Konzepte

Element Software

NetApp
October 01, 2024

Inhalt

Konzepte

Lernen Sie grundlegende Konzepte in Bezug auf Element Software kennen.

- "Produktübersicht"
- Übersicht über die Architektur von SolidFire
- Knoten
- Cluster
- "Sicherheit"
- Konten und Berechtigungen
- "Volumes"
- Datensicherung
- Leistung und Servicequalität

Weitere Informationen

- "SolidFire All-Flash-Storage im Überblick"
- "Dokumentation von SolidFire und Element Software"

Produktübersicht

Ein SolidFire All-Flash-Storage-System besteht aus separaten Hardwarekomponenten (Laufwerke und Nodes), die in einem einzelnen Pool der Storage-Ressourcen kombiniert werden. Dieser Unified Cluster stellt ein einziges Storage-System zur Verwendung durch externe Clients dar und wird mit der NetApp Element Software gemanagt.

Mit der Element Schnittstelle, der API oder anderen Managementtools können Sie die Kapazität und Performance des SolidFire Cluster-Storage überwachen und Storage-Aktivitäten in einer mandantenfähigen Infrastruktur managen.

Funktionen der SolidFire

Ein SolidFire System umfasst folgende Funktionen:

- Bietet hochperformanten Storage für Ihre große Private-Cloud-Infrastruktur
- Flexible Skalierung bei sich ändernden Storage-Anforderungen
- Verwendet eine API-gestützte Softwareschnittstelle für Storage-Managementelemente
- Garantierte Performance dank Quality of Service-Richtlinien
- Umfasst einen automatischen Lastausgleich über alle Nodes im Cluster hinweg
- Automatische Ausbalancierung von Clustern beim Hinzufügen oder Entfernen von Nodes

SolidFire Implementierung

Verwenden Sie von NetApp bereitgestellte und in NetApp Element Software integrierte Storage-Nodes.

"Übersicht über die All-Flash-Storage-Architektur von SolidFire"

Weitere Informationen

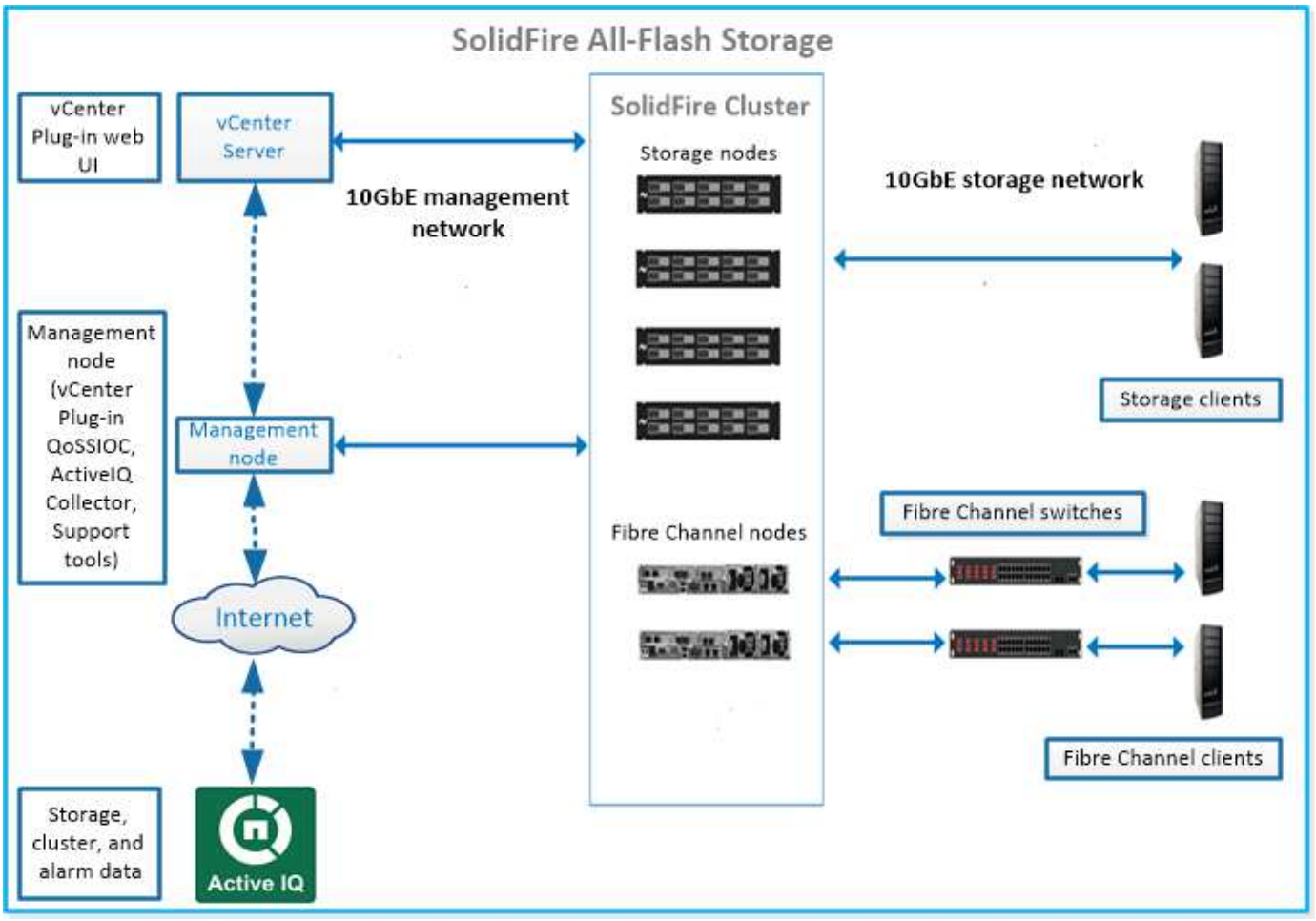
- "SolidFire All-Flash-Storage im Überblick"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Übersicht über die Architektur von SolidFire

Ein SolidFire All-Flash-Storage-System besteht aus separaten Hardwarekomponenten (Laufwerk und Nodes), die in einem Pool von Storage-Ressourcen kombiniert werden. Dabei wird die NetApp Element Software unabhängig auf jedem Node ausgeführt. Dieses einzelne Storage-System wird als Einheit über die UI, die API und andere Managementtools von Element Software gemanagt.

Ein SolidFire Storage-System umfasst die folgenden Hardwarekomponenten:

- **Cluster**: Der Hub des SolidFire Speichersystems, das eine Ansammlung von Knoten ist.
- **Knoten**: Die Hardware-Komponenten in einem Cluster gruppiert. Es gibt zwei Node-Typen:
  - Storage-Nodes: Bei Servern handelt es sich um eine Sammlung von Laufwerken
  - Fibre Channel-Nodes (FC), die Sie zum Herstellen einer Verbindung mit FC-Clients verwenden
- **Laufwerke**: Wird in Speicherknoten verwendet, um Daten für den Cluster zu speichern. Ein Storage-Node enthält zwei Laufwerkstypen:
  - Volume-Metadaten speichern Informationen, die Volumes und andere Objekte innerhalb eines Clusters definieren.
  - Block-Laufwerke speichern Datenblöcke für Volumes.



Sie können das System über die Element Web-UI und andere kompatible Tools verwalten, überwachen und aktualisieren:

- "SolidFire-Softwareschnittstellen"
- "SolidFire Active IQ"
- "Management-Node für Element Software"
- "Management Services"

Allgemeine URLs

Dies sind die allgemeinen URLs, die Sie mit einem SolidFire All-Flash-Storage-System verwenden:

URL	Beschreibung
`https://[storage cluster MVIP address]`	Zugreifen auf die Benutzeroberfläche der NetApp Element Software
`https://activeiq.solidfire.com`	Überwachen Sie Ihre Daten und erhalten Sie Warnmeldungen zu Performance-Engpässen oder potenziellen Systemproblemen.
`https://[management node IP address]`	Der Zugriff auf NetApp Hybrid Cloud Control ermöglicht Ihnen, Ihre Services für die Storage-Installation und -Aktualisierung zu aktualisieren.

URL	Beschreibung
`https://[IP address]:442`	Greifen Sie über die Node-Benutzeroberfläche auf Netzwerk- und Cluster-Einstellungen zu und nutzen Sie Systemtests und Dienstprogramme. "Weitere Informationen ."
`https://[management node IP address]/mnode`	Verwendung von REST-API für Managementservices und anderen Funktionen aus dem Management-Node "Weitere Informationen ."
`https://[management node IP address]:9443`	Registrieren Sie das vCenter Plug-in-Paket im vSphere Web Client. "Weitere Informationen ."

