden.

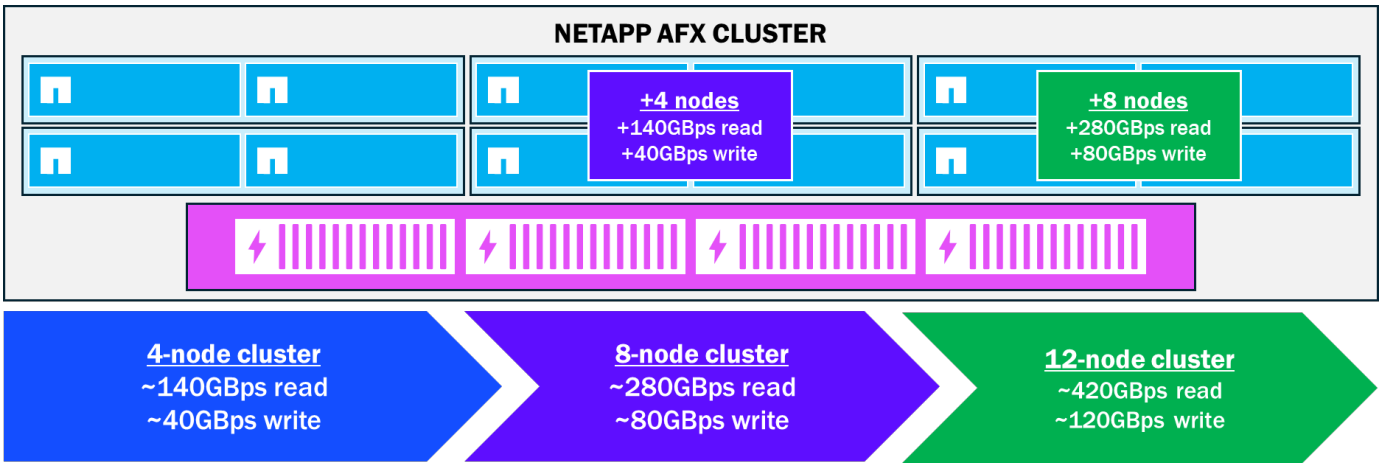
NetApp AFX – Unabhängige Skala



Lineare Skalierung der Knotenleistung

Mit dem Hinzufügen von Knoten zu einem AFX-Cluster werden dem Workload mehr CPU-, RAM- und Netzwerkressourcen zur Verfügung gestellt. Sobald diese Ressourcen in die Umgebung integriert werden, verläuft die Leistungssteigerung linear. Die folgende Grafik veranschaulicht, wie die Leistung steigt, wenn Knoten hinzugefügt werden.

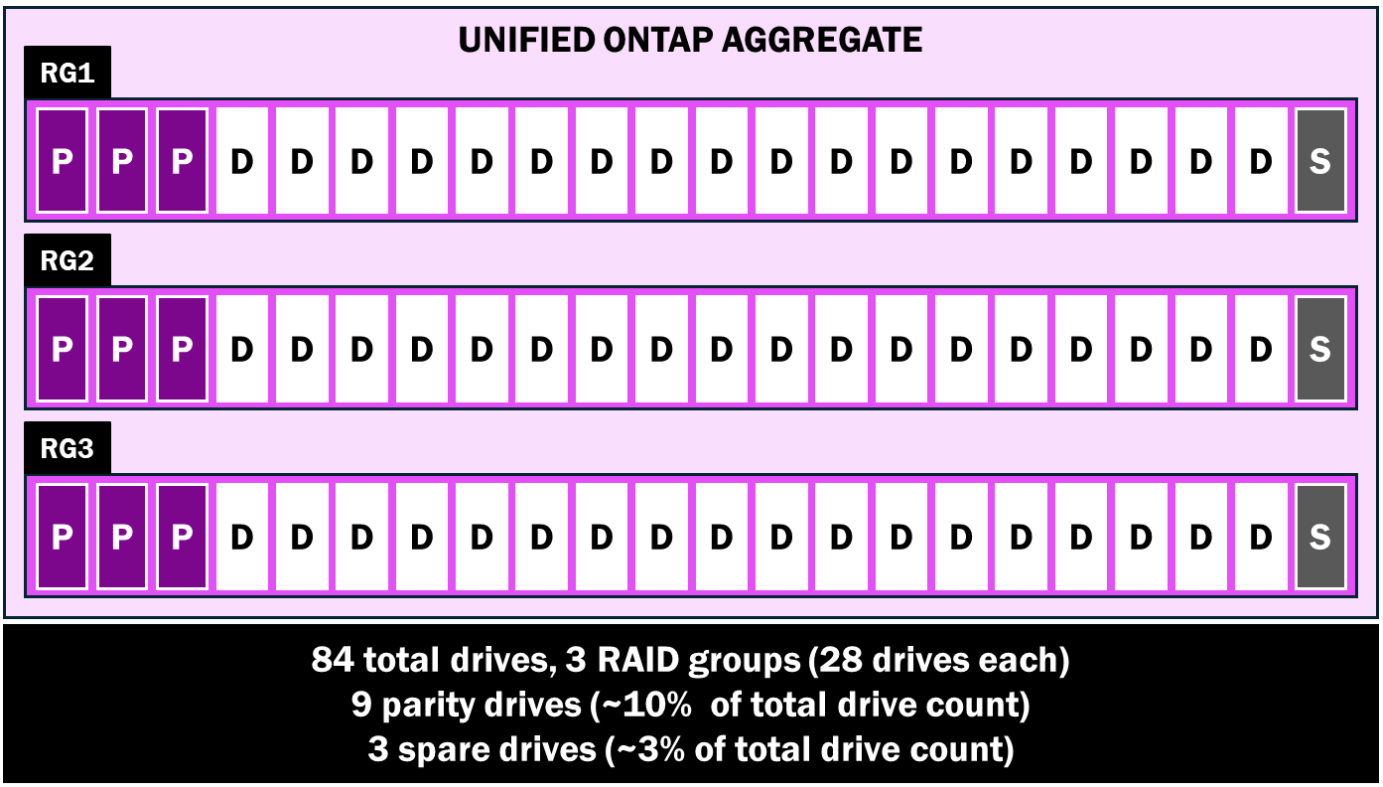
Die Leistung steigt linear mit der Hinzufügung von NetApp AFX-Knoten.



Größere RAID-Gruppen, weniger Paritätslaufwerke

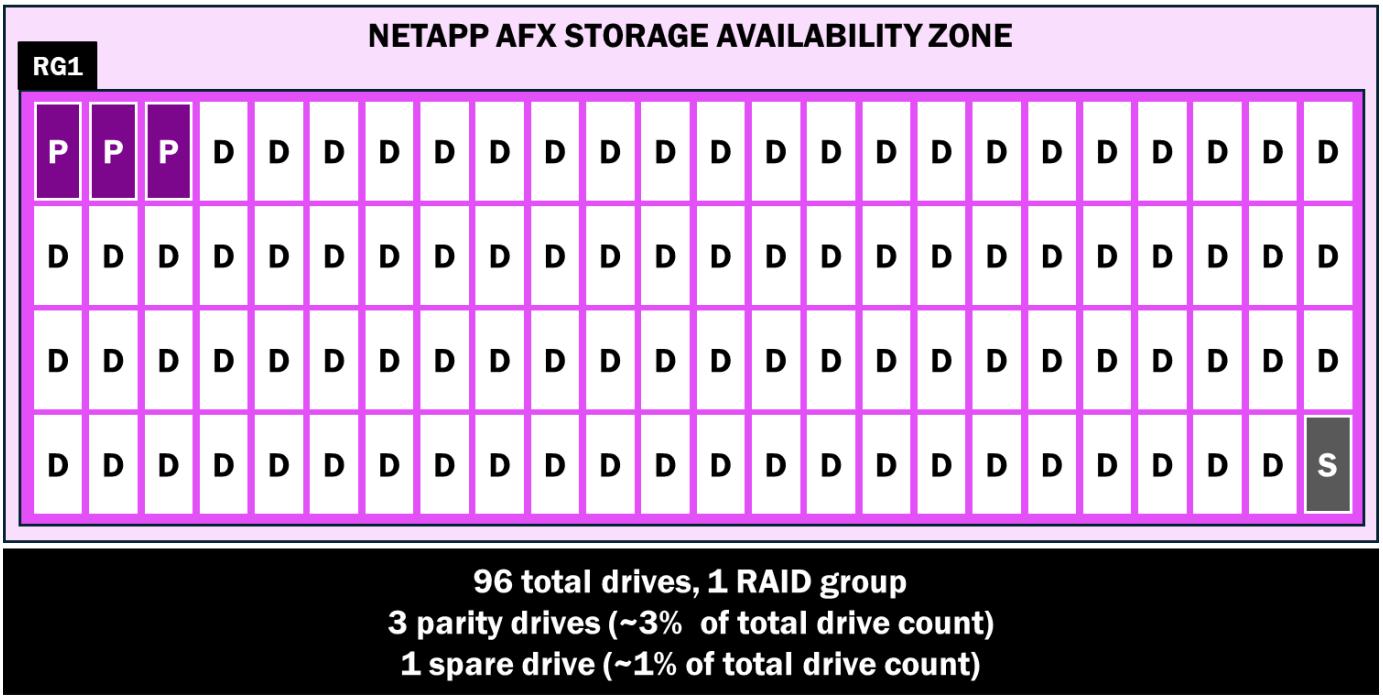
ONTAP bietet eine Kombination aus Datenschutz und Leistung für Festplatten über RAID-Gruppen – insbesondere RAID-TEC, das im Falle von Festplattenausfällen einen dreifachen Paritätsschutz bietet. RAID-TEC kann bis zu drei gleichzeitige Laufwerksausfälle in einer RAID-Gruppe überstehen. In unified ONTAP haben RAID-Gruppen eine maximale Festplattenanzahl von 28, wobei 3 Laufwerke für Parität und 1 Laufwerk als Ersatz reserviert sind. Somit werden 24 der 28 Laufwerke für Datenoperationen/RAID-Stripes verwendet.

Vereinheitlichte ONTAP RAID-Gruppen



NetApp AFX nutzt weiterhin RAID-TEC, erhöht aber die RAID-Gruppengröße auf 96 Laufwerke, benötigt dabei nur 3 Paritätslaufwerke und 1 Ersatzlaufwerk. Größere RAID-Gruppen bieten eine höhere Gesamtleistung, während das Ausfallrisiko durch eine Kombination aus niedrigen Ausfallraten für SSD, gleichmäßiger verteilten Operationen auf eine größere Anzahl von Laufwerken sowie Verbesserungen beim Wiederherstellen von Datenlaufwerken aus Parität in NetApp AFX minimiert wird.

NetApp AFX Storage Availability Zone RAID-Gruppe



Die folgende Tabelle gibt einen ungefähren Wert für die nutzbare Bruttokapazität von 84 Festplatten in Unified

ONTAP und NetApp AFX mit unterschiedlichen Laufwerksgrößen an.

Ungefährer Bruttokapazitätsvergleich, 84 Laufwerke – Unified ONTAP und NetApp AFX

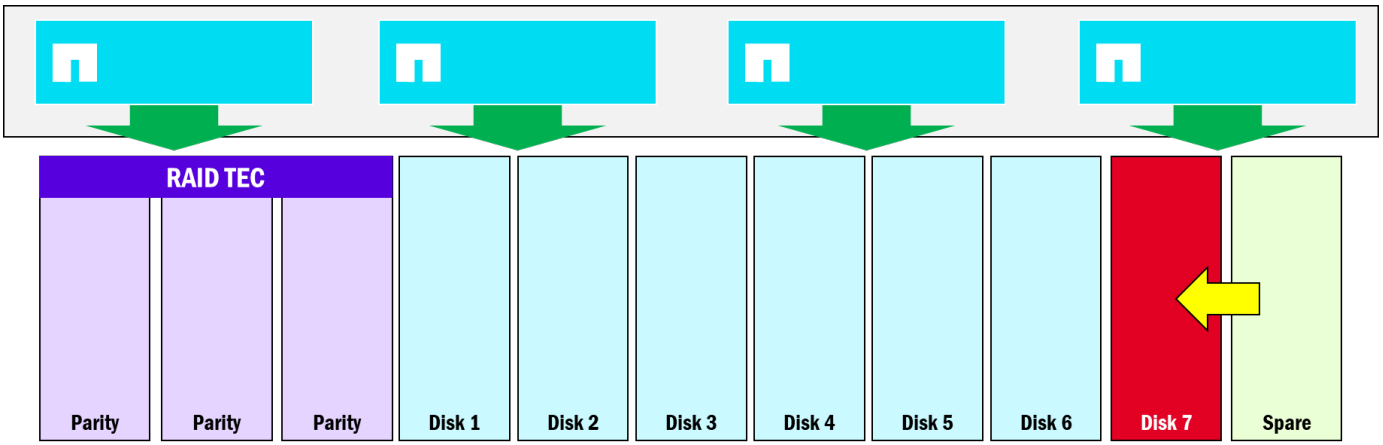
Laufwerksgröße	Ungefähre Bruttokapazität (einheitlich)	Ungefähre Bruttokapazität (AFX)
7,6 TB	~547,2 TB	~608TB (+60,8TB)
15,3 TB	~1101,6TB	~1224TB (+122,4TB)
30,6 TB	~2203,2TB	~2448TB (+244,7TB)
60,1 TB	~4327,2TB	~4808TB (+480,8TB)

Schnellere Wiederherstellungszeiten bei Festplattenausfällen

In unified ONTAP besitzt jeder Knoten eine Teilmenge der Festplatten im Speichersystem. Das bedeutet, dass dieser Knoten nur auf diese Festplatten schreibt, aber auch, dass Festplattenwiederherstellungen im Falle eines Festplattenausfalls nur von einem einzelnen Knoten durchgeführt werden.

NetApp AFX verzichtet auf die Notwendigkeit der Festplattenzugehörigkeit. Dadurch können bei Bedarf alle Laufwerke von einem einzigen Knoten aus beschrieben werden. Das bedeutet auch, dass bei der Wiederherstellung eines Laufwerks aus Parität alle Knoten im Cluster beteiligt sind, sodass die Wiederherstellung deutlich schneller erfolgen kann als wenn ein einzelner Knoten dies allein durchführen müsste.

Festplattenrekonstruktionen in NetApp AFX

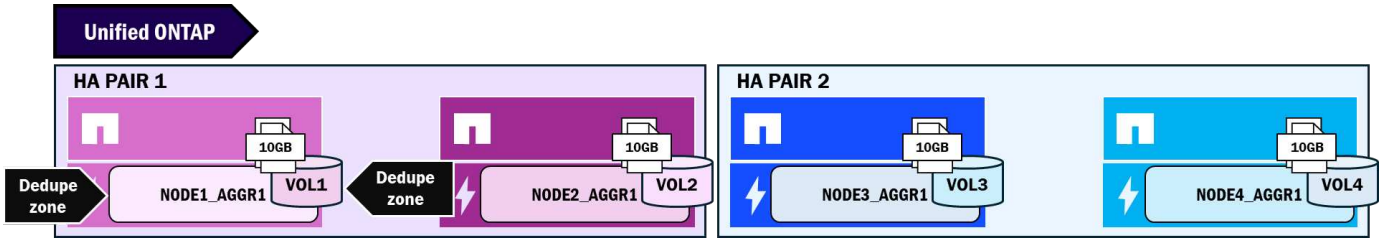


Deduplizierungsdomänen

Die Deduplizierung ermöglicht es einem Speichersystem, doppelte Blöcke in seinem Dateisystem zu finden und anschließend Zeiger auf einen einzelnen Block zu erstellen, um die insgesamt belegte Speicherkapazität zu reduzieren. In unified ONTAP gibt es für die Deduplizierung bestimmte Grenzen, welche Blöcke reduziert werden können. Diese Grenzen hängen von der Art der verwendeten Deduplizierung ab. Im Allgemeinen gilt:

- Volumenbasierte Deduplizierung → Volumengrenze
- Volumenübergreifende Deduplizierung → Aggregatgrenze

Vereinheitlichte ONTAP-Deduplizierungsdomänen



Die folgende Tabelle zeigt das Kapazitätsverhalten für duplizierte Daten in verschiedenen Szenarien in unified ONTAP. Da sich Dateikopien über mehrere Knoten und Aggregate (und somit Deduplizierungsdomänen) erstrecken, verringert sich die Speicherplatzersparnis.

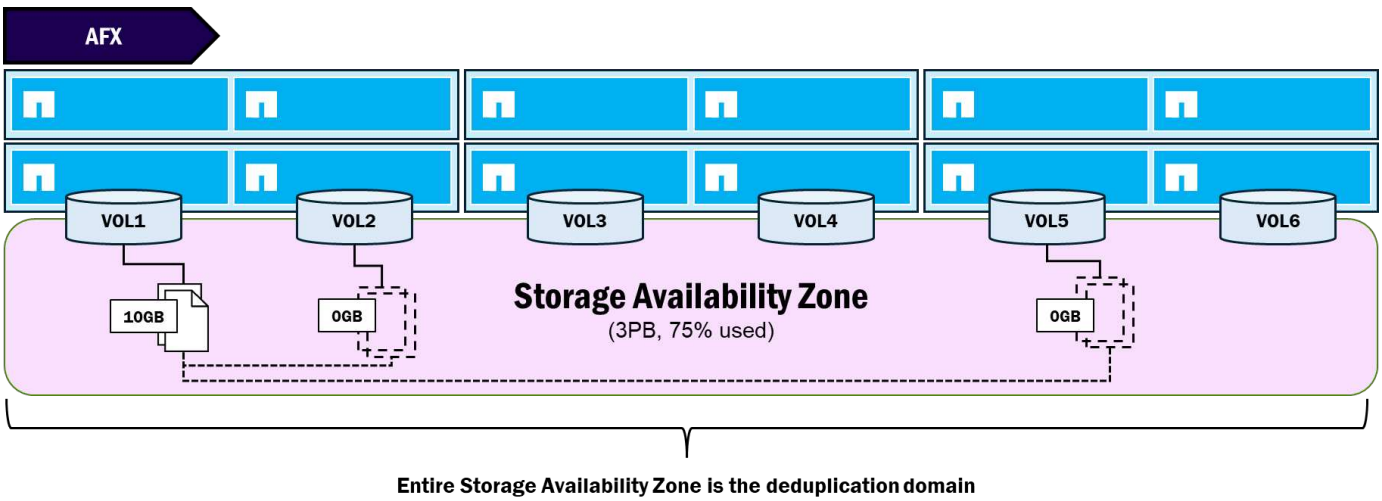
Deduplizierungsverhalten in verschiedenen Szenarien für identische 10GB-Dateien – unified ONTAP

Szenario	Verwendeter Speicherplatz
Vier Kopien derselben 10-GB-Datei, dasselbe Volume (Volume-Deduplizierung)	10 GB
Vier Kopien derselben 10-GB-Datei, unterschiedliche Volumes, gleiches Aggregat (volumeübergreifende Deduplizierung aktiviert)	10 GB
Vier Kopien derselben 10-GB-Datei, 4 verschiedene Volumes, 4 verschiedene Aggregate (volumeübergreifende Deduplizierung aktiviert)	40 GB

Da NetApp AFX physische Aggregate entfernt und das Kapazitätsmanagement in die neue Storage Availability Zone verlagert, ändern sich auch die Grenzen der Deduplizierungsdomäne. In AFX befindet sich die Deduplizierungsdomäne vor Version 9.19.1 auf Volume-Ebene (wie bei unified ONTAP) und auf Node-Ebene (statt auf Aggregatebene).

