Konzepte

Element Software

NetApp
November 18, 2025

Inhalt

Konzepte

Lernen Sie die grundlegenden Konzepte der Element-Software kennen.

- "Produktübersicht"
- SolidFire -Architekturübersicht
- Nodes
- Cluster
- "Sicherheit"
- Konten und Berechtigungen
- "Bände"
- Datenschutz
- Leistung und Servicequalität

Produktübersicht

Ein SolidFire All-Flash-Speichersystem besteht aus einzelnen Hardwarekomponenten (Laufwerk und Knoten), die zu einem einzigen Pool von Speicherressourcen kombiniert werden. Dieser einheitliche Cluster stellt sich externen Clients als ein einziges Speichersystem zur Verfügung und wird mit der NetApp Element Software verwaltet.

Mithilfe der Element-Oberfläche, der API oder anderer Management-Tools können Sie die Speicherkapazität und Leistung des SolidFire Clusters überwachen und die Speicheraktivität in einer Multi-Tenant-Infrastruktur verwalten.

SolidFire Funktionen

Ein Solidfire-System bietet folgende Funktionen:

- Bietet leistungsstarken Speicher für Ihre groß angelegte, private Cloud-Infrastruktur
- Bietet eine flexible Skalierbarkeit, die es Ihnen ermöglicht, sich ändernden Speicheranforderungen gerecht zu werden.
- Nutzt eine API-gesteuerte Element-Softwareschnittstelle für das Speichermanagement
- Gewährleistet die Leistung durch die Anwendung von Richtlinien zur Servicequalität.
- Beinhaltet automatischen Lastausgleich über alle Knoten im Cluster
- Automatische Neuausrichtung der Cluster beim Hinzufügen oder Entfernen von Knoten

SolidFire Einsatz

Nutzen Sie von NetApp bereitgestellte und in die NetApp Element Software integrierte Speicherknoten.

"Überblick über die SolidFire All-Flash-Speicherarchitektur"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"