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SolidFire-Softwareschnittstellen

Sie können ein SolidFire Storage-System mit verschiedenen NetApp Element Software-Schnittstellen und Integrations-Utilities verwalten.

Optionen

- Benutzeroberfläche der NetApp Element Software
- NetApp Element Software-API
- NetApp Element Plug-in für vCenter Server
- NetApp Hybrid Cloud Control
- UIs für Managementknoten
- Zusätzliche Integrations-Tools

Benutzeroberfläche der NetApp Element Software

Ermöglicht die Einrichtung von Element Storage, die Überwachung von Cluster-Kapazität und -Performance und das Management von Storage-Aktivitäten in einer mandantenfähigen Infrastruktur. Element ist das Storage-Betriebssystem, das Herzstück eines SolidFire Clusters ist. Element Software wird unabhängig auf allen Nodes im Cluster ausgeführt und ermöglicht den Nodes des Clusters die Kombination der Ressourcen, die externen Clients als einzelnes Storage-System präsentiert werden. Element Software ist für die gesamte Clusterkoordination, den Umfang und das Management des Systems verantwortlich. Die Softwareschnittstelle basiert auf der Element API.

"Storage-Management mit Element Software"

NetApp Element Software-API

Ermöglicht die Verwendung einer Reihe von Objekten, Methoden und Routinen zum Storage Management. Die Element-API basiert auf dem JSON-RPC-Protokoll über HTTPS. Sie können API-Vorgänge in der Element-UI überwachen, indem Sie das API-Protokoll aktivieren. Dadurch können Sie die Methoden anzeigen, die an das System ausgegeben werden. Sie können sowohl Anfragen als auch Antworten aktivieren, um zu sehen, wie das System auf die ausgestellten Methoden antwortet.

"Storage-Management mit der Element API"

NetApp Element Plug-in für vCenter Server

Ermöglicht die Konfiguration und das Management von Storage-Clustern mit Element Software über eine alternative Schnittstelle für die Element UI in VMware vSphere.

"NetApp Element Plug-in für vCenter Server"

NetApp Hybrid Cloud Control

Ermöglicht die Aktualisierung von Element-Storage- und Managementservices sowie das Management von Storage-Ressourcen über die NetApp Hybrid Cloud Control Schnittstelle.

"Managen und überwachen Sie Storage mit der Übersicht über NetApp Hybrid Cloud Control"

UIs für Managementknoten

Der Managementknoten enthält zwei UIs: Eine Benutzeroberfläche zur Verwaltung VON REST-basierten Diensten und eine Benutzeroberfläche pro Node zur Verwaltung von Netzwerk- und Clustereinstellungen sowie Betriebssystemtests und Dienstprogrammen. Über DIE REST-API-UI steht ein Menü mit Service-bezogenen APIs zur Verfügung, die die Service-basierte Systemfunktionalität vom Management-Node aus steuern.

Zusätzliche Integrations-Tools

Obwohl Sie Ihren Storage in der Regel mit NetApp Element, der NetApp Element API und dem NetApp Element Plug-in für vCenter Server managen, können Sie auf den Storage mithilfe weiterer Integrationstools und -Tools zugreifen.

Element CLI

"Element CLI" Ermöglicht die Steuerung eines SolidFire Storage-Systems über eine Befehlszeilenschnittstelle ohne Einsatz der Element API.

Element PowerShell Tools

"Element PowerShell Tools" Ermöglicht die Verwendung einer Sammlung von Microsoft Windows PowerShell Funktionen, die die Element API zum Managen eines SolidFire Storage-Systems verwenden.

Element-SDKs

"Element-SDKs" Ermöglichen Sie das Management Ihres SolidFire Clusters mit den folgenden Tools:

- Element Java SDK: Ermöglicht Programmierern die Integration der Element-API in die Java-Programmiersprache.
- Element .NET SDK: Ermöglicht Programmierern die Integration der Element-API in die .NET-Programmierplattform.
- Element Python SDK: Ermöglicht Programmierern die Integration der Element-API in die Programmiersprache Python.

SolidFire Postman API Testsuite

Ermöglicht Programmierern, eine Sammlung von Funktionen zu verwenden"Postman", die Element-API-Aufrufe testen.

SolidFire Storage Replication Adapter

"SolidFire Storage Replication Adapter" Die Integration in den VMware Site Recovery Manager (SRM) ermöglicht die Kommunikation mit replizierten SolidFire Storage Clustern und die Ausführung unterstützter Workflows.

SolidFire VRO

"SolidFire VRO" Bietet eine einfache Möglichkeit zur Verwendung der Element API für die Administration Ihres SolidFire Storage-Systems mit VMware vRealize Orchestrator.

SolidFire VSS Provider

"SolidFire VSS Provider" Integriert VSS-Schattenkopien in Element Snapshots und Klone.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ" Ist ein webbasiertes Tool, das kontinuierlich aktualisierte historische Ansichten von Cluster-weiten Daten bietet. Sie können Benachrichtigungen für bestimmte Ereignisse, Schwellenwerte oder Metriken einrichten. Mit SolidFire Active IQ können Sie die Performance und Kapazität des Systems überwachen und über den Cluster-Zustand auf dem Laufenden bleiben.

Folgende Informationen zu Ihrem System finden Sie im SolidFire Active IQ:

- Anzahl der Nodes und Status der Nodes: Ordnungsgemäß, offline oder Fehler
- Grafische Darstellung der CPU-, Speichernutzung und Knotendrosselung
- Details zum Node, z. B. Seriennummer, Steckplatz im Chassis, Modell und Version der NetApp Element Software, die auf dem Storage-Node ausgeführt wird
- CPU- und Storage-bezogene Informationen zu Virtual Machines

Weitere Informationen zu SolidFire Active IQ finden Sie im "SolidFire Active IQ-Dokumentation".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"
- **NetApp Support-Website › Tools für Active IQ**

Management-Node für Element Software

"Management-Node (mNode)"Bei der handelt es sich um eine Virtual Machine, die mit einem oder mehreren softwarebasierten Storage-Clustern parallel ausgeführt wird. Er dient als Upgrade und zur Bereitstellung von Systemservices wie Monitoring und Telemetrie, zum Management von Cluster-Ressourcen und -Einstellungen, zur

Ausführung von Systemtests und Dienstprogrammen und zur Aktivierung des NetApp Support-Zugriffs zur Fehlerbehebung.

Der Management-Node interagiert mit einem Storage-Cluster, um Managementaktionen auszuführen, ist jedoch nicht Mitglied des Storage-Clusters. Managementknoten erfassen regelmäßig über API-Aufrufe Informationen über das Cluster und melden diese Informationen zur Remote-Überwachung an Active IQ (sofern aktiviert). Management-Nodes sind auch für die Koordinierung von Software-Upgrades der Cluster-Nodes verantwortlich.

Ab Element 11.3 fungiert der Management Node als Microservice-Host, wodurch sich ausgewählte Softwareservices schneller außerhalb der Hauptversionen aktualisieren lassen. Diese Microservices oder "Management Services" werden häufig als Service-Bundles aktualisiert.

Managementservices für SolidFire All-Flash-Storage

Ab der Version Element 11.3 werden **Management Services** auf dem gehostet"Management-Node", was schnellere Updates von ausgewählten Software-Services außerhalb der Hauptversionen ermöglicht.

Managementservices bieten zentrale und erweiterte Managementfunktionen für SolidFire All-Flash-Storage. Zu diesen Services gehören u. a. "NetApp Hybrid Cloud Control"die Active IQ System Telemetrie, Protokollierung und Service-Updates sowie der QoSSIOC-Service für das Element Plug-in für vCenter.

Erfahren Sie mehr über "Management Services-Releases".

Knoten

Nodes sind Hardware- oder virtuelle Ressourcen, die in einem Cluster gruppiert werden, um Block-Storage- und Computing-Funktionen bereitzustellen.

NetApp Element Software definiert verschiedene Node-Rollen für ein Cluster. Die Typen der Node-Rollen sind die folgenden:

- Management-Node
- Storage-Node
- Fibre Channel-Node

Nodes-Status Je nach Cluster-Zuordnung variieren.

Management-Node

Ein Management-Node ist eine Virtual Machine, die für Upgrades und die Bereitstellung von Systemservices wie Monitoring und Telemetrie, das Management von Cluster-Assets und -Einstellungen, die Ausführung von Systemtests und Dienstprogrammen sowie den NetApp-Support-Zugriff für die Fehlerbehebung verwendet wird. "Weitere Informationen ."