Ab ONTAP 9.19.1 unterstützt AFX eine globale Deduplizierungsdomäne auf Ebene der Storage Availability Zone, sodass alle duplizierten Blöcke im Cluster-Speicherpool gleich behandelt werden.

NetApp AFX – Globale Deduplizierungsdomäne (ONTAP 9.19.1)



Die folgende Tabelle zeigt das Kapazitätsverhalten für duplizierte Daten in verschiedenen Szenarien in NetApp AFX.

Deduplizierungsverhalten in verschiedenen Szenarien für identische 10GB-Dateien – NetApp AFX

Szenario	Verwendeter Speicherplatz
Vier Kopien derselben 10-GB-Datei, dasselbe Volume (Volume-Deduplizierung)	10GB (9.18.1) 10GB (9.19.1)
Vier Kopien derselben 10-GB-Datei, verschiedene Volumes, gleicher Node (cross-volume Deduplizierung aktiviert)	10GB (9.18.1) 10GB (9.19.1)
Vier Kopien derselben 10GB-Datei, 4 verschiedene Volumes, 4 verschiedene Knoten (cross-volume Deduplizierung aktiviert)	40GB (9.18.1) 10GB (9.19.1)

Funktionen, die entfernt wurden/nicht mehr unterstützt werden

NetApp AFX ist für leistungsstarke NAS- und Objekt-Workloads konzipiert – insbesondere (aber nicht ausschließlich) für KI-Training und -Inferenz. Mit dem Design von NetApp AFX wurden einige Entscheidungen getroffen, um bestimmte Funktionen in ONTAP zu deaktivieren.

- Da der Fokus auf leistungsstarken NAS- und Objekt-Workloads liegt, wurden Block-Workloads aus der NetApp AFX-Lösung entfernt. Es gibt keine Unterstützung für FCP-, iSCSI- oder NVMe-Datenprotokolle, und es ist nicht geplant, Blockprotokolle hinzuzufügen.
- „Disaggregiert“ ist gleichbedeutend mit „deaggregiert“, was bedeutet, dass Aggregate (zumindest als physisches Speicherverwaltungskonzept) entfernt wurden. Die Entfernung des physischen Aggregats vereinfacht nicht nur das Kapazitätsmanagement in ONTAP, sondern bietet auch den Mechanismus, um einen einzigen Kapazitätspool zu ermöglichen.
- Durch die Entfernung der Aggregate entfallen auch die zugehörigen Funktionen. Metrocluster nutzt beispielsweise die Spiegelung auf Aggregatebene für seine Standortausfallsicherung. Daher wird Metrocluster auch aus NetApp AFX entfernt. Die Standortausfallsicherung wird stattdessen durch die neue SnapMirror Active-Sync für NAS-Funktion in ONTAP 9.19.1GA bereitgestellt.
- Die Cold-Data-Tiering-Funktion namens FabricPool ist derzeit für NetApp AFX ebenfalls nicht verfügbar, da sie auch aggregatspezifisch ist.
- Kopiebasierte Volumenverschiebungen sind in NetApp AFX aufgrund der neuen Kapazitätsarchitektur ebenfalls nicht mehr erforderlich. Weitere Informationen finden Sie unter Zero-Copy-Volume-Verschiebungen.
- Entfernung bedeutet auch einige Änderungen an der CLI/GUI/REST API, sodass alle Befehle oder API-Aufrufe für nicht mehr unterstützte Funktionen ebenfalls entfernt werden.
- ZAPI steht NetApp AFX derzeit nicht zur Verfügung.
- NFS-Kopierauslagerung für Virtualisierung (FlexGroup-Volumes nur mit granularer Datenverteilung)

Änderungen im ONTAP-Management

Im Allgemeinen ändert die NetApp AFX-Verwaltung nichts an den Mechanismen zur Clusterverwaltung. Administratoren können weiterhin die CLI, GUI und REST-APIs nutzen, um sich anzumelden und einen Cluster zu konfigurieren. Aber NetApp AFX bot die Möglichkeit, einige Aspekte der Durchführung von Speicherverwaltungsoperationen zu verbessern.

Einfacheres Kapazitätsmanagement

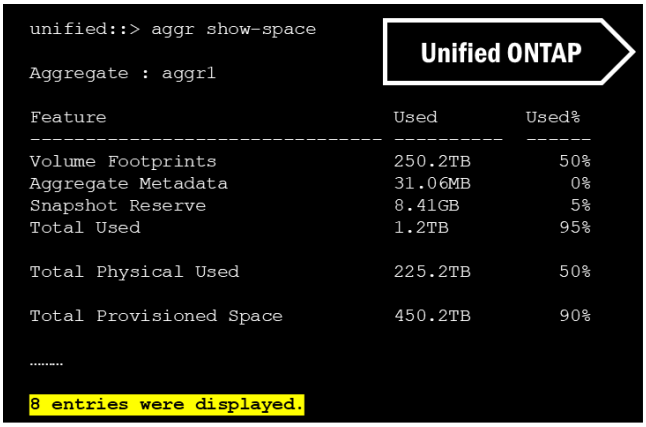
Die NetApp AFX Storage Availability Zone reduziert die Verwaltungspunkte von einem knoten- und

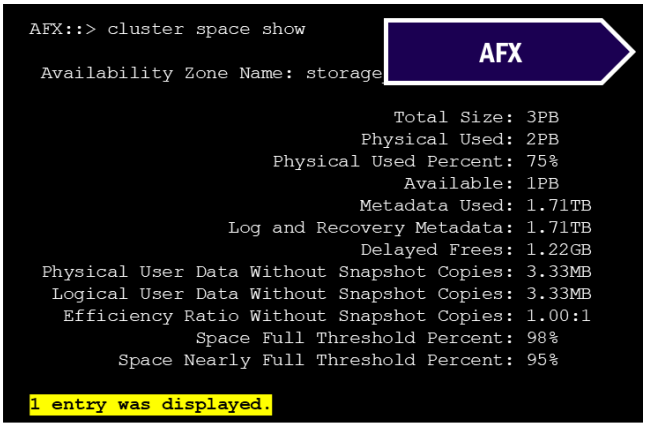
aggregatbasierten Ansatz auf einen einzigen Kapazitätspool, der dem gesamten Cluster zur Verfügung steht. Wenn Volumes wachsen oder schrumpfen, leiht und gibt ONTAP automatisch Kapazität an die bzw. aus der Storage Availability Zone zurück.

Dadurch müssen sich Speicheradministratoren nicht mehr darum kümmern, den verfügbaren freien Speicherplatz auf bis zu 24 Knoten und potenziell Hunderten von Aggregaten zu ermitteln und zu verwalten. Stattdessen gibt es nur einen Ort, an dem die Kapazität verwaltet und angezeigt wird.

Um beispielsweise in der CLI von unified ONTAP die gesamte physische Kapazität eines Clusters anzuzeigen, verwenden Sie „`aggregate show-space`“, was dann jeden Aggregateintrag ausgibt. In NetApp AFX haben Sie „`cluster space show`“, was nur die einzelne Storage Availability Zone anzeigt.

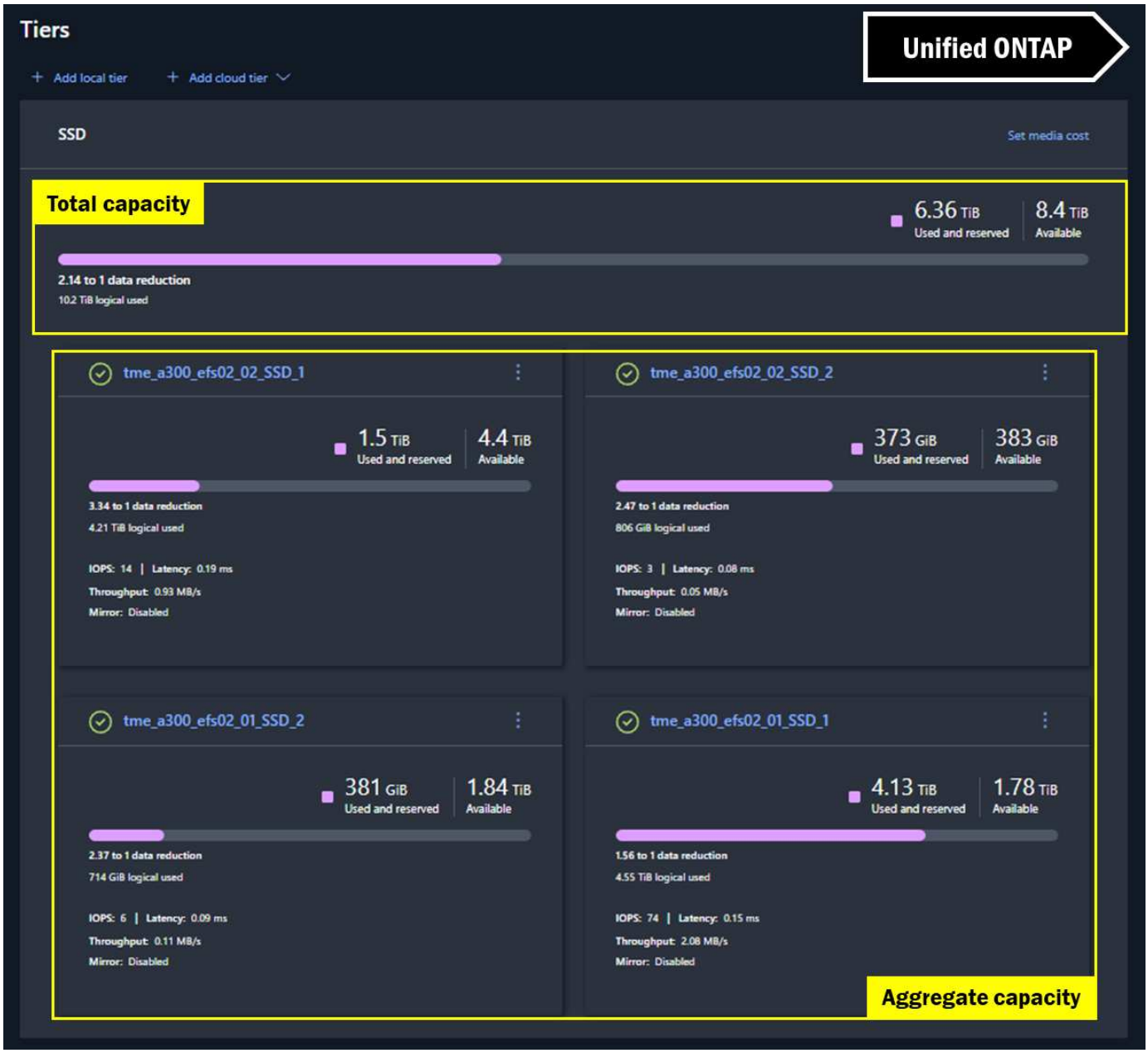
Direkter Vergleich der Kapazitäts-CLI-Befehle in Unified ONTAP und NetApp AFX





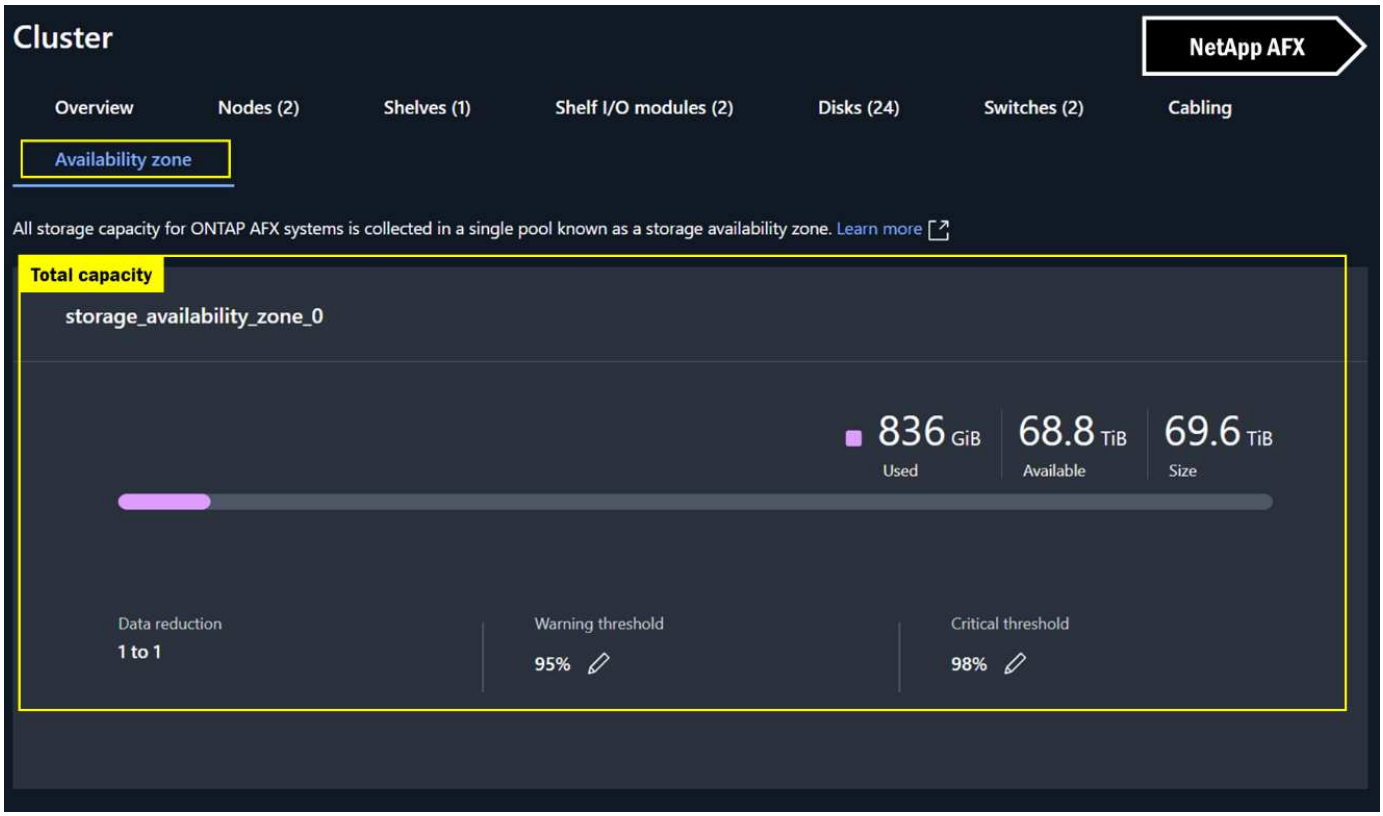
In der Unified ONTAP System Manager GUI werden Tiers verwendet, um die Kapazität anzuzeigen. Tatsächlich versucht die GUI, die ganzheitliche Kapazität für den Cluster darzustellen, indem sie die Gesamtwerte addiert, zeigt jedoch weiterhin die Gesamtnutzung auf Basis jedes einzelnen Aggregats an.

System Manager-Kapazitätsansichten – Unified ONTAP



Im NetApp AFX System Manager ist die Ansicht für den Clusterspeicherplatz nahezu identisch, da jedoch keine Aggregate vorhanden sind, entfallen zusätzliche Berechnungen. Die angezeigte Kapazität entspricht der tatsächlich verfügbaren Kapazität.

System Manager-Kapazitätsansichten – NetApp AFX

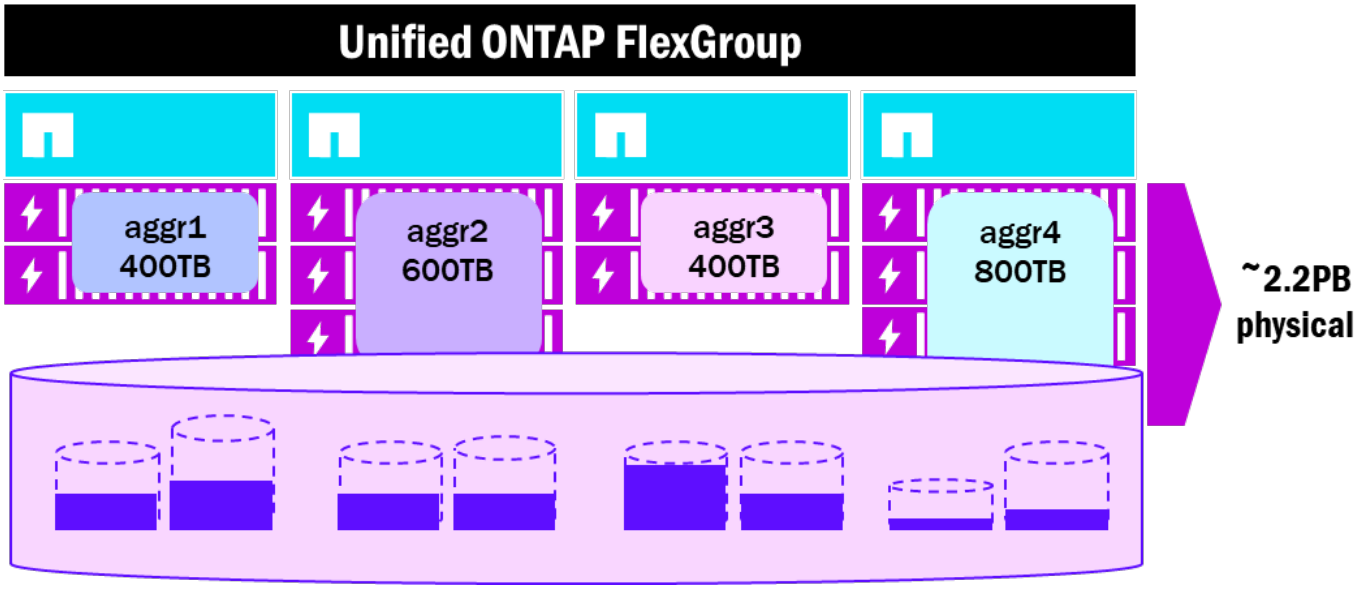


Verbesserungen beim FlexGroup Volume-Management

Ein FlexGroup-Volume besteht aus mehreren zugrunde liegenden FlexVol-Teilvolumes, die auf verschiedenen Knoten und Aggregaten im Cluster erstellt und NAS-Clients als ein einziger großer Namensraum präsentiert werden. FlexGroup-Volumes bieten Vorteile hinsichtlich Leistung, Skalierbarkeit, Lastverteilung und Dateianzahl für rechenintensive Workloads. Da sie jedoch knoten- und aggregatübergreifend koordiniert werden, stoßen sie gelegentlich an physikalische Grenzen, wenn die Kapazität knapp wird, da die von den Aggregaten bereitgestellten unabhängigen Dateisysteme ebenfalls eine eigene Kapazitätsnutzung und -begrenzung haben. Wenn beispielsweise ein Aggregat mit FlexGroup-Volume-Bestandteilen vor anderen Aggregaten im Cluster voll wird, könnte das gesamte FlexGroup selbst von Kapazitäts- oder Leistungsproblemen betroffen sein.