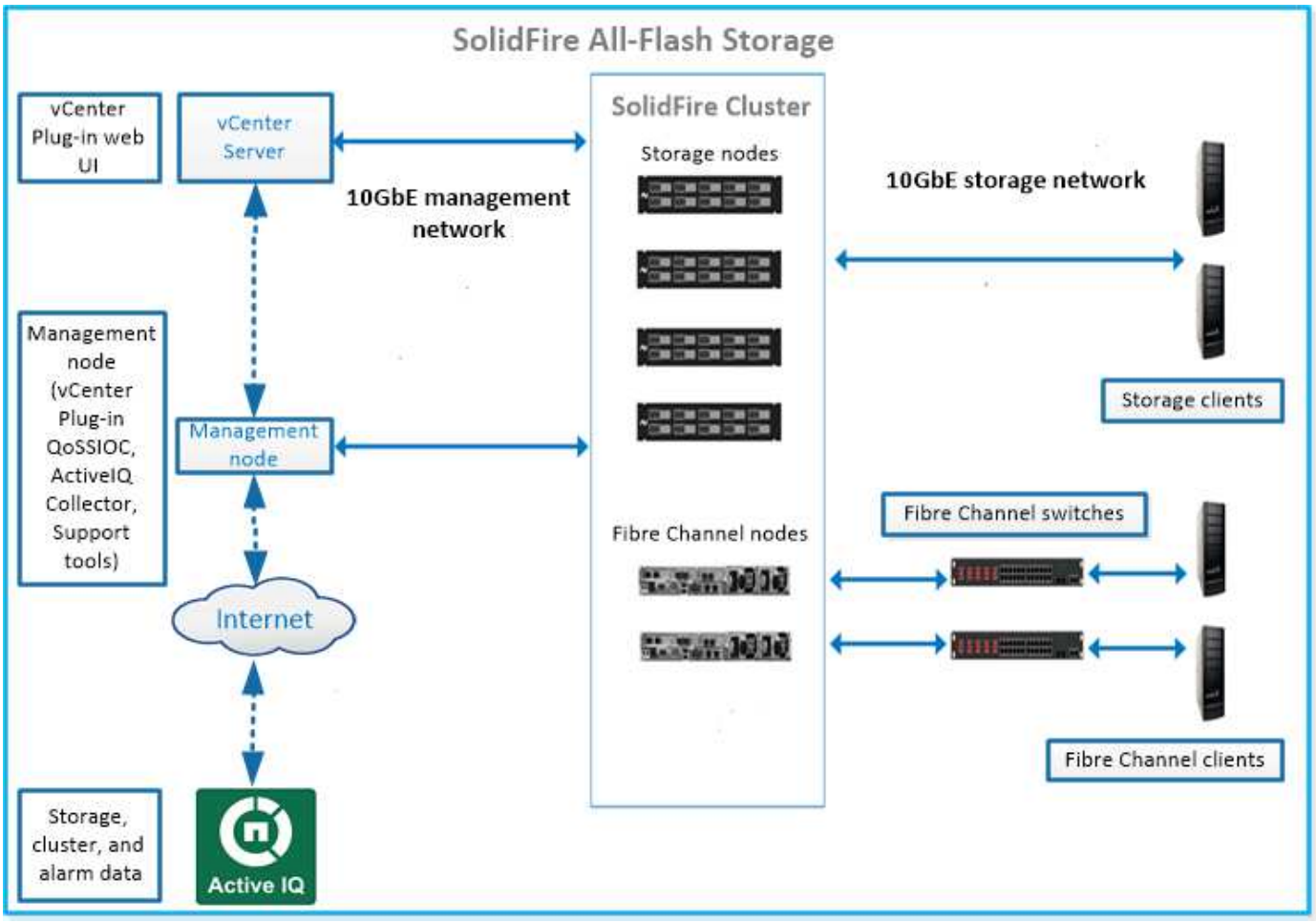
Architektur und Komponenten

Erfahren Sie mehr über die SolidFire -Architektur.

Ein SolidFire All-Flash-Speichersystem besteht aus einzelnen Hardwarekomponenten (Laufwerken und Knoten), die zu einem Pool von Speicherressourcen kombiniert werden, wobei die NetApp Element Software unabhängig auf jedem Knoten läuft. Dieses einzelne Speichersystem wird als eine Einheit mithilfe der Element-Software-Benutzeroberfläche, der API und anderer Verwaltungstools verwaltet.

Ein SolidFire -Speichersystem umfasst folgende Hardwarekomponenten:

- **Cluster**: Der zentrale Knotenpunkt des SolidFire -Speichersystems, der aus einer Sammlung von Knoten besteht.
- **Knoten**: Die zu einem Cluster gruppierten Hardwarekomponenten. Es gibt zwei Arten von Knoten:
  - Speicherknoten sind Server, die eine Sammlung von Laufwerken enthalten.
  - Fibre Channel (FC)-Knoten, die Sie verwenden, um eine Verbindung zu FC-Clients herzustellen
- **Laufwerke**: Werden in Speicherknoten verwendet, um Daten für den Cluster zu speichern. Ein Speicherknoten enthält zwei Arten von Laufwerken:
  - Volume-Metadaten speichern Informationen, die die Volumes und andere Objekte innerhalb eines Clusters definieren.
  - Blocklaufwerke speichern Datenblöcke für Datenträger.



Sie können das System mithilfe der Element-Weboberfläche und anderer kompatibler Tools verwalten, überwachen und aktualisieren:

- "SolidFire Softwareschnittstellen"
- "SolidFire Active IQ"
- "Verwaltungsknoten für die Element-Software"
- "Managementdienstleistungen"

Häufige URLs

Dies sind die gängigen URLs, die Sie mit einem SolidFire All-Flash-Speichersystem verwenden:

URL	Beschreibung
`https://[storage cluster MVIP address]`	Greifen Sie auf die Benutzeroberfläche der NetApp Element Software zu.
`https://activeiq.solidfire.com`	Überwachen Sie Daten und erhalten Sie Benachrichtigungen über etwaige Leistungsengpässe oder potenzielle Systemprobleme.
`https://[management node IP address]`	Greifen Sie auf NetApp Hybrid Cloud Control zu, um Ihre Speicherinstallation zu aktualisieren und die Verwaltungsdienste zu aktualisieren.

URL	Beschreibung
`https://[IP address]:442`	Über die Benutzeroberfläche pro Knoten können Sie auf Netzwerk- und Clustereinstellungen zugreifen und Systemtests und -hilfsmittel nutzen."Erfahren Sie mehr."
`https://[management node IP address]/mnode`	Nutzen Sie die REST-API der Managementdienste und weitere Funktionen des Managementknotens."Erfahren Sie mehr."
`https://[management node IP address]:9443`	Registrieren Sie das vCenter-Plug-in-Paket im vSphere Web Client."Erfahren Sie mehr."

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

SolidFire Softwareschnittstellen

Ein SolidFire -Speichersystem kann mithilfe verschiedener NetApp Element -Softwareschnittstellen und Integrationsprogramme verwaltet werden.