Storage-Node

Ein SolidFire-Storage-Node ist ein Server, der eine Sammlung von Laufwerken enthält, die über die Bond10G-Netzwerkschnittstelle miteinander kommunizieren. Laufwerke im Node enthalten Block- und Metadatenspeicherplatz für den Daten-Storage und das Datenmanagement. Jeder Node enthält ein Factory

Image der NetApp Element Software.

Storage-Nodes weisen folgende Merkmale auf:

- Jeder Node hat einen eindeutigen Namen. Wenn ein Node-Name nicht von einem Administrator angegeben wird, ist er standardmäßig SF-XXXX, wobei XXXX vier zufällige Zeichen enthält, die vom System generiert werden.
- Jeder Node verfügt über einen eigenen hochperformanten NVRAM-Schreib-Cache (Non-Volatile Random Access Memory), um die Systemperformance insgesamt zu verbessern und die Schreiblatenz zu reduzieren.
- Jeder Node ist mit zwei Netzwerken verbunden, Storage und Management, jedes mit zwei unabhängigen Links, um für Redundanz und Performance zu sorgen. Jeder Node benötigt in jedem Netzwerk eine IP-Adresse.
- Sie können mit neuen Storage-Nodes ein Cluster erstellen oder einem vorhandenen Cluster Storage Nodes hinzufügen, um die Storage-Kapazität und Performance zu steigern.
- Nodes können jederzeit ohne Serviceunterbrechung zum Cluster hinzugefügt oder aus dem Cluster entfernt werden.

Fibre Channel-Node

SolidFire Fibre Channel Nodes stellen Konnektivität zu einem Fibre Channel Switch bereit, den Sie mit Fibre Channel Clients verbinden können. Fibre Channel Nodes fungieren als Protokollkonverter zwischen den Fibre Channel- und iSCSI-Protokollen. So können Sie jedem neuen oder vorhandenen SolidFire Cluster Fibre Channel-Konnektivität hinzufügen.

Fibre-Channel-Nodes weisen folgende Merkmale auf:

- Fibre Channel Switches managen den Zustand der Fabric und bieten optimierte Verbindungen.
- Der Datenverkehr zwischen zwei Ports fließt nur durch die Switches; er wird nicht an einen anderen Port übertragen.
- Der Ausfall eines Ports ist isoliert, hat keine Auswirkungen auf den Betrieb anderer Ports.
- Mehrere Ports können gleichzeitig in einem Fabric kommunizieren.

Node-Status des Vorgangs

Je nach Konfigurationsstufe kann ein Node in einem von mehreren Status vorhanden sein.

- **Verfügbar**

  Dem Node ist kein Cluster-Name zugewiesen, der noch nicht Teil eines Clusters ist.

- **Ausstehend**

  Der Node ist konfiguriert und kann einem zugewiesenen Cluster hinzugefügt werden.

  Für den Zugriff auf den Node ist keine Authentifizierung erforderlich.

- **Ausstehend Aktiv**

  Das System installiert gerade kompatible Element Software auf dem Node. Nach Abschluss der Migration

wird der Node in den Status „aktiv“ verschoben.

- * Aktiv*

  Der Knoten ist an einem Cluster beteiligt.

  Zum Ändern des Node ist eine Authentifizierung erforderlich.

In jedem dieser Zustände werden einige Felder schreibgeschützt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Cluster

Ein Cluster ist der Hub eines SolidFire Storage-Systems und besteht aus einer Sammlung von Nodes. Sie müssen mindestens vier Nodes in einem Cluster aufweisen, damit die SolidFire Storage-Effizienz realisiert werden kann. Ein Cluster wird im Netzwerk als einzelne logische Gruppe angezeigt und kann dann als Block-Storage genutzt werden.

Durch das Erstellen eines neuen Clusters wird ein Node als Kommunikationsinhaber für ein Cluster initialisiert und stellt die Netzwerkkommunikation für jeden Node im Cluster her. Dieser Prozess wird nur einmal für jedes neue Cluster durchgeführt. Sie können ein Cluster mithilfe der Element UI oder der API erstellen.

Sie können ein Cluster horizontal skalieren, indem Sie weitere Nodes hinzufügen. Wenn Sie einen neuen Node hinzufügen, wird der Service nicht unterbrochen, und der Cluster nutzt die Performance und Kapazität des neuen Node automatisch.

Administratoren und Hosts können über virtuelle IP-Adressen auf das Cluster zugreifen. Jeder Node im Cluster kann die virtuellen IP-Adressen hosten. Die Management Virtual IP (MVIP) ermöglicht das Clustermanagement über eine 1-GbE-Verbindung, während die Speicher-virtuelle IP (SVIP) den Host-Zugriff auf Speicher über eine 10-GbE-Verbindung ermöglicht. Diese virtuellen IP-Adressen ermöglichen konsistente Verbindungen unabhängig von der Größe oder dem Aufbau eines SolidFire Clusters. Wenn ein Node, der eine virtuelle IP-Adresse hostet, ausfällt, beginnt ein anderer Node im Cluster mit dem Hosten der virtuellen IP-Adresse.

> Ab Element Version 11.0 können Nodes mit IPv4, IPv6 oder beiden Adressen für ihr Managementnetzwerk konfiguriert werden. Dies gilt sowohl für Storage-Nodes als auch für Management-Nodes, mit Ausnahme von Management-Node 11.3 und höher, der IPv6 nicht unterstützt. Beim Erstellen eines Clusters kann nur eine einzelne IPv4- oder IPv6-Adresse für den MVIP verwendet werden, und der entsprechende Adresstyp muss auf allen Knoten konfiguriert werden.

Mehr auf Clustern

- Autorisierende Storage-Cluster
- Drittelregel
- Ungenutzte Kapazität
- Storage-Effizienz

- Storage Cluster Quorum

Autorisierende Storage-Cluster

Der Storage-Cluster ist der Storage-Cluster, mit dem NetApp Hybrid Cloud Control Benutzer authentifizieren kann.

Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster. Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden. Um herauszufinden, welcher Cluster der autoritative Cluster ist, können Sie die API verwenden `GET /mnode/about`. In der Antwort ist die IP-Adresse im `token_url` Feld die virtuelle Management-IP-Adresse (MVIP) des autoritativen Speicher-Clusters. Wenn Sie versuchen, sich bei NetApp Hybrid Cloud Control als Benutzer anzumelden, der sich nicht auf dem autorisierenden Cluster befindet, schlägt der Anmeldeversuch fehl.

Viele Funktionen von NetApp Hybrid Cloud Control wurden für den Einsatz mit mehreren Storage-Clustern entwickelt. Allerdings schränkteutig die Authentifizierung und Autorisierung sein. Die Authentifizierung und Autorisierung im Zusammenhang mit der Authentifizierung besteht darin, dass der Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen kann, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht Anwender in den anderen Storage-Clustern sind.

Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Sie können Benutzer über die verwalten"Benutzeroberfläche von Element Software".

Weitere Informationen zum Arbeiten mit Management-Storage-Cluster-Assets für Nodes finden Sie unter"Erstellen und Managen von Storage-Cluster-Assets".

Drittelregel

Bei einer Kombination von Storage-Node-Typen in einem NetApp SolidFire Storage Cluster kann kein einzelner Storage-Node mehr als 33 % der gesamten Storage Cluster-Kapazität enthalten.

Ungenutzte Kapazität

Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage-Kapazität hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Kapazität sollte immer paarweise hinzugefügt werden, um dies zu vermeiden. Wenn ein Node ungenutzt wird, ist ein geeigneter Cluster-Fehler zu werfen.

Storage-Effizienz

NetApp SolidFire Storage Cluster nutzen Deduplizierung, Komprimierung und Thin Provisioning, um den physischen Storage-Bedarf für das Speichern eines Volumes zu verringern.

- **Komprimierung**

  Bei der Komprimierung wird der physische Storage-Bedarf eines Volumes reduziert, indem Datenblöcke in Komprimierungsgruppen kombiniert werden, die jeweils als einzelne Blöcke gespeichert werden.

- **Deduplizierung**

Dank der Deduplizierung wird die Menge des für ein Volume erforderlichen physischen Storage reduziert, indem doppelte Datenblöcke verworfen werden.

- **Thin Provisioning**

  Ein Thin Provisioning-Volume oder eine LUN ist eine LUN, bei der kein vorab reservierter Storage reserviert wird. Stattdessen wird der Storage dynamisch nach Bedarf zugewiesen. Freier Speicherplatz wird wieder dem Storage-System freigegeben, wenn die Daten vom Volume oder von der LUN gelöscht werden

Storage Cluster Quorum

Element Software erstellt ein Storage-Cluster von ausgewählten Nodes, wobei eine replizierte Datenbank der Clusterkonfiguration erhalten bleibt. Zur Teilnahme am Cluster-Ensemble sind mindestens drei Nodes erforderlich, um das Quorum für die Cluster-Ausfallsicherheit zu erhalten.