Als Folge davon kann es vorkommen, dass sich Speicheradministratoren zu sehr mit der zugrunde liegenden FlexGroup-Infrastruktur beschäftigen und sich weniger auf die Wartung anderer Aspekte der Umgebung konzentrieren.

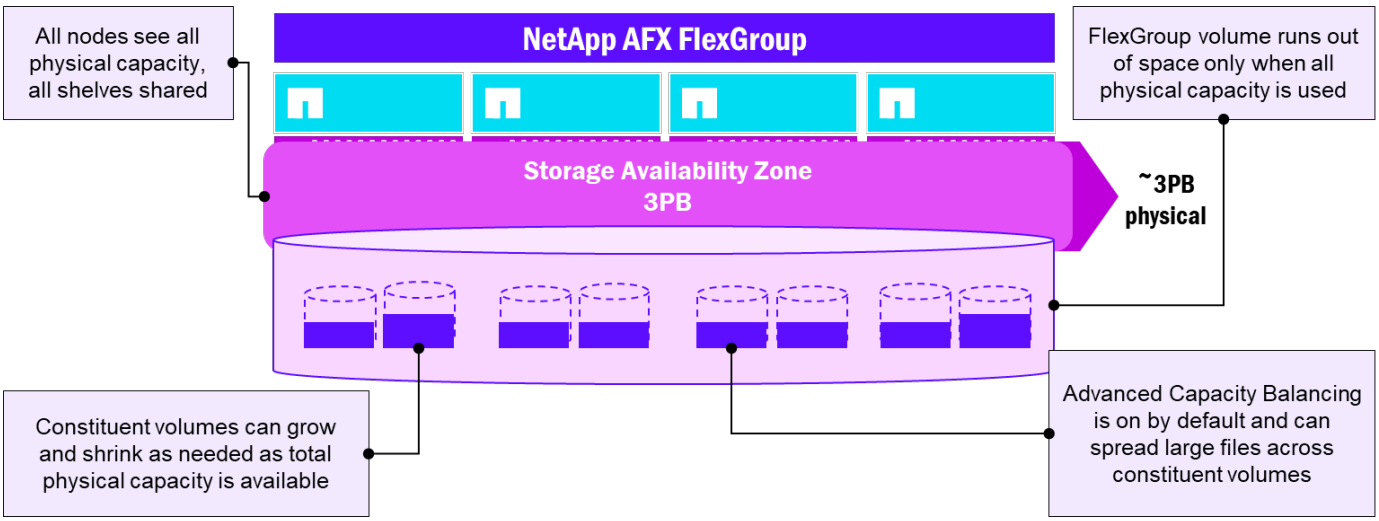
FlexGroup Volume-Layout – Unified ONTAP Aggregates



NetApp AFX stellt die Kapazität in einer einzigen Storage Availability Zone bereit, was der Art und Weise, wie FlexGroup-Volumes vorgesehen sind zu funktionieren, besser entspricht. Anstatt mehrerer Teilvolumes in verschiedenen, potenziell unterschiedlich großen Aggregaten befinden sich alle Volumes im selben Kapazitätspool, was den gesamten Verwaltungsaufwand bei der Verwendung eines FlexGroup-Volumes erheblich vereinfacht.

Darüber hinaus aktiviert AFX standardmäßig die erweiterte Kapazitätsverteilung für FlexGroup-Volumes, wodurch größere Dateien besser auf dem Volume verteilt werden. Jetzt werden FlexGroup-Volume-Komponenten weniger zu einem Verwaltungskonzept und arbeiten stattdessen unauffällig im Hintergrund.

FlexGroup Volume-Layout - NetApp AFX



Automatisierte Speicherverwaltungsaufgaben

Mit der Storage Availability Zone in NetApp AFX wird die gesamte Kapazität auf alle Knoten verteilt. Obwohl die Knoten weiterhin Volumes besitzen, verwaltet ONTAP die Kapazitätsnutzung jedes Knotens automatisch, indem Kapazität je nach Bedarf ausgeliehen und freigegeben wird. Das bedeutet, dass sich Speicheradministratoren nicht mehr darum kümmern müssen, wie der nutzbare Speicherplatz am besten ausbalanciert wird.

Darüber hinaus wird die RAID-Gruppenverwaltung von ONTAP automatisiert, wobei neu hinzugefügte

Festplatten ohne Administratoreingriff bestehenden oder neuen RAID-Gruppen hinzugefügt werden. ONTAP verwaltet außerdem Volume-Verschiebungen zwischen Knoten, ohne dass Daten kopiert werden müssen.

Zero-Copy-Volume-Verschiebungen

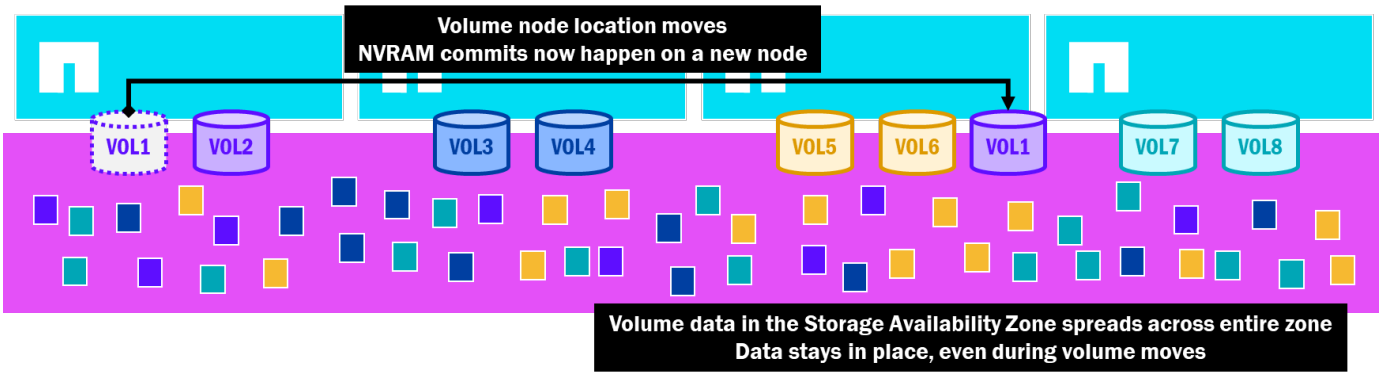
Unified ONTAP bietet eine Möglichkeit, Volumes unterbrechungsfrei zwischen Knoten oder Aggregaten zu verschieben, um die Performance und Kapazitätsnutzung im gesamten Cluster zu verwalten.

Wenn eine Volumenverschiebung gestartet wird, geschieht Folgendes:

- Ein neues leeres Volume wird auf dem angegebenen Zielaggregat erstellt
- Volume-Metadaten (wie z. B. Informationen zur Speichereffizienz, Dateihandles usw.) werden auf das neue Ziel-Volume repliziert.
- Volumendaten werden über das Backend-Cluster-Netzwerk mittels SnapMirror-Technologie auf das Zielvolume repliziert – das Zielaggregat muss über ausreichend freien Speicherplatz für die Verschiebung verfügen, andernfalls schlägt der Verschiebungsauftrag fehl
- Die Volume-Replikation wird erneut durchgeführt, um sicherzustellen, dass beide Volumes mit etwaigen Datenänderungen konsistent sind.
- Es wird ein Umstellungsprozess eingeleitet, um das Ursprungsvolume offline zu nehmen und das Zielvolume als neues Ursprungsvolume für Clients zu aktivieren.
- Client-IO erlebt während der Umstellung eine kurze Pause, aber es sind keine erneuten Mounts erforderlich

In NetApp AFX stellt die Speicherverfügbarkeitszone allen Knoten die gesamte Kapazität zur Verfügung, und alle Knoten können auf jede Festplatte in diesem Pool schreiben. Einmal abgelegte Daten bleiben an ihrem Speicherort – selbst wenn das Volume verschoben wird. Das bedeutet, dass keine Datenkopie erforderlich ist. Der Volume-Verschiebungsprozess ist identisch mit dem von Unified ONTAP, nur dass keine Replikation der Daten über SnapMirror erforderlich ist. Es wird keine zusätzliche Kapazität benötigt.

Null-Kopiervolumenverschiebungen in NetApp AFX



Dank der leichten Volume-Mobilität kann AFX viele Verwaltungsaufgaben automatisieren, ohne dabei Leistungs- oder Kapazitätseinschränkungen in Kauf nehmen zu müssen, und diese Volume-Verschiebungen werden in einigen neuen Funktionen von NetApp AFX verwendet, wie in den unten aufgeführten Themen beschrieben.

HA-Failover-Verhalten

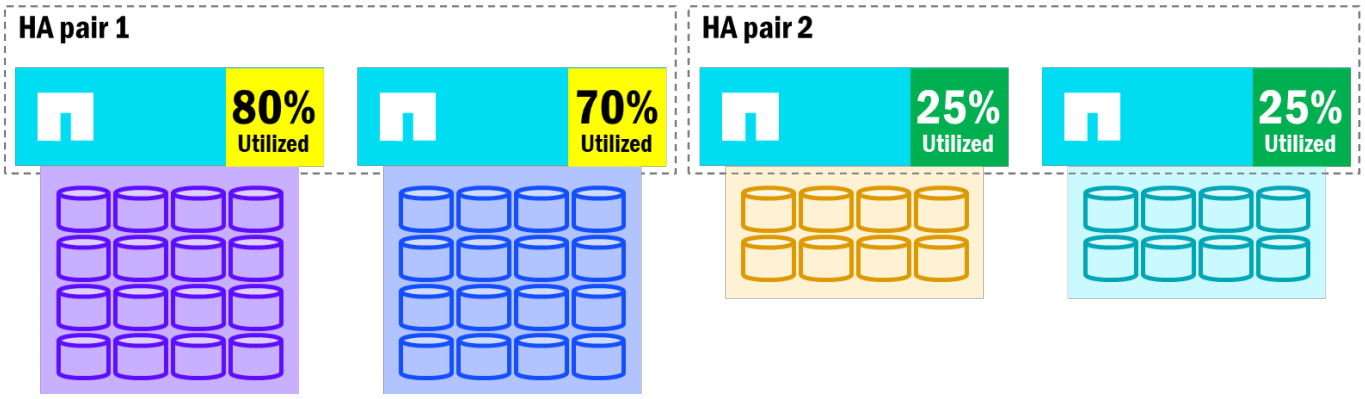
In unified ONTAP besitzt jeder Knoten eigene Festplatten und Aggregate, auf denen Daten über Volumes bereitgestellt werden. Schreibvorgänge werden mithilfe des lokalen NVRAM eines Knotens durchgeführt, um die Daten auf die Festplatten zu schreiben, die der Knoten besitzt. Wenn ein Knoten neu gestartet wird oder

ausfällt, löst ONTAP eine Übernahme der Ressourcen des ausgefallenen Knotens aus, wobei der Besitz von Festplatten und Aggregaten auf den Partnerknoten übertragen wird. Netzwerkschnittstellen werden ebenfalls auf Ports im IP-Adressraum umgeschaltet, und da die NVRAM-Inhalte kontinuierlich über das HA-Paar repliziert werden, schreibt der Knoten die NVRAM-Inhalte, um die Schreibvorgänge des ausgefallenen Knotens auf die Festplatten zu committen. Danach besitzt der verbleibende Knoten die Aggregate und Volumes des ausgefallenen Knotens, bis ein Failback des Knotens erfolgt. Das bedeutet, dass der gesamte Datenverkehr zu diesen Volumes – sowie zu den bereits dem verbleibenden Knoten gehörenden Volumes – auf einem einzigen Knoten verarbeitet wird, bis das Failover-Problem behoben ist.

Im Rahmen der initialen Bereitstellung eines einheitlichen ONTAP-Clusters empfiehlt es sich, Failover-Szenarien im Voraus zu planen, um eine Überlastung des Partnerknotens durch einen einzelnen Knoten zu vermeiden. Dies stellt an sich eine Herausforderung dar, da es schwierig ist vorherzusagen, welche Volumes Performance-Bullies sein könnten, aber Funktionen wie unterbrechungsfreie Volume-Verschiebung und Volume-Quality-of-Service-Richtlinien können bei der Risikominderung helfen.

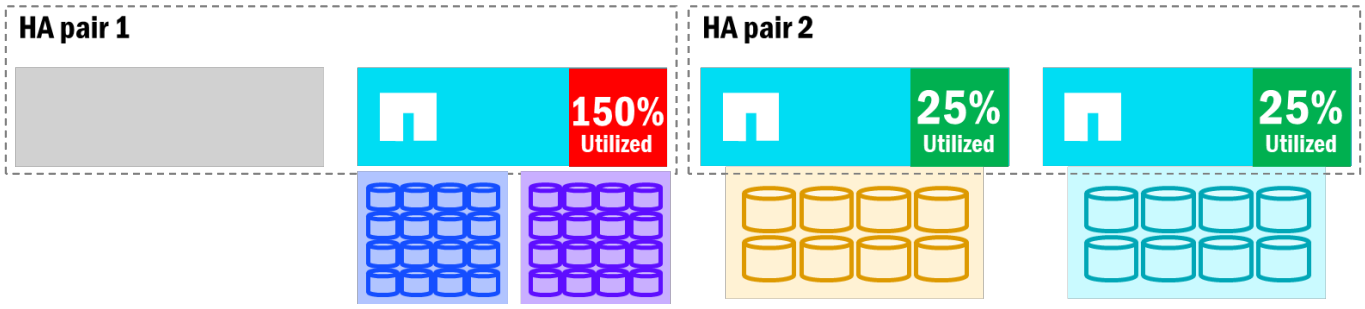
Die folgenden Bilder zeigen, wie es bei vereinheitlichten ONTAP-Clustern zu einer ungleichmäßigen Leistungsverteilung zwischen den Knoten kommen kann und wie ein Failover in manchen Fällen zu Leistungseinbußen führen kann.

Unified ONTAP – potenzielle Ungleichgewichte bei der Knotenauslastung



Wenn die Knoten eines HA-Paares hinsichtlich Volume-Anzahl und Leistungsauslastung unausgewogen sind, beeinträchtigen Knotenausfälle die Gesamtleistung, da der verbleibende Knoten nun alle Volumes des ausgefallenen Knotens verwaltet. Gleichzeitig haben andere Knoten im Cluster möglicherweise Kapazitäten, zusätzliche Aufgaben zu übernehmen.

Unified ONTAP – Auswirkungen des Ausfalls auf die Knotenauslastung



Wenn ein HA-Partner zusätzliche Aufgaben übernehmen muss, kann er überlastet werden und die Leistung aller Volumes auf diesem Knoten beeinträchtigen. Volume-Verschiebungen können die Situation zwar verbessern, erfordern jedoch Kopien zwischen den Knoten (was freien Speicherplatz voraussetzt), und die dafür benötigte Zeit kann die Zeit für das Failback überschreiten. Außerdem wird ein verschobenes Volume

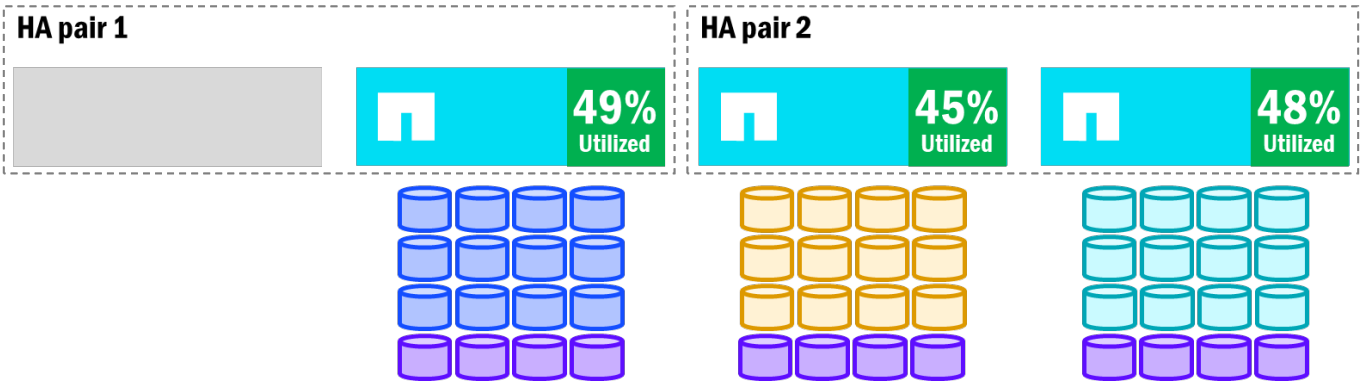
nicht auf den ursprünglichen Knoten zurückgesetzt. Stattdessen verbleibt es auf dem Knoten, auf den Sie es verschoben haben.

Mit NetApp AFX verhalten sich Knotenausfälle etwas anders.

- Da die Knoten keine eigenen Festplatten besitzen und keine physischen Aggregate existieren, erfordert ein Knotenausfall keine Übertragung dieser Ressourcen. Stattdessen werden lediglich die Netzwerkschnittstellen und der Volume-Besitz auf andere Knoten übertragen.
- NVRAM-Commits finden weiterhin statt, jedoch über das HA-Netzwerk anstatt über eine direkte Verbindung.
- Sobald die Volumes das erste Failover auf den Partnerknoten durchgeführt haben, verteilt AFX die Volumes auf die verbleibenden Knoten im Cluster neu. Dies wird durch Zero-Copy-Volume-Verschiebungen ermöglicht.
- Sobald der Knoten wiederhergestellt ist, werden die Volumes wieder auf den ursprünglichen Knoten verschoben.

NetApp AFX sorgt bereits für eine ausgewogene Leistungsverteilung über alle Knoten im Cluster hinweg, um eine relativ gleichmäßige Auslastung zu gewährleisten. Wenn also ein Failover erfolgt und die Volumes neu verteilt werden, sollte die Knotenauslastung im gesamten Cluster ungefähr gleich sein.

NetApp AFX – Volumenausgleich nach Failover



Hinzufügen und Entfernung von Knoten

Sowohl unified ONTAP als auch NetApp AFX ermöglichen das Hinzufügen und Entfernen von Knoten im Cluster. Aufgrund einiger architektonischer Unterschiede unterscheidet sich der Prozess für das Hinzufügen und die Entfernung von Knoten jedoch ein wenig.

Hinzufügen/Entfernung in Unified ONTAP

Wir haben bereits gelernt, dass Unified ONTAP eine direkte Knoten-zu-Festplatten-Zuordnung vorsieht und dass alle Knoten über einige Festplatten und mindestens ein angeschlossenes Aggregat verfügen müssen. Vor diesem Hintergrund gilt Folgendes für Hinzufügungen und Entfernungen.

- Das Hinzufügen von Knoten in unified ONTAP erfordert keine zusätzlichen Schritte, aber um eine ausgewogene Performance auf allen Knoten (einschließlich der neuen Knoten) bereitzustellen, müssten Volumes auf die neuen Knoten verschoben werden. Dies erfordert eine vorherige Analyse der vorhandenen Volumes und ihrer Workloads, Entscheidungen darüber, welche Volumes verschoben werden sollen, und dann die tatsächlichen Volume-Verschiebungen, die wiederum eine Kopie dieser Daten über das Backend-Cluster-Netzwerk erfordern würden.

- Das Entfernen von Knoten in Unified ONTAP erfordert die manuelle Evakuierung der vorhandenen Volumes auf dem Knoten, was bedeutet, dass Sie ermitteln müssen, welche Knoten welche Volumes aufnehmen können, um eine gleichbleibende Performance zu gewährleisten, und dass Sie über ausreichend freie Kapazität verfügen müssen, um einen Platz für diese Volumes bereitzustellen. Wenn freie Kapazität eine Herausforderung darstellt, können zusätzliche Volume-Verschiebungen erforderlich sein, um die Workloads im Cluster etwas zu verschieben. Das Entfernen von Knoten bedeutet auch das Entfernen von HA-Paaren, sodass sich der Arbeitsaufwand verdoppelt. Da Knoten Festplatten besitzen, ist für diese Knoten auch eine vollständige Neuinitialisierung der Festplatten erforderlich. Jede dieser Maßnahmen erhöht den Zeit- und Arbeitsaufwand für eine eigentlich relativ einfache Aufgabe.

Hinzufügen/Entfernung von Knoten in NetApp AFX

Wir haben außerdem festgestellt, dass NetApp AFX nicht die standardmäßige Zuordnung von Knoten zu Festplatten nutzt und keine physischen Aggregate zur Kapazitätsbereitstellung im Cluster verwendet. Daher verhalten sich das Hinzufügen und Entfernen von Knoten etwas anders.

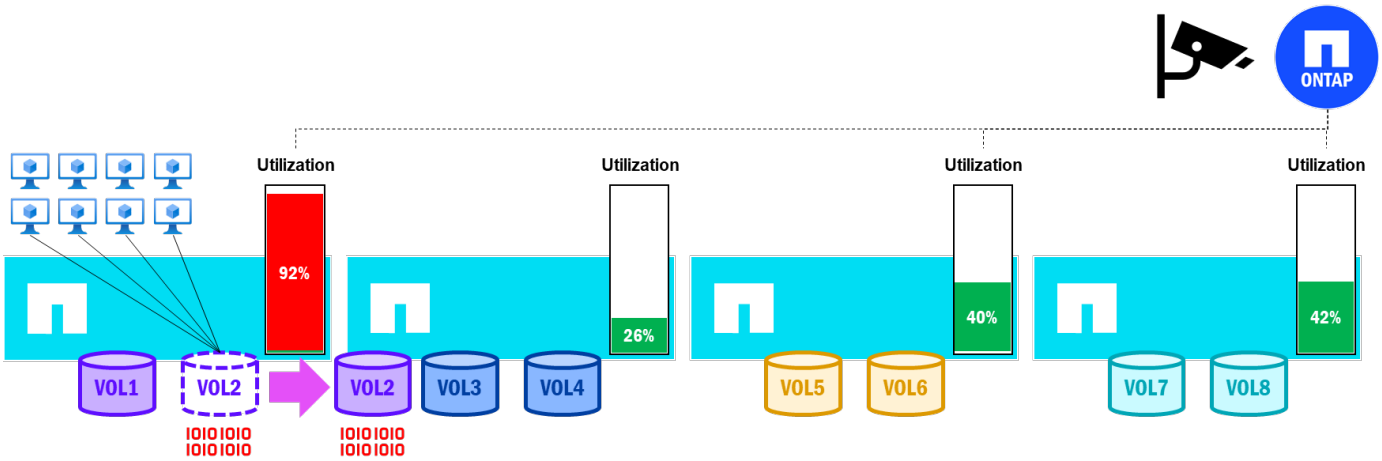
- Das Hinzufügen von Knoten in NetApp AFX erfordert weder eine vorherige Volumenanalyse noch einen administrativen Eingriff, um eine gleichmäßige Verteilung der Volumen auf die einzelnen Knoten sicherzustellen. Stattdessen gleicht ONTAP die Volumenanzahl automatisch auf den neu hinzugefügten Knoten aus, um ein möglichst gleichmäßiges Leistungsprofil zu gewährleisten. ONTAP verschiebt Volumen automatisch zwischen den Knoten, ohne etwas zu kopieren, wodurch Zeit, Kapazität und Aufwand für das Hinzufügen von Knoten zu einem Cluster reduziert werden.
- Das Entfernen von Knoten in NetApp AFX erfordert kaum oder gar keine manuelle Intervention. Wenn ein Knoten zur Entfernung markiert ist, verschiebt ONTAP die Volumes automatisch zwischen den Knoten (ebenfalls ohne Kopieren), um die zu entfernenden Knoten zu evakuieren. Und da keine Festplatten im Besitz der Knoten sind, müssen nach dem Entfernen der Knoten keine Festplatten neu initialisiert werden. Dadurch sind die Knoten in AFX modular aufgebaut und lassen sich einfach nach oben oder unten skalieren.

Performance-getriebene Volumenbewegungen

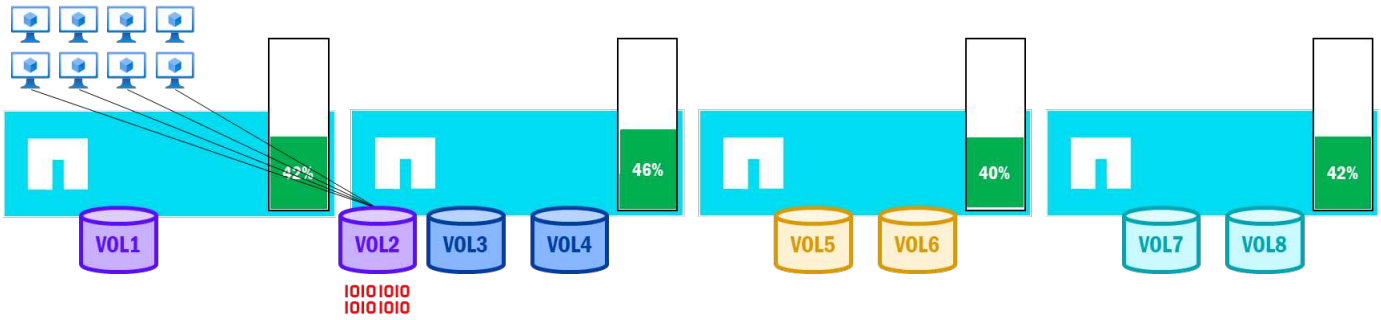
NetApp AFXs Zero-Copy-Volume-Verschiebungsfunktion bedeutet, dass es Volumes bei Bedarf neu ausbalancieren kann, ohne Daten zu kopieren, was eine schnelle Ausführung ermöglicht und keine zusätzliche Kapazität erfordert. Das bedeutet, dass Volume-Verschiebungen einen größeren Anteil am automatisierten Load Balancing verfügbar für ONTAP-Cluster ausmachen können. Da das Verschieben eines Volumes nun praktisch nichts kostet, kann ONTAP dieses wertvolle Werkzeug nutzen, um Funktionen wie Performance-getriebenes Load Balancing von Volumes zu integrieren.

In NetApp AFX mit ONTAP 9.18.1 und höher werden die Auslastung von Knoten, HA-Paaren und Volumes kontinuierlich überwacht, während Leistungsdaten erfasst und analysiert werden. Wenn die Auslastung eines Knotens außerhalb der definierten Schwellenwerte liegt, wählt ONTAP automatisch ein Volume aus, das auf einen weniger ausgelasteten Knoten verschoben wird, um eine ausgewogene Performance im gesamten Cluster zu gewährleisten.

Leistungsabhängige Volumenbewegungen in NetApp AFX – hohe Auslastung löst eine Volumenbewegung aus



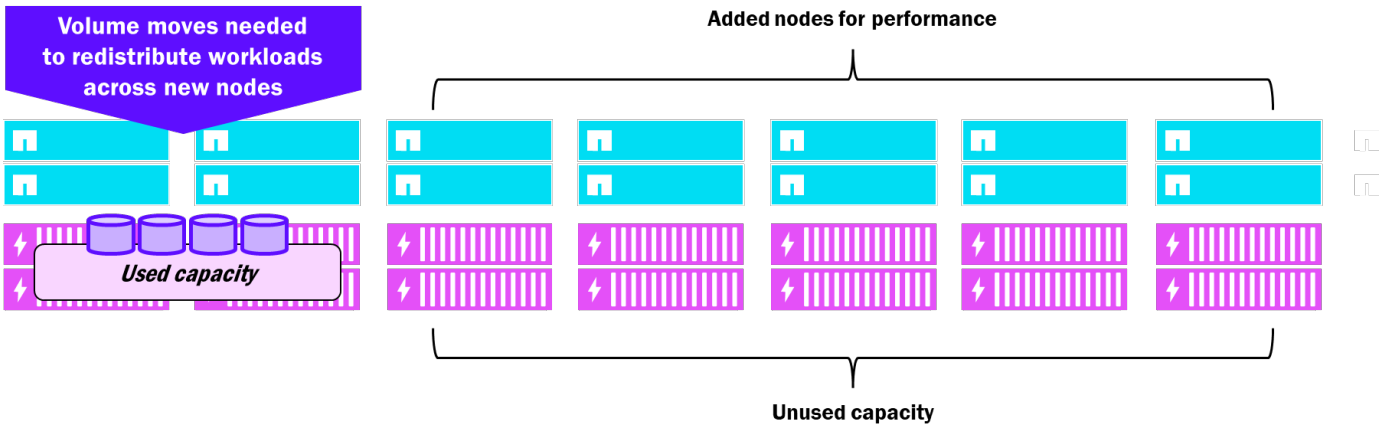
Leistungsoptimierte Volumenverschiebungen in NetApp AFX – Ausgewogene Knotenauslastung nach Volumenverschiebung



Clustergröße und -erweiterung

Unified ONTAP-Cluster unterstützen bis zu 24 Knoten und jeder hinzugefügte Knoten muss ebenfalls mit Festplatten hinzugefügt werden (sowohl für Systemfunktionen als auch für Datendienste). Festplattengehäuse können dem Cluster hinzugefügt werden, sind jedoch immer mit einem einzigen HA-Paar verbunden und gehören ausschließlich einem einzelnen Knoten, selbst wenn der Cluster 24 Knoten umfasst. Das bedeutet, dass dem Cluster Kapazität hinzugefügt wird, selbst wenn nur Leistung erforderlich ist, und dass die Leistungssteigerung größtenteils auf einen bestimmten Satz von Festplatten der neuen Knoten beschränkt ist. Dadurch kann es passieren, dass Sie über zusätzliche Kapazität verfügen, die Sie nicht unbedingt benötigen.

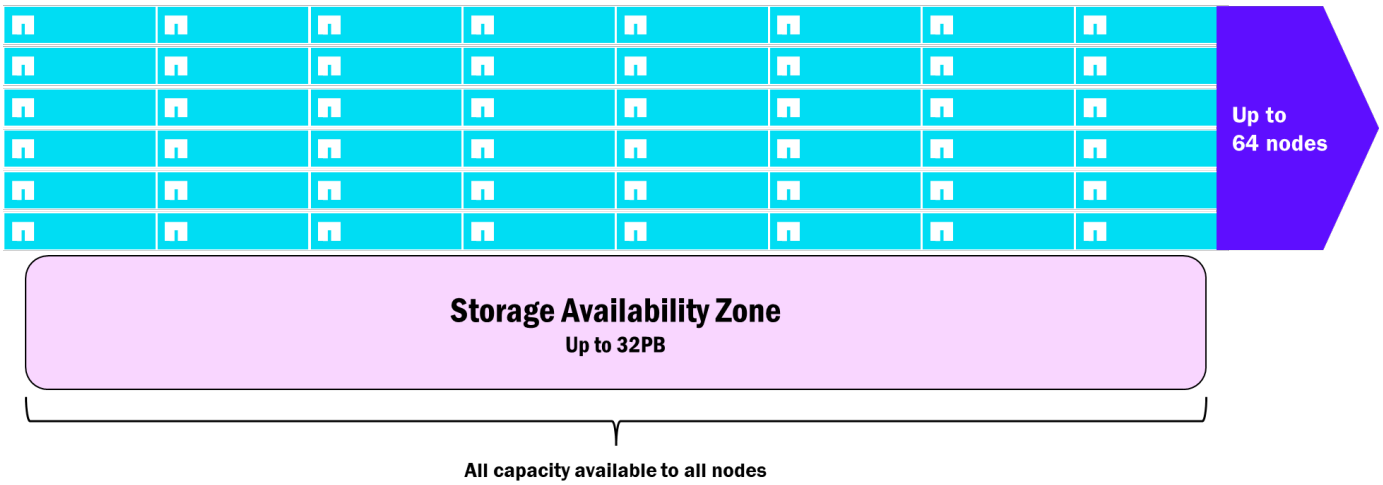
Vereinheitlichtes ONTAP – zusätzliche Skalierungsüberlegungen



NetApp AFX unterstützt größere Cluster. Ab Version 9.19.1 können AFX-Cluster bis zu 32 Knoten in einem

einzelnen Cluster umfassen. Und da alle Knoten alle Festplatten sehen und darauf zugreifen können, können sie sich die Performance und Kapazität (bis zu 32 PB ab ONTAP 9.19.1) dieser Laufwerke teilen, sodass niemals Ressourcen ungenutzt bleiben. Volume-Verschiebungen erfordern keine Kopien, sodass ONTAP Volumes automatisch auf neu hinzugefügte Knoten verschieben kann, um eine gleichmäßige Knotenauslastung sicherzustellen, während die Kapazität gleichmäßig über die Storage Availability Zone verteilt wird.

NetApp AFX – zusätzliche Skalierungsüberlegungen



Änderungen des Root-Volumes

In NetApp ONTAP wird jedem Knoten ein Root-Volume zugewiesen, das für systemspezifische Dateien und Funktionen wie Protokolldateien, Boot-Images, Core-Dateien, Cluster-Datenbanken und mehr verwendet wird.

In unified ONTAP befanden sich diese Root-Volumes auf physischen Root-Aggregaten. Um die von den Root-Aggregaten belegte Kapazität zu reduzieren, wurden sie über Datenlaufwerk-Partitionen hinweg mittels Advanced Disk Partitioning (ADP) erstellt.

NetApp AFX eliminiert physische Aggregate und macht dadurch Root-Aggregate und ADP überflüssig. Root-Volumes existieren weiterhin, befinden sich aber nun in virtualisierten Bereichen des Kapazitätspools und erfordern keine zusätzliche Konfiguration. Auch die Funktionalität von Root-Volumes ändert sich. Boot-Images und replizierte Cluster-Datenbanken werden vom Storage-Stack auf ein Onboard-Bootmedium auf jedem AFX-Knoten verschoben. Jetzt können die Knoten selbst bei einem Ausfall des Storage-Stacks weiterhin booten und ihre Cluster-Berechtigung behalten, was die Fehlersuche vereinfacht.

Onboard-Bootmedien

NetApp AFX-Knoten nutzen ein integriertes Bootmedium, eine NVMe-angeschlossene M.2-Gerät mit ca. 3,8 TB Größe. Diese Bootmedien enthalten Boot-Image-Dateien und replizierte Datenbanken, die von den Speichergehäusen getrennt sind, was zusätzliche Redundanz bei Festplattenzugriffsproblemen bietet. Fällt das Bootmedium aus, wird der Knoten von seinem HA-Partner übernommen und das Bootmedium kann ersetzt werden. Nach dem Austausch lädt ein Speicheradministrator ein neues ONTAP-Image auf das Gerät und ONTAP stellt die Cluster-Datenbank automatisch wieder her, um die volle Funktionalität wiederherzustellen.

Performance

NetApp AFX wurde mit Blick auf Leistung und Skalierbarkeit entwickelt – speziell ausgerichtet auf Workloads, die einen hohen Lese- und Schreibdurchsatz erfordern und

eine einfache, lineare Skalierung ermöglichen.

Leistung pro Knoten

Jeder NetApp AFX-Speicherknoten bietet einen bestimmten Durchsatz für Lese- und Schreibvorgänge. Mit dem Hinzufügen weiterer Knoten zum Cluster erhöht sich diese Leistung linear, wie im Abschnitt „Lineare Skalierung der Knotenleistung“ dieses Dokuments beschrieben.

Aktuell sind die Knotentypen "AFX 1K" und bieten einen Durchsatz für Lese- und Schreibvorgänge in etwa in den unten aufgeführten Mengen. Da neuere Hardware für NetApp AFX verfügbar ist, können sich diese Grenzwerte ändern. HINWEIS: Die maximale Leistung wurde durch den Einsatz mehrerer Clients beim Lesen und Schreiben mehrerer Dateien erreicht, wie im Abschnitt „Benchmark-Ergebnisse“ unten dargestellt.