Sicherheit

Wenn Sie Ihr SolidFire All-Flash-Storage-System nutzen, werden Ihre Daten durch branchenübliche Sicherheitsprotokolle geschützt.

Verschlüsselung für Daten im Ruhezustand (Hardware)

Alle Laufwerke in Storage-Nodes können verschlüsselt werden. Dazu wird die AES 256-Bit-Verschlüsselung auf Laufwerksebene verwendet. Jedes Laufwerk verfügt über einen eigenen Verschlüsselungsschlüssel, der beim ersten Initialized des Laufwerks erstellt wird. Wenn Sie die Verschlüsselungsfunktion aktivieren, wird ein Cluster-weites Passwort erstellt und Datenblöcke des Passworts werden dann auf alle Nodes im Cluster verteilt. Kein Single Node speichert das gesamte Passwort. Das Passwort wird dann verwendet, um den gesamten Zugriff auf die Laufwerke kennwortgeschützt zu machen. Das Kennwort ist erforderlich, um das Laufwerk zu entsperren und wird dann nur benötigt, wenn die Stromversorgung vom Laufwerk entfernt oder das Laufwerk gesperrt ist.

"Aktivieren der Hardware-Verschlüsselung für Daten im Ruhezustand" Keine Auswirkungen auf die Performance oder die Effizienz im Cluster Wenn ein verschlüsselungsfähiges Laufwerk oder Node mit der Element API oder der Element UI aus der Cluster-Konfiguration entfernt wird, wird die Verschlüsselung im Ruhezustand auf den Laufwerken deaktiviert. Nachdem das Laufwerk entfernt wurde, kann das Laufwerk mit der API-Methode sicher gelöscht werden `SecureEraseDrives`. Wenn ein physisches Laufwerk oder ein Knoten gewaltsam entfernt wird, bleiben die Daten durch das Cluster-weite Passwort und die individuellen Verschlüsselungsschlüssel des Laufwerks geschützt.

Verschlüsselung für Daten im Ruhezustand (Software)

Bei einem anderen Verschlüsselungstyp, der Softwareverschlüsselung im Ruhezustand, können alle Daten, die in einem Storage-Cluster auf SSDs geschrieben wurden, verschlüsselt werden. "Wenn aktiviert", Es verschlüsselt alle Daten geschrieben und entschlüsselt alle Daten automatisch in Software gelesen. Softwareverschlüsselung im Ruhezustand spiegelt die SED-Implementierung (Self-Encrypting Drive) in der Hardware, um Datensicherheit ohne SED zu gewährleisten.

Bei SolidFire All-Flash-Storage-Clustern muss die Softwareverschlüsselung im Ruhezustand während der Cluster-Erstellung aktiviert sein und nach dem Erstellen des Clusters nicht deaktiviert werden können.

Sowohl die Software- als auch die Hardware-basierte Verschlüsselung im Ruhezustand können unabhängig voneinander oder kombiniert werden.

Externes Verschlüsselungskeymanagement

Sie können Element Software für das Management der Storage-Cluster-Verschlüsselungen konfigurieren, indem Sie einen KMIP-konformen (Key Management Service) eines Drittanbieters verwenden. Wenn Sie diese Funktion aktivieren, wird der Schlüssel für den Zugriff auf das Passwort für den gesamten Laufwerkszugriff des Storage-Clusters von einem von Ihnen angegebenen KMS gemanagt.

Element kann die folgenden wichtigen Managementservices nutzen:

- Gemalto SafeNet KeySecure
- SafeNet BEI KeySecure
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

Weitere Informationen zum Konfigurieren der externen Schlüsselverwaltung finden Sie in "Erste Schritte mit externem Verschlüsselungsmanagement"der Dokumentation.

Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierung (MFA) ermöglicht es Benutzern, bei der Anmeldung mehrere Arten von Beweisen zur Authentifizierung bei der NetApp Element Web-UI oder der Storage-Node-UI vorzulegen. Sie können Element so konfigurieren, dass nur Multi-Faktor-Authentifizierung für Anmeldungen akzeptiert wird, die sich in Ihr vorhandenes Benutzerverwaltungssystem und Ihren Identitäts-Provider integrieren lassen. Sie können das Element so konfigurieren, dass es sich in einen vorhandenen SAML 2.0-Identitätsanbieter integrieren lässt, der mehrere Authentisierungsschemata wie Passwort- und Textnachricht, Passwort- und E-Mail-Nachricht oder andere Methoden durchsetzen kann.

Sie können Multi-Faktor-Authentifizierung mit gängigen SAML 2.0-kompatiblen Identitäts-Providern (IDPs) wie Microsoft Active Directory Federation Services (ADFS) und Shibboleth kombinieren.

Informationen zur Konfiguration von MFA finden Sie in "Die Multi-Faktor-Authentifizierung aktivieren"der Dokumentation.

FIPS 140-2 für HTTPS und Verschlüsselung von Daten im Ruhezustand

NetApp SolidFire Storage-Cluster unterstützen eine Verschlüsselung, die die Anforderungen des Federal Information Processing Standard (FIPS) 140-2 an kryptografische Module erfüllt. Sie können die Compliance mit FIPS 140-2 auf Ihrem SolidFire Cluster sowohl für HTTPS-Kommunikation als auch für Laufwerksverschlüsselung aktivieren.

Wenn Sie den FIPS 140-2 Betriebsmodus auf dem Cluster aktivieren, aktiviert das Cluster das NetApp Cryptographic Security Module (NCSM) und nutzt die zertifizierte Verschlüsselung nach FIPS 140-2 Level 1 für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und den API. Sie verwenden die `EnableFeature` Element API mit dem `fips` Parameter zur Aktivierung der FIPS 140-2-HTTPS-Verschlüsselung. Auf Storage-Clustern mit FIPS-kompatibler Hardware können Sie mithilfe der Element API mit dem `FipsDrives` Parameter auch die FIPS-Laufwerksverschlüsselung für Daten im Ruhezustand aktivieren `EnableFeature`.

Weitere Informationen zur Vorbereitung eines neuen Storage-Clusters für die Verschlüsselung nach FIPS 140-2 finden Sie unter "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt".

Weitere Informationen zur Aktivierung von FIPS 140-2 auf einem vorhandenen, vorbereiteten Cluster finden Sie unter "Die API für das EnableFeature-Element".

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konten und Berechtigungen

Um die Storage-Ressourcen in Ihrem System zu verwalten und Zugriff zu gewähren, müssen Sie Konten für Systemressourcen einrichten.

Mit Element Storage können Sie folgende Typen von Konten erstellen und verwalten:

- Administratorkonten für das Storage-Cluster
- Benutzerkonten für Storage-Volume-Zugriff
- Maßgebliche Cluster-Benutzerkonten für NetApp Hybrid Cloud Control

Konten für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein:

- **Primary Cluster Administrator Account**: Dieses Administratorkonto wird beim Erstellen des Clusters erstellt. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.
- **Cluster-Administratorkonto**: Sie können einem Cluster-Administratorkonto eine begrenzte Anzahl von Administratorzugriff zur Ausführung bestimmter Aufgaben innerhalb eines Clusters gewähren. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

> Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Sie können "Verwalten von Cluster-Administratorkonten"Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Cluster-Administratorkennwort ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Benutzerkonten

Über Benutzerkonten werden der Zugriff auf die Storage-Ressourcen in einem softwarebasierten Netzwerk von NetApp Element gesteuert. Mindestens ein Benutzerkonto ist erforderlich, bevor ein Volume erstellt werden kann.

Wenn Sie ein Volume erstellen, wird es einem Konto zugewiesen. Wenn Sie ein virtuelles Volume erstellt

haben, ist das Konto der Speichercontainer.

Folgende Aspekte sollten zusätzlich berücksichtigt werden:

- Das Konto enthält die CHAP-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist.
- Einem Konto können bis zu 2000 Volumes zugewiesen sein, aber ein Volume kann nur zu einem Konto gehören.
- Benutzerkonten können über den Erweiterungspunkt für die NetApp Element-Verwaltung verwaltet werden.

Autorisierende Cluster-Benutzerkonten

Autorisierte Cluster-Benutzerkonten können sich gegen alle Storage-Ressourcen authentifizieren, die mit der NetApp Hybrid Cloud Control Instanz der Nodes und Cluster verbunden sind. Mit diesem Konto können Sie Volumes, Konten, Zugriffsgruppen und mehr über alle Cluster hinweg verwalten.

Maßgebliche Benutzerkonten werden über die obere rechte Menü-Option „Benutzermanagement“ in der NetApp Hybrid Cloud Control gemanagt.

Das "Autorisierende Storage-Cluster" ist das Storage-Cluster, das NetApp Hybrid Cloud Control zum Authentifizieren von Benutzern verwendet.

Bei der NetApp Hybrid Cloud Control können sich alle Benutzer, die auf dem autorisierenden Storage-Cluster erstellt wurden, anmelden. Benutzer, die auf anderen Storage Clustern erstellt wurden, können sich bei Hybrid Cloud Control nicht anmelden.

- Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster.
- Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden.

Viele NetApp Hybrid Cloud Control Funktionen funktionieren zwar mit mehreren Storage-Clustern, jedoch bringen Authentifizierung und Autorisierung erforderliche Einschränkungen mit sich. Die Einschränkung der Authentifizierung und Autorisierung besteht darin, dass Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen können, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht in den anderen Storage-Clustern ausgeführt werden. Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Benutzer können über NetApp Hybrid Cloud Control gemanagt werden.

Volume-Konten

Volume-spezifische Konten gelten nur für den Storage Cluster, auf dem sie erstellt wurden. Mit diesen Konten können Sie Berechtigungen für bestimmte Volumes im Netzwerk festlegen, haben aber keine Auswirkungen außerhalb dieser Volumes.

Volume-Konten werden in der Tabelle „NetApp Hybrid Cloud Control Volumes“ gemanagt.

Storage

Volumes

Das Storage-System NetApp Element stellt Storage mithilfe von Volumes bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Element Storage ermöglicht Ihnen das Erstellen, Anzeigen, Bearbeiten, Löschen, Klonen Sichern Sie Volumes für Benutzerkonten oder stellen Sie sie wieder her. Außerdem lassen sich Volumes in einem Cluster managen und Volumes in Volume-Zugriffsgruppen hinzufügen oder entfernen.

Persistente Volumes

Mithilfe persistenter Volumes können Management-Node-Konfigurationsdaten nicht lokal mit einer VM in einem bestimmten Storage-Cluster gespeichert werden, damit Daten auch bei Verlust oder Entfernung von Management-Nodes erhalten bleiben. Persistente Volumes sind eine optionale, jedoch empfohlene Management-Node-Konfiguration.

Eine Option zum Aktivieren von persistenten Volumes ist in den Installations- und Upgrade-Skripten enthalten, wenn "Implementieren eines neuen Management-Node". Persistente Volumes sind Volumes auf einem Element Software-basierten Storage-Cluster, die Konfigurationsinformationen für die Host-Management-Node-VM enthalten, die über den Lebenszyklus der VM hinaus bestehen bleiben. Wenn der Management-Node verloren geht, kann eine VM mit dem Ersatz-Management-Node eine Verbindung herstellen und Konfigurationsdaten für die verlorene VM wiederherstellen.

Persistente Volume-Funktion, sofern diese während der Installation oder des Upgrades aktiviert ist, erstellt automatisch mehrere Volumes. Diese Volumes können, wie jedes softwarebasierte Element Volume, je nach Ihren Vorliebe und Installation über die Web-UI in Element Software, das NetApp Element Plug-in für vCenter Server oder die API angezeigt werden. Persistente Volumes müssen mit einer iSCSI-Verbindung zum Management-Node in Betrieb sein, um die aktuellen Konfigurationsdaten beizubehalten, die für eine Recovery verwendet werden können.

Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht

Virtuelle Volumes (VVols)

VSphere Virtual Volumes ist ein Storage-Paradigma für VMware, das einen Großteil des Storage-Managements für vSphere vom Storage-System in VMware vCenter verschiebt. Mit Virtual Volumes (VVols) können Sie Storage den Anforderungen einzelner Virtual Machines zuweisen.

Bindungen

Der NetApp Element Cluster wählt einen optimalen Protokollendpunkt, erstellt eine Bindung, die den ESXi Host und das virtuelle Volume dem Protokollendpunkt zugeordnet und die Bindung an den ESXi Host zurückgibt. Nach der Bindung kann der ESXi Host I/O-Vorgänge mit dem gebundenen virtuellen Volume ausführen.

Protokollendpunkte

VMware ESXi Hosts verwenden logische I/O-Proxys – als Protokollendpunkte bezeichnet –, um mit virtuellen

Volumes zu kommunizieren. ESXi Hosts binden virtuelle Volumes an Protokollendpunkte, um I/O-Vorgänge durchzuführen. Wenn eine virtuelle Maschine auf dem Host einen I/O-Vorgang durchführt, leitet der zugehörige Protokollendpunkt den I/O-Vorgang an das virtuelle Volume, mit dem sie gekoppelt wird.

Protokollendpunkte in einem NetApp Element-Cluster funktionieren als logische SCSI-Verwaltungseinheiten. Jeder Protokollendpunkt wird automatisch vom Cluster erstellt. Für jeden Node in einem Cluster wird ein entsprechender Protokollendpunkt erstellt. Ein Cluster mit vier Nodes verfügt beispielsweise über vier Protokollendpunkte.

ISCSI ist das einzige unterstützte Protokoll für die NetApp Element-Software. Das Fibre Channel-Protokoll wird nicht unterstützt. Protokollendpunkte können nicht von einem Benutzer gelöscht oder geändert werden, sind keinem Konto zugeordnet und können nicht einer Volume-Zugriffsgruppe hinzugefügt werden.

Storage-Container

Storage-Container sind logische Konstrukte, die NetApp Element-Konten zugewiesen werden und für die Berichterstellung und Ressourcenzuweisung verwendet werden. Sie bilden die Brutto-Storage-Kapazität oder aggregierte Storage-Funktionen, die das Storage-System virtuellen Volumes zur Verfügung stellen kann. Ein VVol Datastore, der in vSphere erstellt wird, wird einem einzelnen Storage-Container zugeordnet. Ein einzelner Storage-Container verfügt standardmäßig über alle verfügbaren Ressourcen des NetApp Element-Clusters. Falls mehr granulare Governance für Mandantenfähigkeit erforderlich ist, können auch mehrere Storage Container erstellt werden.

Storage-Container funktionieren wie herkömmliche Konten und können sowohl virtuelle Volumes als auch herkömmliche Volumes enthalten. Pro Cluster werden maximal vier Storage-Container unterstützt. Zur Nutzung der VVols Funktionen ist mindestens ein Storage-Container erforderlich. Sie können Storage-Container bei der VVols Erstellung in vCenter erkennen.

VASA-Provider

Um vSphere auf die vVol Funktion im NetApp Element Cluster aufmerksam zu machen, muss der vSphere Administrator den NetApp Element VASA Provider mit vCenter registrieren. Der VASA Provider ist der Out-of-Band-Kontrollpfad zwischen vSphere und dem Element Cluster. Er ist verantwortlich für die Ausführung von Anfragen im Element Cluster im Auftrag von vSphere, z. B. die Erstellung von VMs, die Bereitstellung von VMs für vSphere und die Werbung für Storage-Funktionen für vSphere.

Der VASA Provider wird als Teil des Cluster-Master in der Element Software ausgeführt. Der Cluster-Master ist ein hochverfügbarer Service, der bei Bedarf ein Failover auf jeden Node im Cluster ermöglicht. Bei einem Failover des Cluster-Master übernimmt der VASA Provider die Lösung und stellt damit die Hochverfügbarkeit für den VASA-Provider sicher. Alle Provisionierungs- und Storage-Managementaufgaben verwenden den VASA-Provider, der alle erforderlichen Änderungen am Element Cluster übernimmt.

Registrieren Sie bei Element 12.5 und früheren Versionen nicht mehr als einen NetApp Element VASA Provider in einer einzelnen vCenter Instanz. Wenn ein zweiter NetApp Element VASA Provider hinzugefügt wird, macht das alle VVOL Datastores unzugänglich.