Leistungsschätzungen pro Knoten

Knotentyp	Leseleistung max	maximale Schreibleistung
AFX 1K	~35GB/s	~10GB/s

Die aktuellsten Leistungsschätzungen erhalten Sie von Ihrem NetApp Vertriebsteam.

Leistung pro Regal

Jedes Shelf enthält Hochleistungs-Shelf-Module mit 16 x 100-GB-Ethernet-Ports, die RoCEv2-Kommunikation für eine hohe Bandbreite beim Datenaustausch mit den Rechenknoten im Cluster nutzen. Wie jede physische Ressource haben auch diese Shelfs Maximalwerte, die erreicht werden können – insbesondere, da NetApp AFX mehrere Knoten bereitstellen kann, die auf denselben Satz von Festplatten zugreifen. Die folgende Tabelle zeigt die geschätzte maximale Lese- und Schreibleistung für ein einzelnes Shelf für TLC- und QLC-Laufwerke. Weitere Informationen zu den Unterschieden zwischen TLC und QLC finden Sie hier "TLC vs. QLC".

Schätzungen der Leistung pro Regal

Regalmodul-Typ	Leseleistung max	maximale Schreibleistung
NSM 140	140GB/s (TLC und QLC)	70GB/s TLC 35GB/s QLC

Die aktuellsten Leistungsschätzungen erhalten Sie von Ihrem NetApp Vertriebsteam.

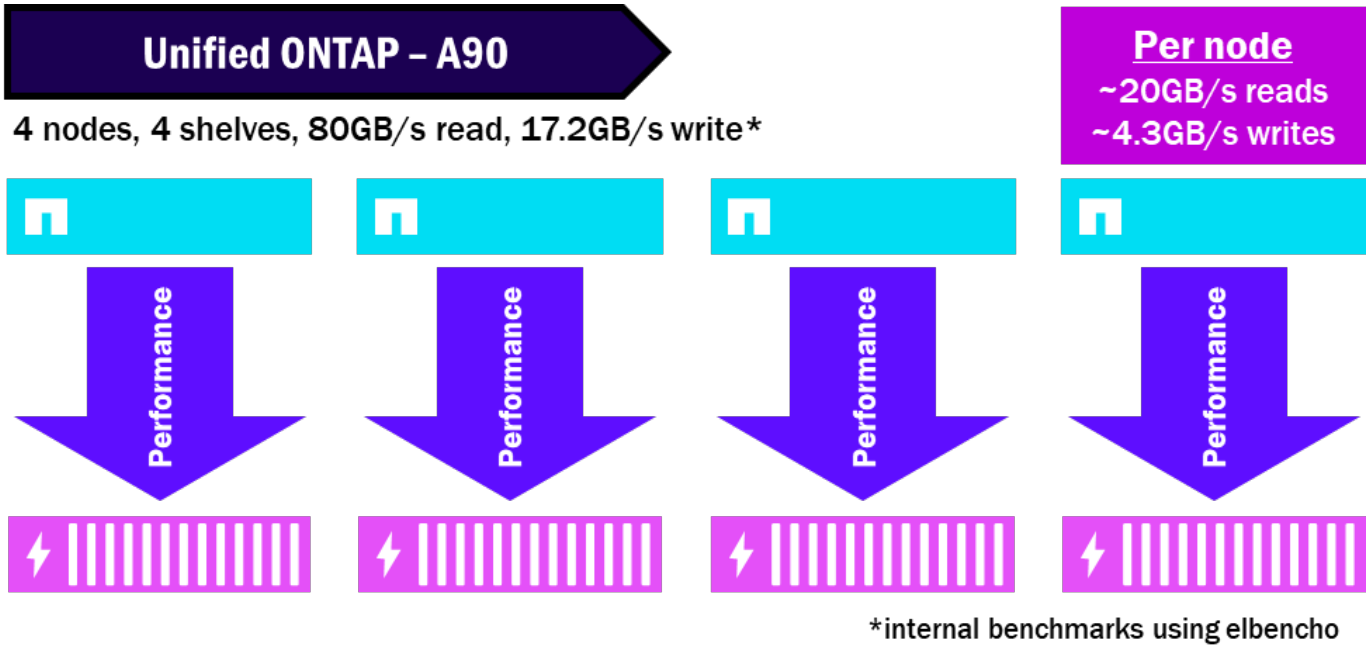
Leistungsdichte

Durch die Entkopplung der Speicherknoten von den Regalen in der disaggregierten ONTAP-Architektur können mehr Knoten den Datenverkehr auf weniger Regale leiten, was dazu beiträgt, den gesamten Platzbedarf des Rechenzentrums zu reduzieren, um mit nur der benötigten Kapazität maximale Performance zu erzielen.

Dieses Konzept der „Leistungsdichte“ ermöglicht es Speicheradministratoren, das Beste aus der vorhandenen Hardware herauszuholen, ohne ihre Speicherumgebung jemals überdimensionieren zu müssen.

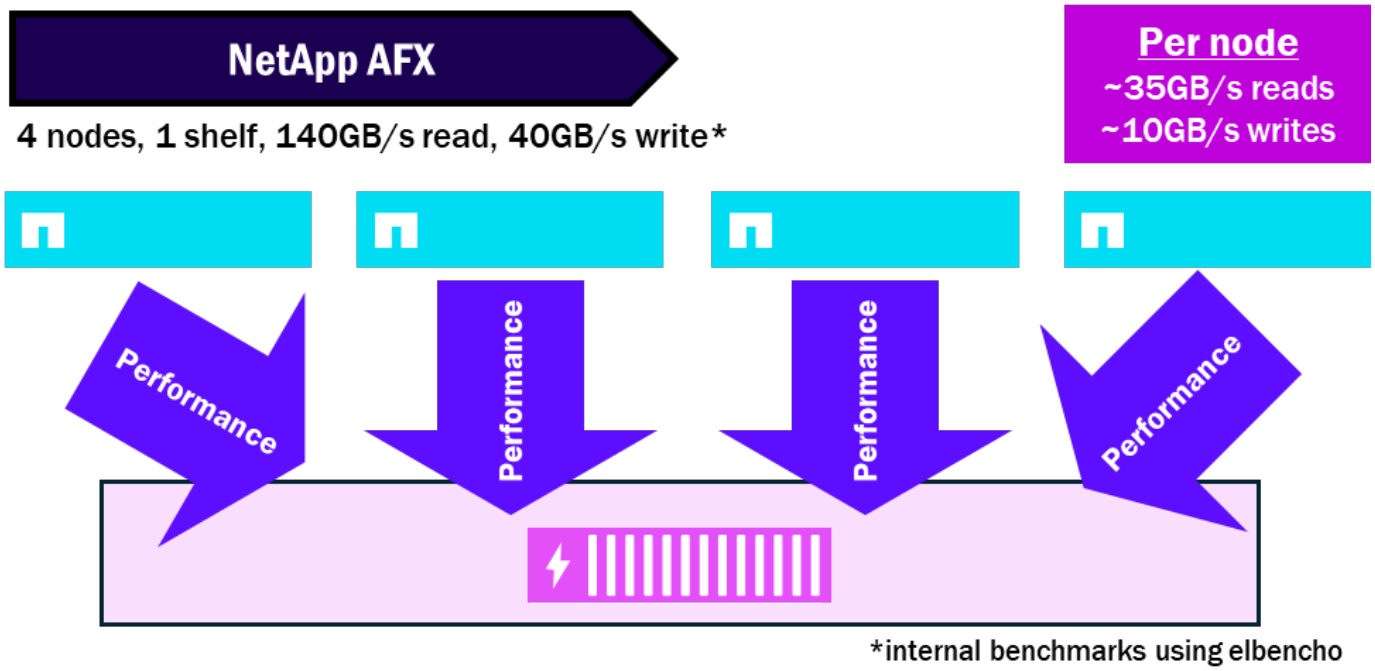
In einem einheitlichen ONTAP Cluster, da jeder Knoten über einen eigenen Satz von Festplatten verfügt, wird die Leistung nur auf die Festplatten konzentriert, die dem jeweiligen Knoten gehören, und da nur ein Knoten auf einen Satz von Festplatten zugreifen kann, kann er die verfügbaren Festplatten nicht unbedingt auslasten und seine maximale Leistung erreichen.

Unified ONTAP – Wie die Leistung aufgeteilt wird



NetApp AFX bündelt alle Festplatten in einer einzigen Storage Availability Zone, sodass alle Knoten alle Festplatten nutzen können. Und da die Festplatten und Knoten entkoppelt sind, benötigen Sie nicht so viele Shelfs, um die gleiche Performance zu erzielen. Dies verdichtet die Performance und maximiert das maximale Leistungspotenzial des Shelfs.

NetApp AFX – Leistungsdichte



Knoten-zu-Regal-Verhältnisse

Unified ONTAP-Knoten benötigen mindestens einen Festplattensatz pro Knoten und können mehrere Shelfs an einen einzelnen Knoten anschließen. Dadurch können Leistungsengpässe an einem einzelnen Knoten

auftreten, da dieser möglicherweise seine eigenen Festplatten nicht vollständig auslasten kann.

NetApp AFX stellt allen Knoten alle Festplattengehäuse zur Verfügung. Jedes Gehäuse enthält Module mit 16 x 100GB RoCE-fähigen Schnittstellen, um die maximale Leistung pro Gehäuse zu erhöhen. Dadurch können mehrere Knoten ein einzelnes Gehäuse vollständig auslasten, indem sie auf dieselben Festplatten lesen und schreiben.

Ab ONTAP 9.19.1 beträgt das node:shelf Sättigungsverhältnis etwa 4:1.

Benchmark-Ergebnisse

Im folgenden Abschnitt werden Benchmark-Ergebnisse mit einem NetApp AFX-Cluster und den folgenden Konfigurationsparametern dargestellt.

- 4 Knoten, 4 Datenschnittstellen
- 2 Regale (7,6-TB-Festplatten)
- ONTAP 9.19.1
- NFSv4.2 (pNFS, Session Trunking)
- FlexGroup-Volume
- "ElBencho"Benchmark
- Schreibvorgänge: elbencho --hosts=x.x.x.[y-z] -d -w -b 1M -t 80 --iodepth 1 --direct -s 600g /fio_vol1/
- Lesevorgänge: elbencho --hosts=x.x.x.[y-z] -r -b 256k -t 80 --lat --iodepth 2 --direct -s 600g --infloop /fio_vol1/
- 4 Cisco C240 M8 Server, 2 Port * 200GbE CX-7 Karten, 80 Threads
- NFS-Mountoptionen: rw,vers=4.2,rsize=1048576,wsize=1048576,trunkdiscovery,proto=tcp

Die oben genannte Konfiguration erreichte nahezu die maximal verfügbaren Lesevorgänge des 4-Knoten-Clusters (~134GB/s) und lag genau an den maximal zulässigen Schreibvorgängen pro Knoten (40GB/s).

NetApp AFX – ElBencho Leseleistung, 4 Knoten

NetApp AFX – ElBencho Schreibleistung, 4 Knoten

Aggressives Read-Ahead

Bei Medienstreaming-Workloads wird ein 4K-Film oft in Zehntausende von Dateien aufgeteilt, die jeweils typischerweise 50 MB bis 250 MB groß sind. Jede Datei repräsentiert ein Frame, und die Anwendung liest ein komplettes Frame in einer einzigen Anfrage. Um einen flüssigen, unterbrechungsfreien Stream ohne sichtbare

Pufferung zu gewährleisten, müssen diese Frame-Lesevorgänge ohne Aussetzer abgeschlossen werden.

ONTAP bietet eine Option auf Volume-Ebene (`-aggressive-readahead-mode`) zur Optimierung dieser Workloads. Ab ONTAP 9.19.1 wurde auf AFX ein neuer `cross_file_sequential_read` Modus für aggressives Vorlesen eingeführt, um Workloads mit vorhersehbaren E/A-Mustern bei ähnlichen Dateitypen (z. B. Medienrendering und Streaming) zu beschleunigen.

cross_file_sequential_read sagt die nächste zu lesende Datei anhand ihres Namens voraus und beginnt mit dem Vorabruf dieser Dateien, bevor der Client den Leseaufruf ausführt. Die Vorhersagelogik geht davon aus, dass alle Dateien in einem Verzeichnis einem Namensmuster mit monoton steigender numerischer Endung folgen (z. B. Datei1, Datei2, Datei3). Alle Dateien im Verzeichnis müssen diesem Muster entsprechen, wobei entweder die Dezimal- oder die Hexadezimalnummerierung verwendet wird. Dateinamen dürfen bis zu 255 Zeichen lang sein. Die Logik ist unabhängig von der Dateinamenerweiterung und generiert die nächsten Dateinamen im aktuellen Verzeichnis ausschließlich anhand des aktuellen Dateinamens. Existiert ein zuvor mit Dezimalzahlen generierter Dateiname nicht im Verzeichnis, werden die Namen mit Hexadezimalzahlen neu generiert. Existiert keiner der generierten Dateinamen, wird für diese Gruppe kein Vorabruf durchgeführt. Der Vorabruf wird fortgesetzt, sobald der nächste Leseaufruf des Clients erfolgt.

Mit diesen aktivierten Optionen "Frametest" konnten Leistungsbenchmarks 30.000 4K-Frames mit 30 Bildern pro Sekunde mit 30 Clients (NFSv3 und SMB3) und 34 Clients (NFSv4.1) lesen, ohne dass ein einziger Frame verloren ging.

Während sequenzielles Lesen über mehrere Dateien hinweg primär für Medien-Workloads konzipiert ist, können auch andere leseintensive Workloads mit vorhersehbaren Zugriffsmustern und Dateinamen – wie beispielsweise AI-Training und -Inference – davon profitieren.

Überlegungen und Vorbehalte

- Gemeinsamer Puffer-Cache – Aggressives Vorlesen nutzt denselben Puffer-Cache wie andere Volumes auf dem Knoten. Die Aktivierung kann die Leseleistung anderer Volumes auf diesem Knoten beeinträchtigen.
- Zugrundeliegende Speicherleistung – Wenn Dateien nicht schnell genug gelesen werden können (z. B. auf HDD-basierten FAS-Systemen), können zwischengespeicherte Daten verdrängt werden, bevor der Client-Lesevorgang stattfindet, wodurch die Vorteile des sequenziellen Lesens zunichte gemacht werden.
- Anforderungen an das Zugriffsmuster – Wenn das Lesemuster der Arbeitslast nicht sequenziell ist oder wenn die Dateien in einem Verzeichnis nicht in aufsteigender sequenzieller Reihenfolge benannt sind, bietet der aggressive Lesevorlaufmodus cross_file_sequential_read keine nennenswerten Vorteile.

Leistungsverbesserungen in NFSv4.x

NFS Version 3 gilt seit Jahrzehnten als Goldstandard für NFS-Anwendungen – seit seiner offiziellen Veröffentlichung im Jahr 1995. Die Kombination aus Leistung und Ausfallsicherheit macht einen Wechsel zu neueren NFS-Versionen aus gutem Grund schwierig.

NFSv3 hat jedoch auch seine Grenzen. Die Zustandslosigkeit des Protokolls ist zwar vorteilhaft für die Leistung und minimiert Unterbrechungen bei einem Speicherausfall, aber weniger vorteilhaft für die Datenkonsistenz und das Sperrenmanagement. Ein NFS-Server speichert keine Sperrzustände, daher kann der NFS-Server im Fehlerfall die Sperren freigeben oder auch nicht, und der NFS-Client weiß möglicherweise nicht, ob eine Datei gesperrt ist oder nicht.

```
 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^]).
Obwohl NFSv4.x schon seit über 20 Jahren existiert, hat es aus
verschiedenen Gründen noch keine breite Akzeptanz gefunden.
```

- Komplexität des Identitätsmanagements: In vielen Umgebungen ist keine Namensdienstinfrastruktur vorhanden, um die Namenszeichenfolge und die Kerberos-Sicherheitsanforderungen in NFSv4.x richtig nutzen zu können.
- Bedarf an neueren NFS-Clients: Dieses Problem ist in modernen NFS-Umgebungen heutzutage weniger dringlich, je weiter wir uns vom ursprünglichen Veröffentlichungsdatum von NFSv4 entfernen. Fast alle aktuell verwendeten Betriebssysteme beinhalten NFS-Clients mit vollständiger NFSv4-Unterstützung, aber es gibt noch ältere Systeme, denen die notwendigen NFSv4.x-Pakete fehlen. Tatsächlich benötigen einige Anwendungen weiterhin ältere NFS-Versionen.
- Die Mentalität „Was nicht kaputt ist, muss man nicht reparieren“: IT-Organisationen in Unternehmen sind bekanntermaßen sehr konservativ, wenn es um die Einführung neuerer Technologien geht – selbst solcher, die schon seit über 20 Jahren existieren. Und wenn die aktuelle NFS-Version einwandfrei funktioniert, warum ändern?
- Leistungsbedenken: Die Leistung eines zustandsbehafteten Protokolls wie NFSv4.x blieb in den letzten 20 Jahren weitgehend hinter der des zustandslosen NFSv3 zurück. In der Vergangenheit überwogen die Leistungseinbußen oft die Vorteile von NFSv4.x.

NFSv4.x-Verbesserungen in ONTAP 9.18.1 mit AFX

Einige architektonische Änderungen an ONTAP haben der NFS-Performance im Allgemeinen einen dringend benötigten Schub gegeben und zu einer deutlichen Verbesserung der NFSv4.x-Performance im Allgemeinen beigetragen.

Nachfolgend eine kurze Zusammenfassung einiger dieser Änderungen.

Verbesserung des sequenziellen Lesens: NFSv4.1 30 % besser als NFSv3

ONTAP 9.18.1 führt die Unterstützung für Multipath-IO mit NFSv4.1 ein. Anstatt Lesevorgänge vom WAFL-Dateisystem zu verarbeiten, verlagert MPIO diese in eine Netzwerkdomäne, um sie multipath-sicher zu bedienen. Dieser Ansatz reduziert Kontextwechsel, ermöglicht eine höhere Parallelität im sequenziellen Leseverkehr und verringert den Aufwand für die Pufferverwaltung durch Umgehung von WAFL.

Verbesserung der zufälligen Lesegeschwindigkeit für FlexGroup volumes: NFSv4.1 innerhalb von 7 % von NFSv3

FlexGroup Volumes sind Volumes, die aus mehreren Teilvolumes zusammengesetzt sind und diese als einen einzigen, einheitlichen Namensraum darstellen. In AFX sind bei FlexGroup Volumes die erweiterte Kapazitätsverteilung standardmäßig aktiviert, wodurch Dateien, die größer als 10 GB sind, als Multipart-Dateien auf mehrere Teilvolumes verteilt werden. Aufgrund der räumlichen Trennung dieser Dateiteile war die Leistung bei zufälligen Lesezugriffen mit NFSv4.x traditionell etwas geringer (ca. 18 % weniger als mit NFSv3). ONTAP 9.18.1 führt die Unterstützung für zwischengespeicherte IO bei Multipart-Lesezugriffen mit NFSv4.x

ein, um dieses Problem zu beheben. HINWEIS: Diese Änderung betrifft nicht FlexVol Volumes.

Sequenzielles Schreiben: +10 % Verbesserung gegenüber früheren Versionen

Eine Verbesserung der Replikation von NVLOG-Daten, die für die HA-Failover-Funktionalität verwendet werden, steigerte die gesamte sequenzielle Schreibperformance von NetApp AFX-Systemen.

Metadatenoperationen: Innerhalb von 15 % der Leistung von NFSv3 bei EDA-Benchmarks

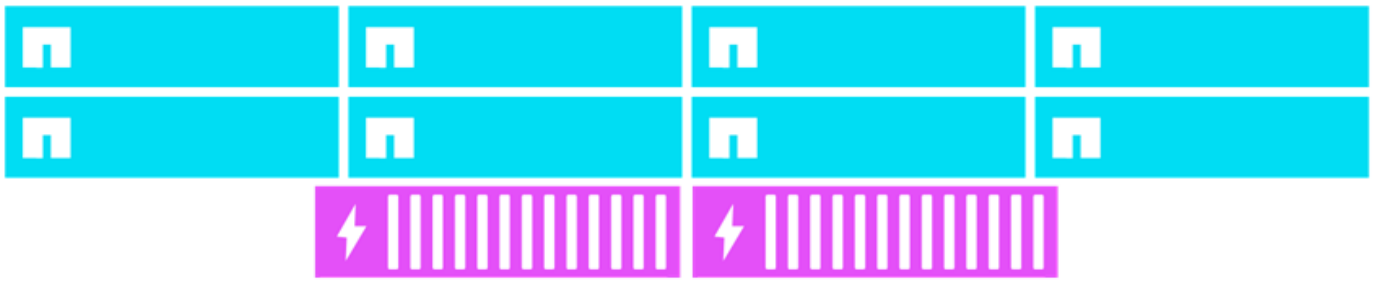
NFSv4.1 serialisiert traditionell alle OPEN- und CLOSE-Operationen, wobei ein Clusterknoten sie nacheinander verarbeitet, bevor sie vom Netzwerk an WAFL gesendet werden. ONTAP 9.18.1 führt Concurrent Open Close (COC) ein, wodurch die Netzwerkserialisierung durch eine geänderte Behandlung von Race Conditions entfällt, was die in früheren Versionen aufgetretenen OPEN/CLOSE-Engpässe beseitigt.

All diese Änderungen – zusammen mit den in AFX vorgenommenen Architekturänderungen – haben es ermöglicht, die Gesamtleistung von NFSv4.1 in ONTAP 9.18.1 zu verbessern.

Ergebnisse sequenzieller Ein-/Ausgabe

Einer der Bereiche, in denen einige moderate Leistungsverbesserungen festgestellt wurden, war bei sequenzieller IO (d. h. IO, die vorhersehbar ist und nacheinander ausgeführt wird). In Standard-Leistungstests mit fio verbesserte AFX unter ONTAP 9.18.1 die sequenzielle Leseleistung um fast 30 % und die sequenzielle Schreibleistung um 10 %.

NetApp AFX – NFSv4.1 sequenzielle IO-Leistung in ONTAP 9.18.1



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

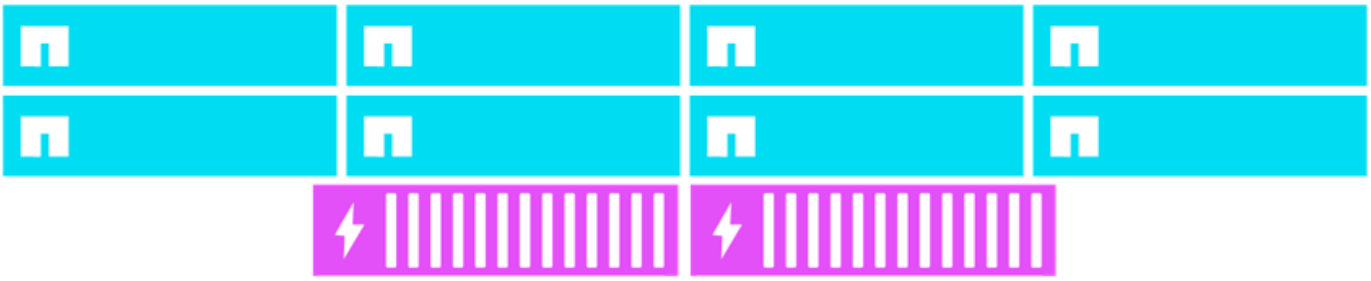
Ergebnisse von Arbeitslasten mit hohem Metadatenaufkommen

Noch beeindruckender sind die Verbesserungen bei einem der größten Leistungsengpässe von NFSv4.x – den Metadaten. Dabei handelt es sich um zufällige IOs, üblicherweise im 4K-Bereich, die zur Verwaltung von Dateibesitzern und -attributen, zum Erstellen und Auflisten von Dateien usw. verwendet werden. Aufgrund der Zustandsabhängigkeit von NFSv4.x sind diese Arten von Operationen tendenziell rechenintensiver und latenzbehafteter, was wiederum die insgesamt mögliche Leistung reduziert.

Mit den Änderungen in AFX ONTAP 9.18.1 hat sich die Leistung von NFSv4.x für diese Art von Arbeitslasten erheblich verbessert und die Lücke zur Leistung von NFSv3 (innerhalb von 15%) geschlossen.

Unsere Performance-Engineering-Teams verglichen die Leistung von Standard-Benchmarks für KI-Bild, EDA und Software-Builds und stellten massive Verbesserungen gegenüber der vorherigen ONTAP Version fest.

NetApp AFX – NFSv4.1 Metadaten-IO-Leistung in ONTAP 9.18.1



	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%

Management-Tools

Obwohl es in der Darstellung des Speichers in NetApp AFX einige recht große architektonische Unterschiede gibt, sind der Funktionsumfang und die Verwaltung von ONTAP praktisch unverändert. Dies ist so beabsichtigt. ONTAP ist ONTAP und der Lernaufwand sollte möglichst gering sein. Und in diesem Fall läuft NetApp AFX weiterhin mit ONTAP.

Verwaltung – CLI

In NetApp AFX ist die CLI nahezu identisch mit der von unified ONTAP angebotenen CLI. Befehle werden größtenteils weiterhin auf Clusterebene ausgeführt, während es weiterhin Befehle auf Knotenebene gibt, die ausgeführt werden können. Es gibt weiterhin Befehlsverzeichnisse der obersten Ebene und Unterbefehle sowie die Tab-Vervollständigung von Befehlen. Darüber hinaus funktionieren alle gleichen CLI-Kurzbefehle (zum Beispiel das Filtern von Inhalten mit `-fields`).

Die einzigen wesentlichen Unterschiede in der NetApp AFX-CLI betreffen die hinzugefügten und entfernten Funktionen (wie im Abschnitt „“ dieses Dokuments beschrieben). Wurde eine Funktion (z. B. Aggregate oder Metrocluster) entfernt, ist der entsprechende CLI-Befehl nicht mehr verfügbar.

Darüber hinaus werden, wenn neue Funktionen und Features zu NetApp AFX hinzugefügt werden, auch neue Befehle verfügbar sein. Beispielsweise interagiert das neue "NetApp AI Data Engine (AIDE)" Add-on direkt mit einem NetApp AFX-Cluster über das Backend-Cluster-Netzwerk. Infolgedessen werden die `dcn` und `data-engine` Befehlsverzeichnisse zur NetApp AFX-CLI hinzugefügt.

Die folgende Liste zeigt die obersten Befehlsverzeichnisse, die mit Administratorrechten in einem NetApp AFX-

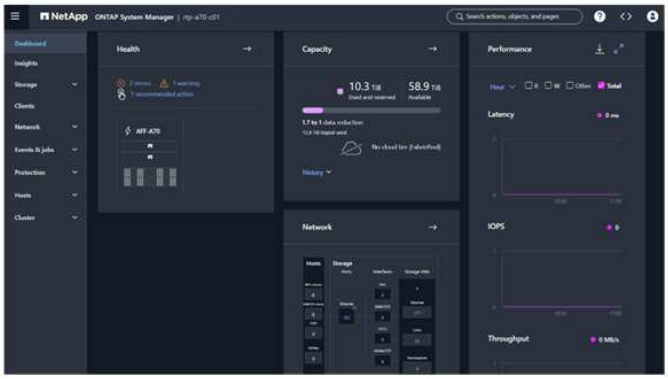
Cluster verfügbar sind. Neu hinzugefügte Befehle sind fett hervorgehoben.

```
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
```

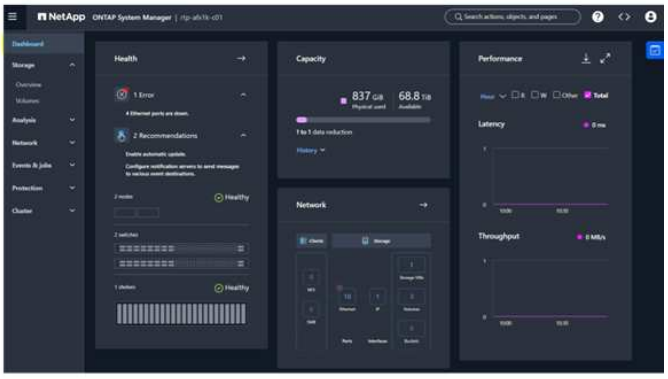
Verwaltung – GUI

Der System Manager ist nach wie vor die grafische Benutzeroberfläche zur Interaktion mit NetApp AFX-Clustern für die Ressourcenverwaltung, und beim ersten Anmelden werden Sie wahrscheinlich auf den ersten Blick nicht erkennen, dass Sie nicht mehr in einem einheitlichen ONTAP System angemeldet sind.

Vergleich der einheitlichen ONTAP- und NetApp AFX System Manager-Startseiten nebeneinander



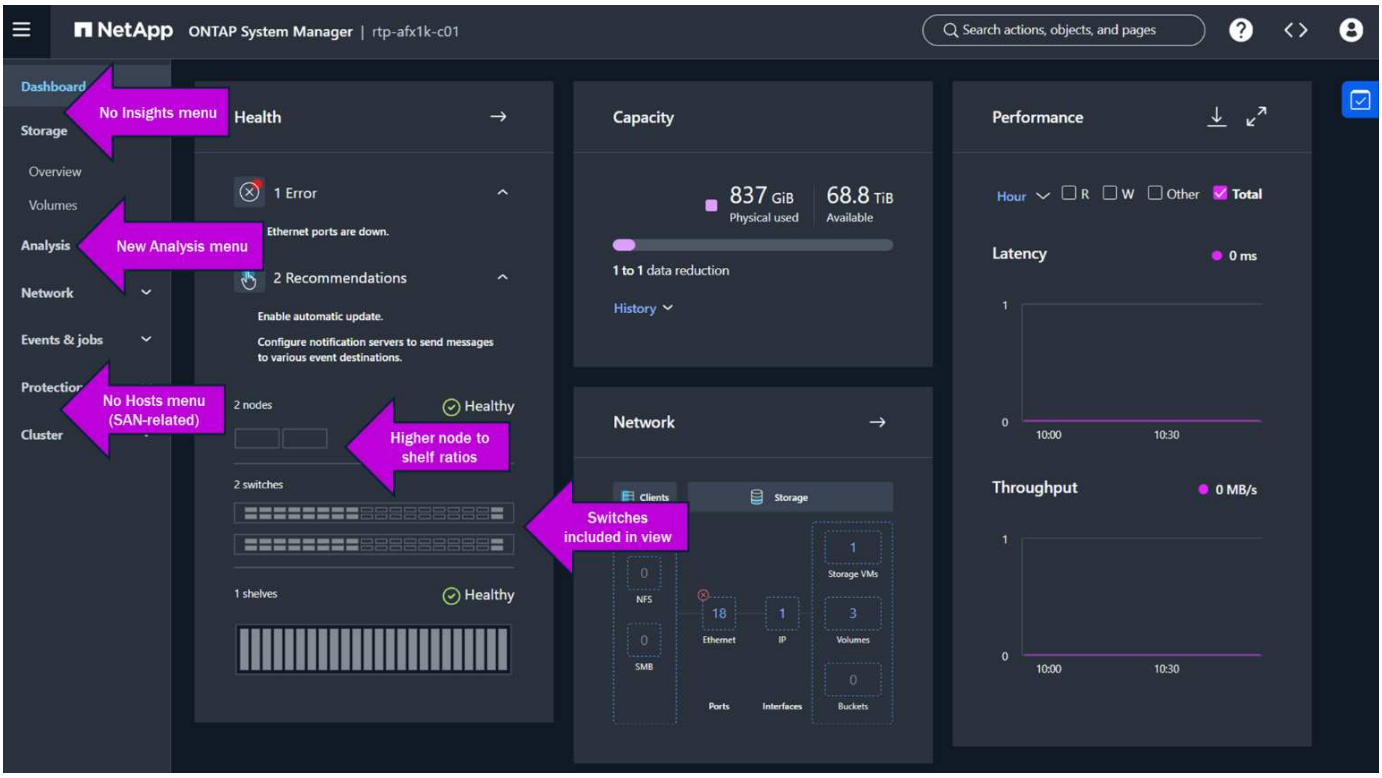
System Manager Dashboard view
Unified ONTAP



System Manager Dashboard view
NetApp AFX

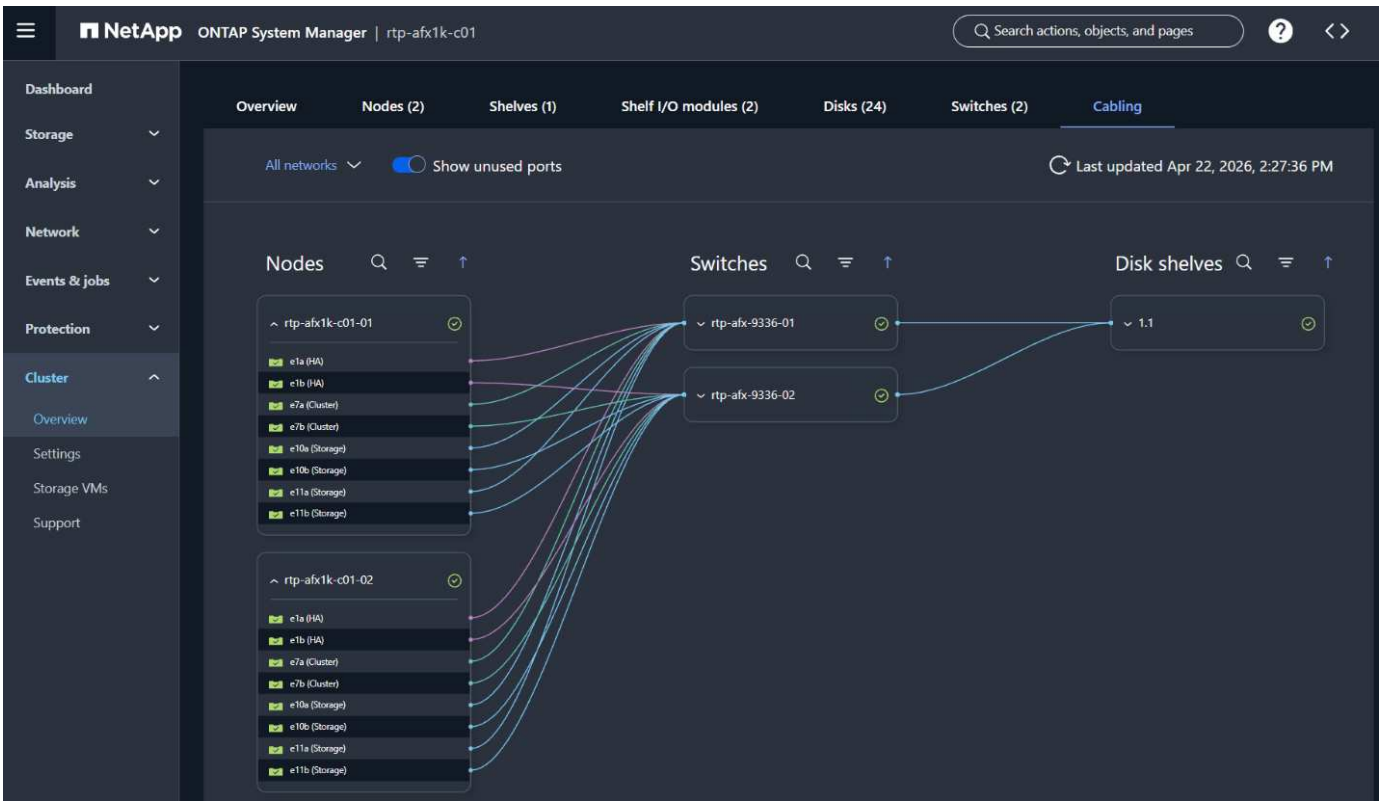
Wie Sie oben sehen können, gibt es im System Manager für Unified ONTAP und NetApp AFX nicht viele offensichtliche Unterschiede. Es gibt jedoch einige Hinweise.

Wie sich NetApp AFX im System Manager unterscheidet



Beim Navigieren durch Menüs und Dashboards bleibt fast alles unverändert. Volumes zeigen weiterhin die belegte und die Gesamtkapazität an. Netzwerkschnittstellen zeigen weiterhin Ports und IP-Adressen an. Sie können weiterhin Schutzrichtlinien für SnapMirror konfigurieren. Hardwareansichten sind weiterhin verfügbar. Aber NetApp AFX erweitert die Ansichten auch ein wenig, indem es eine neue Verkabelungsansicht bietet, in der Sie detailliert sehen können, wo alle Kabel im gesamten Speichersystem angeschlossen sind.

NetApp AFX-Kabelansicht



REST-APIs

NetApp AFX ist ebenfalls bestrebt, die Mehrheit der ONTAP REST API-Aufrufe beizubehalten, was bedeutet, dass, wenn Sie eine Suite von Automatisierungstools auf Basis der REST API erstellt haben, diese in den meisten Fällen weiterhin verwendet werden können. Die wichtigsten Ausnahmen umfassen Aggregate, Metrocluster, SAN und einige Leistungsindikatoren. Die vollständige REST API-Dokumentation finden Sie im System Manager des NetApp AFX-Clusters, indem Sie zu https://clus_mgmt_ip/docs/api navigieren.