VASA-Unterstützung für bis zu 10 vCenters steht als Upgrade-Patch zur Verfügung, wenn Sie bereits einen VASA Provider bei vCenter registriert haben. Befolgen Sie zur Installation die Anweisungen im VASA39-Manifest, und laden Sie die Datei .tar.gz von der Site herunter"NetApp Software-Downloads". Der NetApp Element VASA Provider verwendet ein NetApp Zertifikat. Bei diesem Patch wird das Zertifikat von vCenter nicht verändert, um mehrere vCenters für die Verwendung von VASA und VVols zu unterstützen. Ändern Sie das Zertifikat nicht. Benutzerdefinierte SSL-Zertifikate werden von VASA nicht unterstützt.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Volume-Zugriffsgruppen

Durch die Erstellung und Nutzung von Volume-Zugriffsgruppen können Sie den Zugriff auf eine Gruppe von Volumes steuern. Wenn Sie einen Satz von Volumes und einen Satz von Initiatoren einer Volume-Zugriffsgruppe zuordnen, gewährt die Zugriffsgruppe diesen Initiatoren Zugriff auf diese Gruppe von Volumes.

Volume-Zugriffsgruppen im NetApp SolidFire Storage ermöglichen den Zugriff auf eine Sammlung von Volumes durch iSCSI-Initiator-IQNs oder Fibre Channel-WWPNs. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann ohne CHAP-Authentifizierung auf jedes Volume in der Gruppe zugreifen. Jeder WWPN, den Sie einer Zugriffsgruppe hinzufügen, ermöglicht den Fibre-Channel-Netzwerkzugriff auf die Volumes in der Zugriffsgruppe.

Volume-Zugriffsgruppen verfügen über die folgenden Grenzen:

- Maximal 128 Initiatoren pro Volume-Zugriffsgruppe.
- Maximal 64 Zugriffsgruppen pro Volume.
- Eine Zugriffsgruppe kann aus maximal 2000 Volumes bestehen.
- Ein IQN oder WWPN kann nur zu einer Volume-Zugriffsgruppe gehören.
- Bei Fibre Channel Clustern kann ein einzelnes Volume zu maximal vier Zugriffsgruppen gehören.

Initiatoren

Initiatoren ermöglichen den Zugriff auf externe Clients auf Volumes in einem Cluster. Diese dienen als Einstiegspunkt für die Kommunikation zwischen Clients und Volumes. Sie können Initiatoren für CHAP-basierten Zugriff anstelle von kontenbasierten Speichervolumes verwenden. Wenn ein einzelner Initiator einer Volume-Zugriffsgruppe hinzugefügt wird, können die Mitglieder der Volume-Zugriffsgruppen auf alle der Gruppe hinzugefügten Storage Volumes zugreifen, ohne dass eine Authentifizierung erforderlich ist. Ein Initiator kann nur einer Zugriffsgruppe angehören.

Datensicherung

Zu den Datensicherungsfunktionen gehören Remote-Replizierung, Volume Snapshots, Volume-Klonen, Protection Domains und Hochverfügbarkeit mit Double Helix Technologie.

Element Storage-Datensicherung umfasst folgende Konzepte:

- Typen der Remote-Replizierung
- Volume Snapshots zur Datensicherung
- Volume-Klone

- Übersicht über Backup- und Restore-Prozesse für Element Storage
- Sicherungsdomänen
- Benutzerdefinierte Sicherungsdomänen
- Hochverfügbarkeit mit Double Helix

Typen der Remote-Replizierung

Die Remote-Replikation von Daten kann folgende Formen annehmen:

- Synchrone und asynchrone Replizierung zwischen Clustern
- Reine Snapshot Replizierung
- Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Weitere Informationen finden Sie unter "TR-4741: NetApp Element Software Remote Replication".

Synchrone und asynchrone Replizierung zwischen Clustern

Für Cluster mit NetApp Element Software ermöglicht Echtzeitreplizierung die schnelle Erstellung von Remote-Kopien von Volume-Daten.

Ein Storage-Cluster kann mit bis zu vier anderen Storage-Clustern gekoppelt werden. Sie können Volume-Daten für Failover- und Failback-Szenarien synchron oder asynchron von einem Cluster in einem Cluster-Paar replizieren.

Synchrone Replizierung

Die synchrone Replizierung repliziert die Daten kontinuierlich vom Quell-Cluster zum Ziel-Cluster und wird von Latenz, Paketverlust, Jitter und Bandbreite beeinträchtigt.

Synchrone Replizierung eignet sich für die folgenden Situationen:

- Replizierung mehrerer Systeme über kurze Entfernungen
- Ein Disaster-Recovery-Standort lokal an der Quelle
- Zeitkritische Applikationen und der Schutz von Datenbanken
- Business-Continuity-Applikationen, bei denen der sekundäre Standort als primärer Standort fungieren muss, wenn der primäre Standort ausfällt

Asynchrone Replizierung

Die asynchrone Replikation repliziert kontinuierlich Daten von einem Quellcluster zu einem Zielcluster, ohne auf die Bestätigungen aus dem Zielcluster zu warten. Während der asynchronen Replizierung werden Schreibvorgänge dem Client (Applikation) bestätigt, nachdem sie im Quell-Cluster durchgeführt wurden.

Asynchrone Replizierung eignet sich für die folgenden Situationen:

- Der Disaster-Recovery-Standort ist weit von der Quelle entfernt und die Applikation toleriert keine durch das Netzwerk verursachten Latenzen.
- Das Netzwerk, das die Quell- und Ziel-Cluster verbindet, weist Bandbreiteneinschränkungen auf.

Reine Snapshot Replizierung

Bei der Datensicherung nur mit Snapshots werden geänderte Daten zu einem bestimmten Zeitpunkt in ein Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume sind nicht.

Sie können die Häufigkeit der Snapshot Replikationen festlegen.

Die Snapshot Replizierung hat keine Auswirkungen auf die asynchrone oder synchrone Replizierung.

Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Mit der NetApp SnapMirror Technologie können Snapshots repliziert werden, die mit NetApp Element Software für Disaster Recovery-Zwecke in ONTAP erstellt wurden. In einer SnapMirror Beziehung stellt Element einen Endpunkt dar, und ONTAP ist der andere.

SnapMirror ist eine NetApp Snapshot Replizierungstechnologie für Disaster Recovery, die für das Failover von primärem Storage auf sekundärem Storage an einem externen Standort ausgelegt ist. Die SnapMirror Technologie erstellt ein Replikat bzw. eine Spiegelung der Arbeitsdaten im sekundären Storage, von dem aus Sie bei einem Ausfall am primären Standort weiterhin Daten bereitstellen können. Daten werden auf Volume-Ebene gespiegelt.

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als Datensicherungsbeziehung bezeichnet. Die Cluster werden als Endpunkte bezeichnet, in denen sich die Volumes befinden und die Volumes, die die replizierten Daten enthalten, müssen peed sein. Eine Peer-Beziehung ermöglicht einen sicheren Datenaustausch zwischen Clustern und Volumes.

SnapMirror wird nativ auf den NetApp ONTAP Controllern ausgeführt und ist in Element integriert, das auf NetApp HCI und SolidFire Clustern ausgeführt wird. Die Logik zur Steuerung von SnapMirror befindet sich in ONTAP Software. Daher müssen alle SnapMirror Beziehungen mindestens ein ONTAP System erfordern, um die Koordination durchzuführen. Benutzer managen die Beziehungen zwischen Element- und ONTAP-Clustern. Dies erfolgt hauptsächlich über die Element UI. Einige Managementaufgaben befinden sich jedoch im NetApp ONTAP System Manager. Benutzer können SnapMirror auch über die CLI und die API managen, die sowohl in ONTAP als auch in Element verfügbar sind.

Siehe "TR-4651: NetApp SolidFire SnapMirror Architektur und Konfiguration" (Anmeldung erforderlich)

Sie müssen die SnapMirror Funktion auf Cluster-Ebene manuell mit der Element Software aktivieren. Die SnapMirror Funktion ist standardmäßig deaktiviert und wird nicht automatisch im Rahmen einer neuen Installation oder eines Upgrades aktiviert.

Nach der Aktivierung von SnapMirror können Sie SnapMirror Beziehungen über die Registerkarte Datensicherung in der Element Software erstellen.

NetApp Element Software 10.1 und höher unterstützt SnapMirror Funktionen zum Kopieren und Wiederherstellen von Snapshots mit ONTAP Systemen.

Systeme mit Element 10.1 und höher beinhalten Code, der direkt mit SnapMirror auf ONTAP Systemen mit 9.3 oder höher kommunizieren kann. Die Element API bietet Methoden zur Aktivierung der SnapMirror Funktion in Clustern, Volumes und Snapshots. Zudem umfasst die Element UI Funktionen zum Managen von SnapMirror Beziehungen zwischen Element Software und ONTAP Systemen.

Beginnend mit Element 10.3 und ONTAP 9.4 Systemen können ONTAP-basierte Volumes in Element Volumes repliziert werden, und zwar in bestimmten Anwendungsfällen mit eingeschränkter Funktionalität.

Weitere Informationen finden Sie in der ONTAP-Dokumentation.

Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes, mit der Sie später ein Volume auf diesen speziellen Zeitpunkt wiederherstellen können.

Während Snapshots einem Volume-Klon ähneln, sind Snapshots lediglich Replikate von Volume-Metadaten. Sie können also nicht mounten oder darauf schreiben. Das Erstellen eines Volume-Snapshots nimmt ebenfalls nur eine geringe Menge an Systemressourcen und Platz in Anspruch, sodass die Snapshot-Erstellung schneller als das Klonen erfolgt.

Sie können Snapshots in einem Remote-Cluster replizieren und als Sicherungskopie des Volumes verwenden. Dadurch können Sie ein Rollback eines Volumes zu einem bestimmten Zeitpunkt mit dem replizierten Snapshot durchzuführen. Sie können auch einen Klon eines Volumes aus einem replizierten Snapshot erstellen.

Sie können ein Backup von Snapshots aus einem Element Cluster auf einem externen Objektspeicher oder auf einem anderen Element Cluster erstellen. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, müssen Sie über eine Verbindung zum Objektspeicher verfügen, der Lese-/Schreibvorgänge ermöglicht.

Sie können einen Snapshot eines einzelnen Volumes oder mehrerer zur Datensicherheit erstellen.

Volume-Klone

Ein Klon eines einzelnen oder mehrerer Volumes ist eine zeitpunktgenaue Kopie der Daten. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist.

Dies ist ein asynchroner Prozess und die erforderliche Zeit hängt von der Größe des zum Klonen benötigten Volumes und der aktuellen Cluster-Last ab.

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu acht aktive Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

Übersicht über Backup- und Restore-Prozesse für Element Storage

Backups und Restores von Volumes mit anderen SolidFire Storage-Systemen sowie in sekundären Objektspeichern mit Amazon S3 oder OpenStack Swift möglich.

Sie können ein Volume unter folgender Adresse sichern:

- Ein SolidFire Storage-Cluster
- Ein Amazon S3-Objektspeicher
- OpenStack Swift Objektspeicher

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifest-Informationen aus dem ursprünglichen Backup-Prozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire Storage-System gesichert wurde, sind keine Manifest-Informationen erforderlich.

Sicherungsdomänen

Eine Protection Domain ist ein Knoten oder eine Gruppe von Knoten, die so gruppiert sind, dass ein Teil oder sogar alle Knoten ausfallen könnten, ohne dass die Datenverfügbarkeit beeinträchtigt wird. Protection-Domänen ermöglichen es einem Storage-Cluster, automatisch den Verlust eines Chassis (Chassis-Affinität) oder einer gesamten Domäne (Chassis-Gruppe) zu heilen.

Sie können die Überwachung der Schutzdomäne manuell mit dem Erweiterungspunkt für die NetApp Element-Konfiguration im NetApp Element-Plug-in für vCenter Server aktivieren. Sie können einen Schutz-Domain-Schwellenwert basierend auf Node- oder Chassis-Domänen auswählen. Sie können die Überwachung von Schutzdomänen auch über die Element-API oder die Web-Benutzeroberfläche aktivieren.

Ein Protection Domain-Layout weist jeden Knoten einer bestimmten Protection Domain zu.

Es werden zwei unterschiedliche Protection Domain Layouts unterstützt, sogenannte Protection Domain Levels.

- Auf Node-Ebene befindet sich jeder Node in einer eigenen Protection Domain.
- Auf Chassis-Ebene befinden sich nur Nodes, die sich ein Chassis teilen, in derselben Protection Domain.
  - Das Layout auf Chassis-Ebene wird automatisch von der Hardware bestimmt, wenn der Node zum Cluster hinzugefügt wird.
  - In einem Cluster, in dem sich jeder Node in einem separaten Chassis befindet, sind diese beiden Ebenen funktional identisch.

Wenn Sie ein neues Cluster erstellen und Storage-Nodes verwenden, die sich in einem gemeinsam genutzten Chassis befinden, sollten Sie möglicherweise über die Protection Domains-Funktion einen Ausfallschutz auf Chassis-Ebene in Betracht ziehen.

Benutzerdefinierte Schutzdomänen

Sie können ein benutzerdefiniertes Schutz-Domain-Layout definieren, das Ihrem spezifischen Gehäuse- und Node-Layout entspricht und wo jeder Knoten mit einer und nur einer benutzerdefinierten Schutzdomäne verknüpft ist. Standardmäßig ist jeder Knoten derselben benutzerdefinierten Standard-Schutzdomäne zugewiesen.

Falls keine benutzerdefinierten Sicherungsdomänen zugewiesen sind:

- Der Cluster-Vorgang wird nicht beeinträchtigt.
- Die benutzerdefinierte Ebene ist weder tolerant noch widerstandsfähig.

Wenn Sie benutzerdefinierte Protection Domains für einen Cluster konfigurieren, gibt es drei mögliche Schutzstufen, die Sie im Element Web UI Dashboard sehen können:

- Nicht geschützt: Das Speicher-Cluster ist nicht vor dem Ausfall einer seiner benutzerdefinierten Schutz-Domains geschützt. Um dies zu beheben, fügen Sie dem Cluster zusätzliche Speicherkapazität hinzu oder konfigurieren Sie die benutzerdefinierten Schutz-Domains des Clusters neu, um das Cluster vor möglichen Datenverlusten zu schützen.
- Fehlertolerant: Der Speicher-Cluster verfügt über genügend freie Kapazität, um Datenverlust nach dem Ausfall einer seiner benutzerdefinierten Schutz-Domains zu verhindern.
- Fehler ausfallsicher: Der Speicher-Cluster verfügt über genügend freie Kapazität, um sich nach dem Ausfall einer seiner benutzerdefinierten Schutz-Domains selbst zu heilen. Nach Abschluss des Heilungsprozesses wird das Cluster vor Datenverlust geschützt, wenn weitere Domänen ausfallen sollten.

Wenn mehr als eine benutzerdefinierte Schutzdomäne zugewiesen wird, weist jedes Subsystem Duplikate zu separaten benutzerdefinierten Schutzdomänen zu. Ist dies nicht möglich, so wird das Zuweisen von Duplikaten zu separaten Nodes rückgängig gemacht. Jedes Subsystem (z. B. Behälter, Schichten, Protokollendpunktanbieter und Ensemble) erledigt dies unabhängig voneinander.

Sie können die Element-Benutzeroberfläche verwenden"Konfigurieren Sie benutzerdefinierte Sicherungsdomänen", um , oder Sie können die folgenden API-Methoden verwenden:

- "GetProtectionDomainLayout" - Zeigt an, in welchem Gehäuse und in welcher benutzerdefinierten Schutzdomäne sich jeder Knoten befindet.
- "SetProtectionDomainLayout" - Ermöglicht die Zuweisung einer benutzerdefinierten Schutzdomäne zu jedem Knoten.

Hochverfügbarkeit mit Double Helix

Die Double Helix Datensicherung ist eine Replizierungsmethode, die mindestens zwei redundante Datenkopien auf alle Laufwerke innerhalb eines Systems verteilt. Der Ansatz „RAID-less“ ermöglicht es einem System, mehrere gleichzeitige Ausfälle auf allen Ebenen des Storage-Systems zu absorbieren und schnell zu reparieren.

Leistung und Servicequalität

Ein SolidFire Storage Cluster bietet QoS-Parameter (Quality of Service) für einzelne Volumes. Sie können die Cluster-Performance, die in ein- und Ausgaben pro Sekunde (IOPS) gemessen wird, mit drei konfigurierbaren Parametern garantieren, die QoS definieren: Das IOPS-Minimum, das IOPS-Maximum und die Burst-IOPS.

SolidFire Active IQ verfügt über eine Seite mit QoS-Empfehlungen zur optimalen Konfiguration und Einrichtung von QoS-Einstellungen.

Parameter für die Servicequalität

IOPS-Parameter werden folgendermaßen definiert:

- **Minimum IOPS** - die Mindestanzahl kontinuierlicher ein- und Ausgänge pro Sekunde (IOPS), die der Storage Cluster einem Volume zur Verfügung stellt. Die für ein Volume konfigurierten IOPS-Mindestwerte sind das garantierte Performance-Niveau für ein Volume. Die Performance sinkt nicht unter dieses Niveau.
- **Maximale IOPS** - die maximale Anzahl an anhaltenden IOPS, die der Storage Cluster einem Volume zur Verfügung stellt. Wenn Cluster-IOPS-Niveaus kritisch hoch sind, wird diese IOPS-Performance nicht überschritten.
- **Burst IOPS** - die maximale Anzahl von IOPS in einem kurzen Burst Szenario erlaubt. Wenn ein Volume unter dem IOPS-Maximum ausgeführt wurde, werden Burst Credits gesammelt. Wenn Performance-Level sehr hoch sind und auf ein Maximum geschoben werden, sind kurze Anstiegen von IOPS auf dem Volume zulässig.