Off-Box ONTAP Verwaltungstools

NetApp AFX bietet Unterstützung für externe ONTAP-Verwaltungstools, wie zum Beispiel:

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

NetApp AFX unterstützt derzeit Folgendes nicht:

- NetApp ActiveIQ Unified Manager

Netzwerk, Sicherheit und Betrieb

NetApp AFX unterstützt denselben Netzwerk-Stack, dieselben Sicherheitsfunktionen, Datenschutztechnologien, unterbrechungsfreie Betriebsabläufe und Volumentypen wie unified ONTAP, mit einigen Anpassungen, die speziell für die disaggregierte Architektur gelten.

Netzwerkbetrieb

Der Netzwerk-Stack in NetApp AFX ist identisch mit dem von unified ONTAP.

- Data LIFs werden weiterhin verwendet, um internen und externen Diensten Netzwerkadressen bereitzustellen.
- Jeder Knoten verfügt über einen eigenen Satz physischer und virtueller Ports.
- VLANs, ifgroups und BGP werden weiterhin unterstützt.
- LIFs können weiterhin zwischen physischen Knoten und Ports im Cluster umschalten.
- IPspaces/Broadcast-Domänen sind weiterhin gleich konfiguriert.
- Jede SVM kann über ein eigenes dediziertes Datennetzwerk verfügen.
- Managementnetzwerke können von Datennetzwerken getrennt werden.
- Abgesehen von der neuen Unterstützung für 400-GB-Netzwerke ändert sich an den Client-Datennetzwerken nichts.
- Backend-Cluster-Switches werden weiterhin über eine von NetApp bereitgestellte „golden configuration“-Datei konfiguriert.

Zu den wichtigsten Netzwerkunterschieden gehören:

- Die Backend-Cluster-Netzwerkports unterstützen jetzt nur noch 100-GB-Verbindungen zu den Cluster-Switches.

- Da die Cluster-Switches 400GB-fähig sind, verwenden die Backend-Knotenverbindungen 4 x 100GB Breakout-Kabel, um die Anzahl der an den Switches verwendeten Ports zu reduzieren.
- NVRAM wird nun über eine neue HA-VLAN-Konfiguration auf den Switches zwischen HA-Paaren im Backend-Cluster-Netzwerk gespiegelt.
- Ein neues DCN-Netzwerk wird standardmäßig für die AI Data Engine hinzugefügt. Diese IP-Adressen werden automatisch generiert und können bei Bedarf geändert werden.

Sicherheit

NetApp AFX läuft auf ONTAP, was bedeutet, dass es dieselbe Sicherheit wie ONTAP verwendet. Alle Kryptomodule sind identisch, was bedeutet, dass die Sicherheitszertifizierungen identisch sein werden, sobald die Zertifizierungsprozesse abgeschlossen sind. NetApp AFX nutzt außerdem dieselbe Unterstützung für Sicherheitsverschlüsselungen wie das einheitliche ONTAP.

Darüber hinaus unterstützt NetApp AFX viele der Sicherheitsfunktionen von unified ONTAP, einschließlich (aber nicht beschränkt auf):

- Autonomer Schutz Durch Ransomware
- Sichere Mandantenfähigkeit
- Verschlüsselung ruhender Daten (Volume-Verschlüsselung) und während der Übertragung (TLS 1.3)
- Selbstverschlüsselnde Laufwerke (SEDs)
- NFS- und SMB-Kerberos-Authentifizierung und -Verschlüsselung
- Überprüfung durch mehrere Administratoren
- SnapLock

Informationen darüber, welche Zertifizierungen unified ONTAP erhalten hat (sowie weitere Informationen zur Sicherheitshärtung), finden Sie hier:

- "NetApp Produktsicherheit"
- "Übersicht über die Erhöhung der Sicherheit durch ONTAP"

Snapshots und Datenschutz

NetApp AFX nutzt dieselben Snapshot- und Replikationstechnologien wie unified ONTAP, ohne dass sich die Funktionsweise dieser Features wesentlich ändert. Tatsächlich kann AFX mit unified ONTAP Systemen auf dieselbe "Regeln und Konfigurationen" Weise replizieren, wie Sie es gewohnt sind.

Die einzige Ausnahme bei der Replikation in AFX betrifft FlexGroup-Volumes, die auf ein einheitliches ONTAP-System repliziert werden. In diesem Fall muss das Zielsystem mit ONTAP 9.16.1 oder höher ausgeführt werden, um die Unterstützung für Advanced Capacity Balancing bereitzustellen.

Unterbrechungsfreier Betrieb

ONTAP ermöglicht unterbrechungsfreie Vorgänge wie Datenträgerverschiebungen, Upgrades, Clusterwartung, Speicherausfallsicherungen und mehr. NetApp AFX bietet dieselben unterbrechungsfreien Vorgänge, jedoch mit einigen Anpassungen.

- Volumenverschiebungen erfolgen weiterhin unterbrechungsfrei, erfordern aber keine Kopie mehr.
- Speicherausfälle erfolgen weiterhin unterbrechungsfrei, aber nach dem ersten Ausfall werden die Volumes auf alle verbleibenden Knoten im Cluster neu verteilt.

- LIF-Migrationen sind identisch.
- Hardwarewartung und -aufrüstungen sind identisch.

Volumentypen

Unified ONTAP unterstützt verschiedene Volume-Typen, wie zum Beispiel:

- FlexVols
- FlexGroup Volumes
- FlexCache
- FlexClone
- Objekt-Buckets

NetApp AFX bietet volle Unterstützung für jeden dieser Volume-Typen sowie volle Interoperabilität für FlexCache-Volumes mit einheitlichen ONTAP-Systemen.

Weitere Informationen darüber, wie FlexGroup Volumes von der AFX-Architektur profitieren, finden Sie unter "Verbesserungen beim FlexGroup Volume-Management".

Hardware-Details

Der folgende Abschnitt enthält Details zur NetApp AFX-Cluster-Hardware. Aktuelle Informationen zur NetApp AFX-Hardware finden Sie unter "https://hwu.netapp.com".

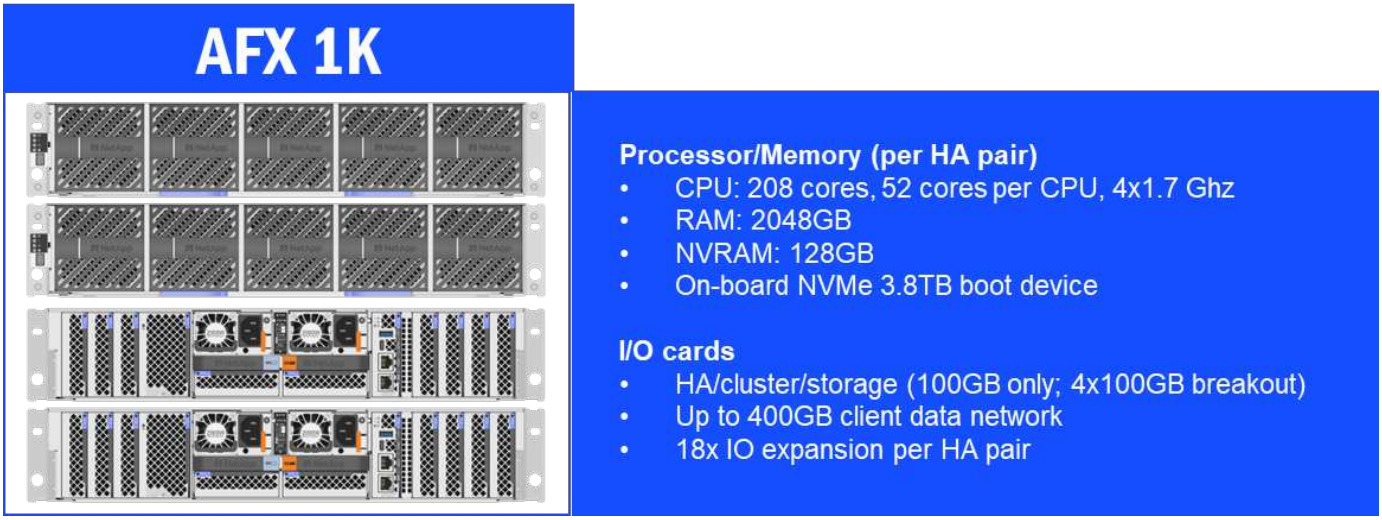
Unterstützte Hardware

Die aktuellsten Informationen zur unterstützten Hardware für NetApp AFX finden Sie unter "https://hwu.netapp.com".

Nodes

NetApp AFX-Knoten basieren auf dem AFF A1K-Knotenmodell für Unified ONTAP Cluster. Diese Knoten verfügen über keine internen Festplatten und sind modular aufgebaut, um je nach Leistungsbedarf einfach Knoten hinzufügen oder entfernen zu können. Jeder Knoten belegt 2 HE im Rack und die Leistung steigt linear mit der Anzahl der Knoten in einem AFX-Cluster.

NetApp AFX 1K-Knotendetails



Hardware-Steckplätze

NetApp AFX 1K-Knoten verwenden die folgenden Slot-Zuweisungen.

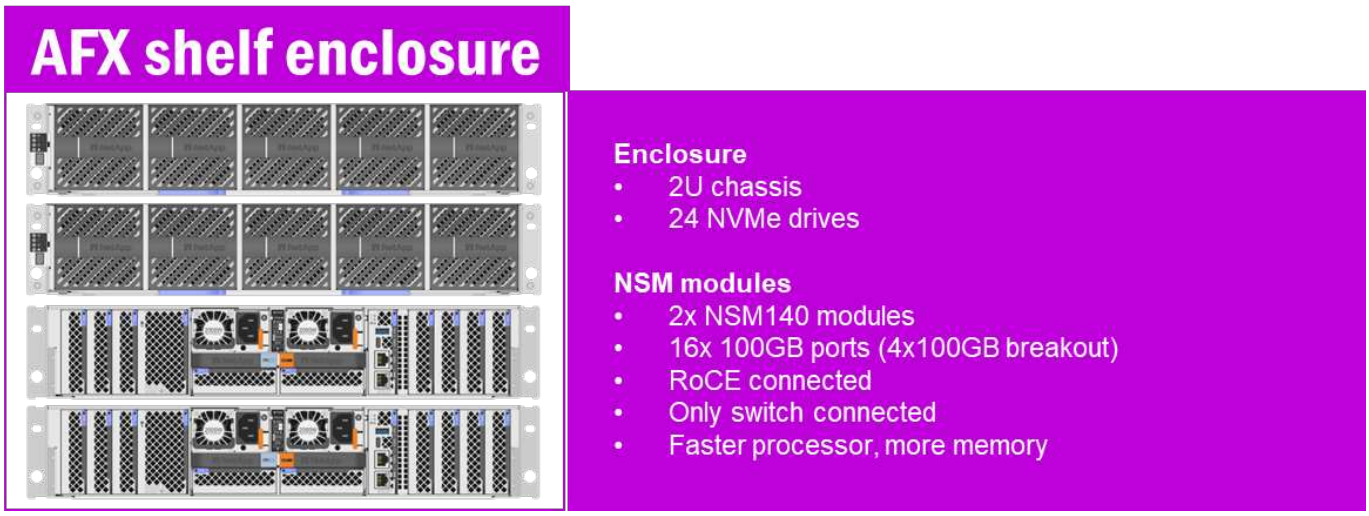
- Steckplatz 1 ist für die HA-Replikation vorgesehen
- Steckplatz 7 ist für die Clusterreplikation vorgesehen
- Die Steckplätze 10 und 11 sind für die Kommunikation mit dem Storage-Shelf vorgesehen

Shelfs

NetApp AFX-Einschübe verwenden dieselben Gehäuse wie die AFF-Systeme. Der Hauptunterschied zwischen den Einschüben in AFX liegt im verwendeten Modul. Die NSM140-Module bieten verbesserte Leistungsmerkmale und ermöglichen disaggregiertes ONTAP. Einige wichtige Punkte:

- Nur vollständig bestückte Regale werden unterstützt.
- Die Regale werden von NetApp AFX automatisch erkannt, sobald sie angeschlossen sind.
- Derzeit wird keine Unterstützung für die Regalentfernung angeboten.

NetApp AFX-Regalgehäusedetails

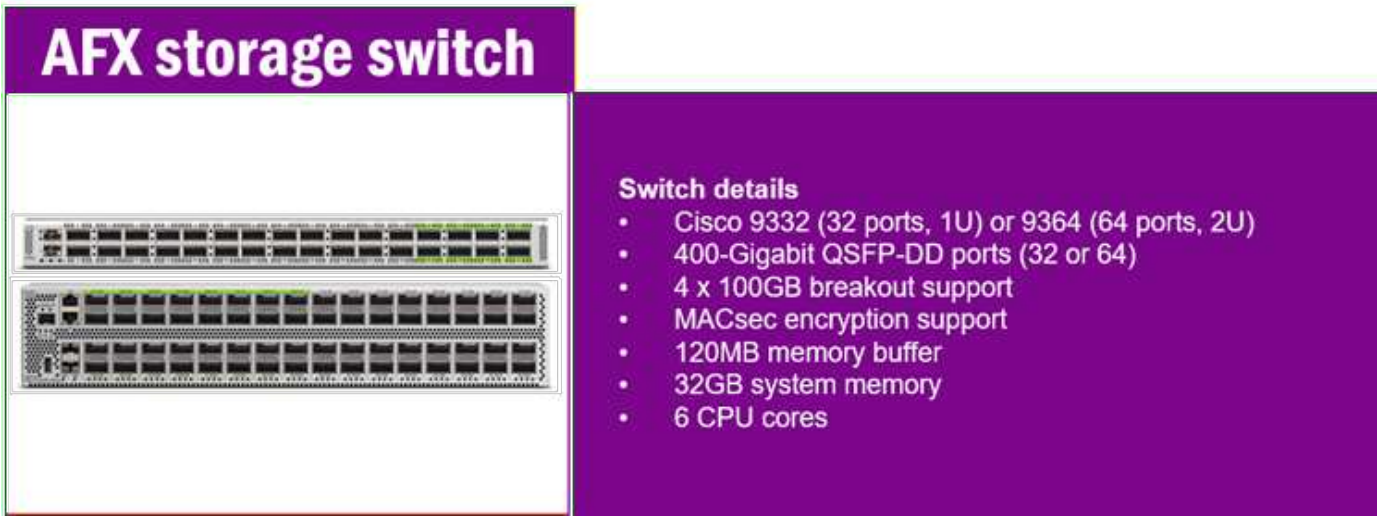


Switches

NetApp AFX nutzt weiterhin Backend-Cluster-Switches für die Intracluster-Kommunikation, wie zum Beispiel die Cluster-Datenbankreplikation, Remote-Datenoperationen, Speicheroperationen und NVRAM-Spiegelung. Funktional bestehen die einzigen Unterschiede zwischen Unified ONTAP und NetApp AFX Cluster-Switches darin:

- 400GbE-Unterstützung
- Neues HA-VLAN
- Weitere Informationen finden Sie unter "Cisco Switches Datenblatt".

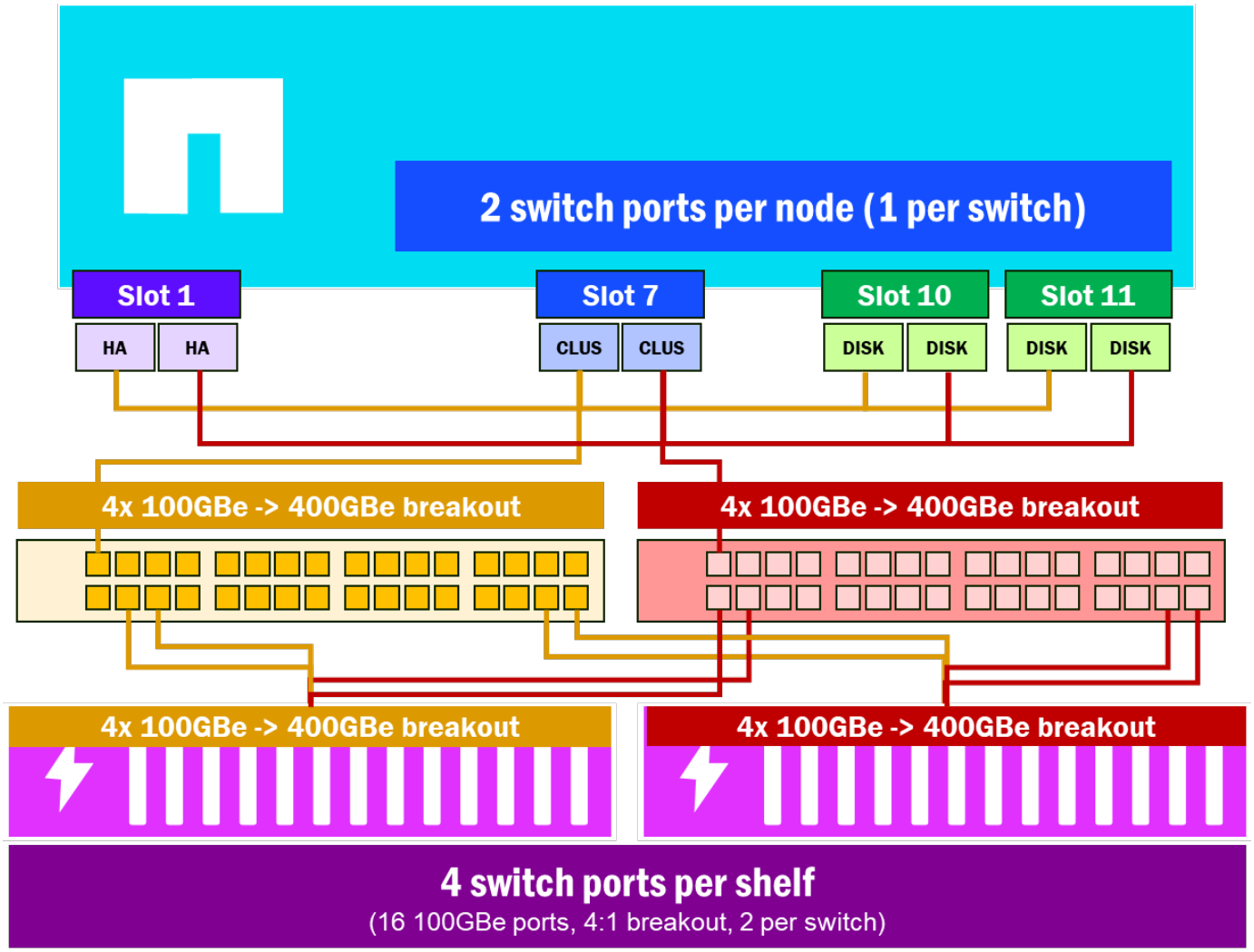
NetApp AFX-Clusterschalter



Cluster-Switch-Konnektivität

NetApp AFX nutzt Backend-Cluster-Switches intensiv für viele seiner zentralen Architekturkonzepte. So werden beispielsweise Cluster-Schnittstellen, Speicheradapter, Speichershelfs und NVRAM-Karten an die Cluster-Switches angeschlossen. Aktuell unterstützen all diese Schnittstellen nur 100GB-Kommunikation, während die Switches 400GB unterstützen. Daher werden die 100GB-Schnittstellen über 4 x 100GB-Breakout-Kabel mit den 400GB-Schnittstellen des Switches verbunden. Dadurch wird die Anzahl der Ports an den Switches reduziert. Beispielsweise belegen 16 x 100GB-Speichershelf-Modul-Ports nur 4 Ports an den Switches, während die insgesamt 8 Ports der Nodes 2 Switch-Ports nutzen.