  Element Software verwendet Burst IOPS, wenn ein Cluster eine niedrige IOPS-Auslastung aufweist.

  Ein einzelnes Volume kann Burst-IOPS anhäufen und die Gutschriften verwenden, um über ihren maximalen IOPS bis zu ihrem IOPS-Burst-Level für einen festgelegten „Burst-Zeitraum“ zu steigen. Ein Volume kann bis zu 60 Sekunden lang hochgehen, wenn das Cluster über die Kapazität verfügt, um die Burst-Kapazität aufzunehmen. Ein Volume kann für jede Sekunde, in der das Volume unter seinem

maximalen IOPS-Limit ausgeführt wird, eine Sekunde Burst Credit (bis zu einem Maximum von 60 Sekunden) angesammelt werden.

Die IOPS-Burst-IOPS-Werte sind auf zwei Arten begrenzt:

- Ein Volume kann für einige Sekunden einen Spitzenwert über dem maximalen IOPS erzielen, der der Anzahl der Burst Credits entspricht, die es beim Volume gesammelt hat.
- Wenn ein Volume über die Einstellung für maximale IOPS platzt, ist es durch die Einstellung für Burst IOPS eingeschränkt. Daher überschreitet der IOPS-Burst niemals die Burst-IOPS-Einstellung für das Volume.

- **Effektive max. Bandbreite** - die maximale Bandbreite wird berechnet, indem die Anzahl der IOPS (basierend auf der QoS-Kurve) mit der I/O-Größe multipliziert wird.

  Beispiel: QoS-Parametereinstellungen für 100 Min IOPS, 1000 Max IOPS und 1500 Burst IOPS wirken sich auf die Performance-Qualität aus:

  - Workloads können ein Maximum von 1000 IOPS erreichen und halten, bis sich der Zustand von Workload-Engpässen für IOPS im Cluster bemerkbar macht. Die IOPS werden dann inkrementell reduziert, bis sich die IOPS auf allen Volumes innerhalb der designierten QoS-Bereiche befinden und die Konflikte für die Performance sinken.
  - Die Performance auf allen Volumes wird über den Mindestwert von 100 IOPS erreicht. Die Werte sinken nicht unter die Einstellung für Min IOPS, könnten aber bei Entlastung der Workloads über 100 IOPS bleiben.
  - Die Performance beträgt in einem kontinuierlichen Zeitraum niemals mehr als 1000 IOPS oder weniger als 100 IOPS. Die Performance von 1500 IOPS (Burst IOPS) ist zulässig, aber nur für die Volumes, die Burst Credits aufgesammelt haben, wenn sie unter dem IOPS-Maximum laufen und nur für kurze Zeit zulässig sind. Burst-Werte werden niemals aufrechterhalten.

QoS-Wertbegrenzungen

Hier sind die möglichen Mindest- und Höchstwerte für QoS.

Parameter	Mindestwert	Standard	4 4 KB	5 8 KB	6 16 KB	262KB
IOPS-Minimum	50	50	15.000	9,375*	5556*	385*
IOPS-Maximum	100	15.000	200,000**	125.000	74.074	5128
IOPS-Burst	100	15.000	200,000**	125.000	74,074	5128

*Diese Schätzungen sind ungefähr. **Maximale IOPS und Burst IOPS können auf 200,000 gesetzt werden. Diese Einstellung ist jedoch nur erlaubt, die Performance eines Volumes effektiv zu nutzen. Die tatsächliche maximale Performance eines Volumes wird durch die Auslastung des Clusters und die Performance pro Node begrenzt.

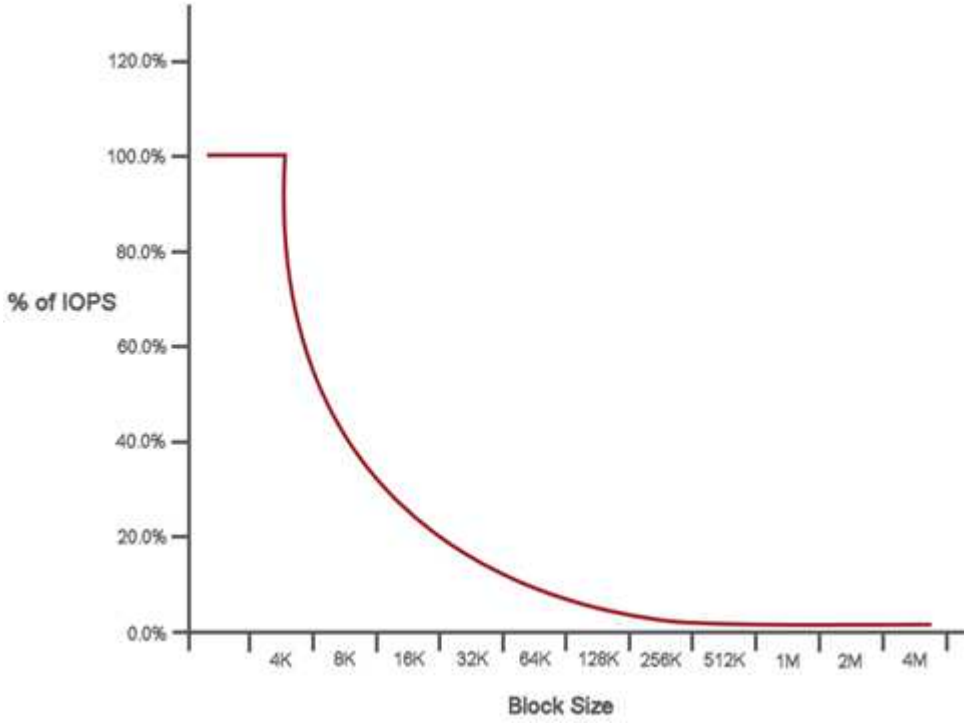
QoS-Performance

Die QoS-Performance-Kurve zeigt die Beziehung zwischen Blockgröße und dem Prozentsatz der IOPS.

Die Blockgröße und die Bandbreite haben direkte Auswirkungen auf die Anzahl der IOPS, die eine Applikation erreichen kann. Element Software berücksichtigt die Blockgröße, die durch die Normalisierung der

Blockgrößen auf 4 kb erhält. Je nach Workload kann das System die Blockgrößen erhöhen. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das für die Verarbeitung größerer Blockgrößen erforderlich ist. Mit einer höheren Bandbreite verringert sich auch die Anzahl an IOPS, die das System erreichen kann.

Die QoS-Performance-Kurve zeigt die Beziehung zwischen zunehmenden Blockgrößen und dem sinkenden Prozentsatz an IOPS:



Wenn Blockgröße beispielsweise 4 kb und eine Bandbreite 4000 kbit/s beträgt, betragen die IOPS 1000. Bei einer Blockgröße von bis zu 8.000 USD erhöht sich die Bandbreite auf 5000 kBit/s und der IOPS-Wert sinkt auf 625. Unter Berücksichtigung der Blockgröße übernimmt das System dafür, dass Workloads mit niedrigerer Priorität, bei denen größere Blockgrößen zum Beispiel Backups und Hypervisor-Aktivitäten verwendet werden, nicht zu viele der Performance in Anspruch nehmen, die durch Datenverkehr mit höherer Priorität durch kleinere Blöcke benötigt wird.

QoS-Richtlinien (QoS

Mit einer QoS-Richtlinie können Sie standardisierte Quality-of-Service-Einstellungen erstellen und speichern, die auf viele Volumes angewendet werden können.

QoS-Richtlinien eignen sich am besten für Serviceumgebungen, beispielsweise mit Datenbank-, Applikations- oder Infrastrukturservern, die selten neu gestartet werden und den konstanten Zugriff auf den Storage benötigen. Einzelne Volume-QoS eignet sich am besten für lichtstarke VMs, z. B. virtuelle Desktops oder spezielle VMs mit Kiosk-Typ. Diese können täglich neu gestartet, eingeschaltet oder mehrfach ausgeschaltet werden.

QoS- und QoS-Richtlinien sollten nicht gemeinsam eingesetzt werden. Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

Der ausgewählte Cluster muss zur Verwendung von QoS-Richtlinien Element 10.0 oder höher sein. Anderenfalls sind QoS-Richtlinienfunktionen nicht verfügbar.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"