NetApp AFX-Schalterverkabelung



Festplattentypen und -größen

NetApp AFX unterstützt derzeit nur NVMe-SSDs in folgenden Größen:

- 7,6 TB
- 15,3 TB
- 30,1 TB
- 60,6 TB

TLC vs. QLC

NetApp AFX kann sowohl TLC- als auch QLC-Flashtypen nutzen. Die 7,6- und 15,3-TB-Laufwerke sind TLC-Modelle, während Laufwerke mit mehr als 30,1 TB QLC sein werden. Unabhängig vom Medientyp können die NVIDIA SuperPod Zertifizierungsleistungsstandards erfüllt werden.

Alle mit NetApp AFX verwendeten Laufwerke sind Hochleistungslaufwerke, wobei QLC und TLC beim Lesen nahezu identische Leistungen erbringen. Bei der Schreibleistung liegt QLC im Vergleich zu TLC etwas zurück und kann bei schreibintensiven Anwendungen etwas stärkeren Verschleiß aufweisen.

Die Leistungszahlen finden Sie unter "Leistung pro Regal".

Bei der Auswahl des Laufwerkstyps sollten Sie berücksichtigen, welche Arbeitslasten der Speicher

beherbergen wird und welche Kompromisse zwischen Leistung und Kapazitätsdichte damit verbunden sind.

Höchstwerte und Grenzwerte

Im folgenden Abschnitt werden die Maximal- und Minimalwerte eines NetApp AFX-Clusters im Vergleich zu Unified ONTAP behandelt.

Die aktuellsten Grenzwerte finden Sie unter "Hardware Universe".

NetApp AFX-Maximal- und Minimalwerte

Limit	Einheitliches ONTAP	NetApp AFX
Volumenanzahl (Cluster)	• 30.000 (plattformabhängig)	• 30.000
Gesamtgröße	• 800 TB	• k. A.
Knotenanzahl	• 24	• 8 (9.17.1) • 32 (9.19.1RC1)
Gesamtkapazität	• Abhängig von Knoten und Laufwerk. Siehe "hwu.netapp.com" für Details.	• 2PB (9.17.1) • 3PB (9.18.1RC1) • 16PB (9.18.1GA Release) • 20PB (9.19.1RC0) • 32PB (9.19.1RC1)
Unterstützte Regalanzahl	• 8 pro HA-Paar • 192 pro Cluster	• 12 pro Cluster (9.18.1GA) • 17 pro Cluster (9.19.1RC0) • 25 pro Cluster (9.19.1RC1) (keine HA-Paarbeschränkung)
Gesamtzahl der unterstützten Laufwerke	• 240 pro HA-Paar • 2880 (24 Knoten)	• 288 pro Cluster (basierend auf Regalanzahlbeschränkungen; keine HA-Paar-Beschränkung) • 408 pro Cluster (9.19.1RC0) • 600 pro Cluster (9.19.1RC1)
Volumengröße	• 300TB (FlexVol) • 60PB (FlexGroup)	• 300TB (FlexVol) • 60PB (FlexGroup)*
Maximale Anzahl an Dateien pro Volume	• 2 Milliarden (FlexVol) • 400 Milliarden (FlexGroup)	• 2 Milliarden (FlexVol) • 400 Milliarden (FlexGroup)

Limit	Einheitliches ONTAP	NetApp AFX
Maximale Anzahl an Dateien pro Verzeichnis (Standardwert 320MB maxdirsize-Wert)	• ~4 Millionen (FlexVol) • ~2 Millionen (FlexGroup)	• ~4 Millionen (FlexVol) • ~2 Millionen (FlexGroup)
SnapMirror gleichzeitige Übertragungen	• 250	• 250
Anzahl der qtrees	• 4096	• 4096
Maximale Anzahl TCP-Verbindungen pro Knoten	• 100.000	• 100.000
Maximale Anzahl an Sperren pro Knoten	• 3 Millionen	• 3 Millionen
Maximale Anzahl an Datenschnittstellen (Cluster)	• 4096	• 4096
Maximale Anzahl an Bestandteilen – FlexGroup	• 200	• 200 • 512 in 9.19.1 RC1
Maximale Anzahl von Intercluster-LIFs	• 8	• 8
Maximale Anzahl von IP spaces	• 512	• 512
Maximale Anzahl von FlexCache pro Ursprung	• 100	• 100
Maximale Anzahl von FlexCache (Knoten)	• 400	• 400

Wo finde ich weitere Informationen

Um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren, lesen Sie bitte die folgenden Dokumente und/oder Websites:

- "Hardware Universe"
- "AFX Produktseite"
- "Aufbau des KI-gestützten Unternehmens: Warum die Infrastruktur entscheidend ist"
- "Blog: Entscheidung zwischen NFSv3 und NFSv4.X"
- "AFX Datenblatt"

Technische Berichte von ONTAP SnapCenter

SnapCenter stellt eine einheitliche Plattform für applikationskonsistente Datensicherung und Klonmanagement bereit. SnapCenter vereinfacht Backups und Wiederherstellungen sowie das Lifecycle Management von Klonen durch applikationsintegrierte Workflows. Dank Storage-basiertem Datenmanagement steigert SnapCenter die Performance sowie Verfügbarkeit und verringert den Zeitaufwand für Test und Entwicklung.

Diese technischen Berichte erweitern die "SnapCenter"Produktdokumentation.

SnapCenter für Oracle

"TR-4700: SnapCenter Plug-in für Oracle Database Best Practices"
NetApp SnapCenter ist eine einheitliche, skalierbare Plattform für Oracle-konsistente Datensicherung, die komplexe Vorgänge mit zentraler Kontrolle und Übersicht automatisiert. Erfahren Sie mehr über empfohlene Vorgehensweisen für die Implementierung von Oracle-Datenbanken mit SnapCenter.

"TR-4964: Backup, Wiederherstellung und Klonen von Oracle Datenbanken mit SnapCenter Services"
Erfahren Sie, wie Sie SnapCenter Services für Backup, Wiederherstellung und Klonen von Oracle Datenbanken einrichten, die auf Amazon FSX für ONTAP Storage- und EC2 Computing-Instanzen bereitgestellt werden. Die Einrichtung und Nutzung sind zwar wesentlich einfacher, jedoch bieten SnapCenter-Services wichtige Funktionen, die über das SnapCenter-Interface verfügbar sind.

SnapCenter für Microsoft SQL Server

"TR-4714: Best Practices für Microsoft SQL Server mit NetApp SnapCenter"
Erfahren Sie, wie Sie Microsoft SQL Server erfolgreich auf NetApp Storage mit SnapCenter für die Datensicherung implementieren.

SnapCenter für Microsoft Exchange Server

"TR-4681: Best Practices für Microsoft Exchange Server mit NetApp SnapCenter"
Erfahren Sie, wie Sie Microsoft Exchange Server mit SnapCenter zur Datensicherung erfolgreich auf NetApp Storage bereitstellen.

SnapCenter für SAP HANA

"TR-4614: SAP HANA Backup und Recovery mit SnapCenter" SnapCenter ist eine einheitliche, skalierbare Plattform für applikationskonsistente Datensicherung für SAP HANA und andere Datenbanken. SnapCenter bietet zentrale Steuerung und Überwachung, während die Möglichkeit delegiert wird, dass Benutzer anwendungsspezifische Sicherungs-, Wiederherstellungs- und Klonvorgänge verwalten können. Mit SnapCenter steht Datenbank- und Speicheradministratoren ein einziges Tool zur Verfügung, um Sicherungs-, Wiederherstellungs- und Klonvorgänge für eine Vielzahl von Anwendungen und Datenbanken zu verwalten.

"TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter"
Informieren Sie sich über die empfohlenen Vorgehensweisen für die SAP HANA Datensicherung auf Amazon FSX für NetApp ONTAP und SnapCenter. Der Themengebiete umfassen SnapCenter-Konzepte, Konfigurationsempfehlungen und Betriebs-Workflows, einschließlich Konfiguration, Backup-Vorgänge, Und Restore- und Recovery-Vorgänge.

"TR-4667: Automatisierung von SAP HANA Systemkopien und Klonvorgängen mit SnapCenter" Mit SnapCenter Storage-Klonen und der Möglichkeit, Vorgänge vor und nach dem Klonen flexibel zu definieren, beschleunigen und automatisieren SAP Systemadministratoren Vorgänge zum Kopieren, Klonen oder Aktualisieren von SAP-Systemen. Erfahren Sie mehr über die Wahl eines beliebigen SnapCenter Snapshot Backups in jedem beliebigen primären oder sekundären Storage. Ermöglicht es Ihnen, Ihre wichtigsten Anwendungsfälle wie logische Beschädigung, Disaster Recovery-Tests oder die Aktualisierung eines SAP QA-Systems zu bewältigen.

"TR-4719: SAP HANA System Replication Backup and Recovery with SnapCenter"
SnapCenter Technologie und das SAP HANA Plug-in können für Backup und Recovery in einer SAP HANA System Replication-Umgebung eingesetzt werden.

"TR-4667: Automatisierung von SAP HANA-Systemkopien und Klonvorgängen mit SnapCenter" Die Fähigkeit, applikationskonsistente NetApp Snapshots auf Storage-Ebene zu erstellen, ist die Grundlage für die Systemkopien und Systemklonvorgänge. Storage-basierte Snapshot Backups werden mit dem NetApp SnapCenter Plug-in für SAP HANA und Schnittstellen der SAP HANA Datenbank erstellt. SnapCenter registriert Snapshot-Backups im SAP HANA Backup-Katalog, sodass die Backups für Restore, Recovery und Klonvorgänge verwendet werden können.

SnapCenter-Härtungsleitfaden

"TR-4957: Handbuch zur Erhöhung der Sicherheit für NetApp SnapCenter"
Erfahren Sie, wie Sie SnapCenter so konfigurieren, dass Unternehmen vorgeschriebene Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen.

Technische Berichte zum ONTAP Tiering

Mit der Daten-Tiering-Lösung von FabricPool wird die Benutzerfreundlichkeit von Flash-Systemen in Unternehmen verbessert, während gleichzeitig die Anpassung der Applikationsarchitektur für Storage-Effizienz mühsam vermieden wird. FabricPool senkt den Storage-Platzbedarf und die damit verbundenen Kosten für eine Systemumgebung. Aktive Daten bleiben auf High-Performance-SSDs. Inaktive Daten werden auf kostengünstigen Objektspeicher verschoben, wobei die Storage-Effizienz erhalten bleibt.

Diese technischen Berichte erweitern die "ONTAP FabricPool"Produktdokumentation.

"TR-4598: FabricPool Best Practices"
Erfahren Sie mehr über die Funktionen, Anforderungen, Implementierung und empfohlene Practices für FabricPool.

"TR-4826: NetApp FabricPool with StorageGRID Recommendation Guide"
Erfahren Sie mehr über die empfohlenen Vorgehensweisen für die Implementierung und Größenbestimmung von StorageGRID als Kapazitäts-Tier für die FabricPool der ONTAP-Komponente. Dieses Dokument behandelt außerdem die Kernfunktionen, Anforderungen, Implementierung und empfohlene Vorgehensweisen bei der Verwendung von StorageGRID.

"TR-4695: Datenbank-Storage-Tiering mit NetApp FabricPool"
Informieren Sie sich über die Vorteile und Konfigurationsoptionen von FabricPool mit unterschiedlichen Datenbanken, wie etwa dem relationalen Datenbankmanagementsystem (RDBMS) von Oracle.

Technische Berichte zur ONTAP Virtualisierung

NetApp Virtualisierungslösungen helfen Ihnen, den maximalen Nutzen aus Ihren Servern zu ziehen. Mit einer reaktionsschnellen virtuellen Serverinfrastruktur, die auf zukunftsweisenden, hochleistungsfähigen ONTAP Flash-Systemen basiert, können Sie schneller auf Ihre Daten zugreifen. Eine granulare virtuelle Infrastruktur lässt sich unterbrechungsfrei auf Datenmengen im Petabyte-Bereich skalieren und bietet die Performance, die für den gemeinsamen Zugriff auf mehrere Workloads erforderlich ist. ONTAP trägt durch wichtige Partnerschaften, Implementierungsanleitungen, Applikationsintegration und ein ausgereiftes Design dazu bei, den Einsatz von virtuellen Serverinfrastrukturen einfacher zu machen. ONTAP bietet viele empfohlene Praktiken und Lösungen für eine robuste Virtualisierungsumgebung sowohl vor Ort als auch in der Cloud.

Diese technischen Berichte erweitern die "ONTAP Tools für VMware vSphere"Produktdokumentation.

"TR-4597: VMware vSphere für ONTAP" ONTAP ist seit fast zwei Jahrzehnten eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich mit innovativen Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen. Dieses Dokument bietet eine Einführung in die ONTAP Lösung für vSphere sowie in die neuesten Produktinformationen und empfohlenen Vorgehensweisen zur Optimierung der Implementierung, Risikominderung und Vereinfachung des Managements.

"TR-4400: VMware vSphere Virtual Volumes (VVols) mit NetApp ONTAP" ONTAP ist seit über zwei Jahrzehnten eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich mit innovativen Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen. Dieses Dokument behandelt die ONTAP Funktionen für VMware vSphere Virtual Volumes (VVols), einschließlich der neuesten Produktinformationen und Anwendungsfälle sowie empfohlene Vorgehensweisen und andere Informationen zur Optimierung der Implementierung und Reduzierung von Fehlern.

"TR-4900: VMware Site Recovery Manager mit NetApp ONTAP" ONTAP ist seit seiner Einführung in das moderne Datacenter im Jahr 2002 eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich um innovative Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen. Dieses Dokument enthält eine Einführung in die ONTAP Lösung für VMware Site Recovery Manager (SRM), die branchenführende VMware Software für Disaster Recovery (DR), sowie in die neuesten Produktinformationen und empfohlene Verfahren zur Optimierung der Implementierung, Risikominderung und Vereinfachung des fortlaufenden Managements.

"Einführung in die Automatisierung für ONTAP und vSphere" Seit den ersten Tagen von VMware ESX ist die Automatisierung ein integraler Bestandteil des Managements von VMware Umgebungen. Die Möglichkeit, Infrastruktur als Code zu implementieren und Verfahren auf private Cloud-Vorgänge auszuweiten, um Bedenken hinsichtlich Skalierbarkeit, Flexibilität, Self-Provisioning und Effizienz zu zerstreuen. In diesem Dokument wird die ONTAP Lösung zur Automatisierung der ONTAP- und VMware vSphere-Umgebung vorgestellt.

"WP-7353: ONTAP Tools for VMware vSphere – Product Security" In diesem Dokument werden die Techniken und Technologien beschrieben, mit denen ONTAP-Tools für VMware vSphere 9.X sowohl vor vorhandenen als auch vor neuen Bedrohungen in Produktumgebungen gesichert werden.

"WP-7355: SnapCenter Plug-in VMware vSphere – Produktsicherheit" In diesem Dokument werden die Techniken und Technologien beschrieben, mit denen das NetApp SnapCenter Plug-in für VMware vSphere 4.X

sowohl vor vorhandenen als auch vor neuen Bedrohungen in Produktumgebungen gesichert wird.

"TR-4568: NetApp Implementierungsrichtlinien und Storage Best Practices für Windows Server" Microsoft Windows Server ist ein Betriebssystem der Enterprise-Klasse, das Netzwerke, Sicherheit, Virtualisierung, Cloud, virtuelle Desktop-Infrastruktur, Zugriffsschutz, Informationssicherheit, Webservices, Anwendungsplattformen-Infrastruktur und vieles mehr umfasst. Der Schwerpunkt dieses Dokuments liegt auf Microsoft Windows. Der Schwerpunkt liegt dabei auf der Hyper-V Virtualisierungstechnologie, einschließlich der neuesten Produktinformationen und empfohlenen Vorgehensweisen, um die Implementierung zu optimieren, Risiken zu reduzieren und das Management zu vereinfachen.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

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

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

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

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

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

Datenschutzrichtlinie

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

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

ONTAP

"Hinweis für ONTAP 9.16.1" "Hinweis für ONTAP 9.16.0" "Hinweis für ONTAP 9.15.1" "Hinweis für ONTAP 9.15.0" "Hinweis für ONTAP 9.14.1" "Hinweis für ONTAP 9.14.0" "Hinweis für ONTAP 9.13.1" "Hinweis zu ONTAP 9.12.1" "Hinweis zu ONTAP 9.12.0" "Hinweis zu ONTAP 9.11.1" "Hinweis zu ONTAP 9.10.1" "Hinweis für ONTAP 9.10.0" "Hinweis zu ONTAP 9.9.1" "Hinweis zu ONTAP 9.8" "Hinweis für ONTAP 9.7" "Hinweis für ONTAP 9.6" "Hinweis für ONTAP 9.5" "Hinweis für ONTAP 9.4" "Hinweis für ONTAP 9.3" "Hinweis für ONTAP 9.2" "Hinweis für ONTAP 9.1"

ONTAP Mediator für MetroCluster IP-Konfigurationen

"9.9.1 Hinweis für ONTAP Mediator für MetroCluster IP-Konfigurationen" "9.8 Hinweis für ONTAP Mediator für MetroCluster IP-Konfigurationen" "9.7 Hinweis für ONTAP Mediator für MetroCluster IP-Konfigurationen"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.