Optionen

- NetApp Element Software-Benutzeroberfläche
- NetApp Element Software-API
- NetApp Element Plug-in für vCenter Server
- NetApp Hybrid Cloud Control
- Benutzeroberflächen der Verwaltungsknoten
- Zusätzliche Integrationshilfsmittel und -werkzeuge

NetApp Element Software-Benutzeroberfläche

Ermöglicht die Einrichtung von Element-Speicher, die Überwachung der Clusterkapazität und -leistung sowie die Verwaltung der Speicheraktivitäten in einer Multi-Tenant-Infrastruktur. Element ist das Speicherbetriebssystem, das das Herzstück eines SolidFire Clusters bildet. Die Element-Software läuft unabhängig auf allen Knoten im Cluster und ermöglicht es den Knoten des Clusters, Ressourcen zu kombinieren, die externen Clients als ein einziges Speichersystem präsentiert werden. Die Element-Software ist für die gesamte Clusterkoordination, Skalierung und Verwaltung des Gesamtsystems verantwortlich. Die Softwareschnittstelle basiert auf der Element API.

"Speicherverwaltung mit der Element-Software"

NetApp Element Software-API

Ermöglicht die Verwendung einer Reihe von Objekten, Methoden und Routinen zur Verwaltung des Elementspeichers. Die Element-API basiert auf dem JSON-RPC-Protokoll über HTTPS. Sie können API-Operationen in der Element-Benutzeroberfläche überwachen, indem Sie das API-Protokoll aktivieren; dadurch können Sie die an das System gesendeten Methoden einsehen. Sie können sowohl Anfragen als auch Antworten aktivieren, um zu sehen, wie das System auf die aufgerufenen Methoden reagiert.

"Speicherverwaltung mit der Element-API"

NetApp Element Plug-in für vCenter Server

Ermöglicht die Konfiguration und Verwaltung von Speicherclustern, auf denen die Element-Software läuft, über eine alternative Schnittstelle zur Element-Benutzeroberfläche innerhalb von VMware vSphere.

"NetApp Element Plug-in für vCenter Server"

NetApp Hybrid Cloud Control

Ermöglicht Ihnen die Aktualisierung der Element-Speicher- und Verwaltungsdienste sowie die Verwaltung von Speicherressourcen über die NetApp Hybrid Cloud Control-Schnittstelle.

"Speicher verwalten und überwachen mit NetApp Hybrid Cloud Control"

Benutzeroberflächen der Verwaltungsknoten

Der Management-Knoten enthält zwei Benutzeroberflächen: eine Benutzeroberfläche zur Verwaltung von REST-basierten Diensten und eine knotenspezifische Benutzeroberfläche zur Verwaltung von Netzwerk- und Clustereinstellungen sowie Betriebssystemtests und -dienstprogrammen. Über die REST-API-Benutzeroberfläche können Sie auf ein Menü mit dienstbezogenen APIs zugreifen, die die Funktionalität des dienstbasierten Systems vom Verwaltungsknoten aus steuern.

Zusätzliche Integrationshilfsmittel und -werkzeuge

Obwohl Sie Ihren Speicher üblicherweise mit NetApp Element, der NetApp Element API und dem NetApp Element Plug-in für vCenter Server verwalten, können Sie zusätzliche Integrationsprogramme und Tools verwenden, um auf den Speicher zuzugreifen.

Element CLI

"Element CLI"ermöglicht es Ihnen, ein SolidFire -Speichersystem über eine Befehlszeilenschnittstelle zu steuern, ohne die Element-API verwenden zu müssen.

Element PowerShell Tools

"Element PowerShell Tools"Ermöglicht Ihnen die Verwendung einer Sammlung von Microsoft Windows PowerShell-Funktionen, die die Element API verwenden, um ein SolidFire -Speichersystem zu verwalten.

Element SDKs

"Element SDKs"Mit diesen Tools können Sie Ihren SolidFire -Cluster verwalten:

- Element Java SDK: Ermöglicht Programmierern die Integration der Element API in die Programmiersprache Java.
- 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 die Nutzung einer Sammlung von"Briefträger" Funktionen, die Element-API-

Aufrufe testen.

SolidFire Speicherreplikationsadapter

"SolidFire Speicherreplikationsadapter"Integriert sich in VMware Site Recovery Manager (SRM), um die Kommunikation mit replizierten SolidFire Speicherclustern zu ermöglichen und unterstützte Workflows auszuführen.

SolidFire vRO

"SolidFire vRO"bietet eine komfortable Möglichkeit, die Element API zur Verwaltung Ihres SolidFire -Speichersystems mit VMware vRealize Orchestrator zu verwenden.

SolidFire VSS-Anbieter

"SolidFire VSS-Anbieter"Integriert VSS-Schattenkopien mit Element-Snapshots und -Klonen.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ"ist ein webbasiertes Tool, das kontinuierlich aktualisierte historische Ansichten von clusterweiten Daten bereitstellt. Sie können Benachrichtigungen für bestimmte Ereignisse, Schwellenwerte oder Kennzahlen einrichten. SolidFire Active IQ ermöglicht es Ihnen, die Systemleistung und -kapazität zu überwachen und sich über den Zustand des Clusters auf dem Laufenden zu halten.

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

- Anzahl der Knoten und Status der Knoten: betriebsbereit, offline oder fehlerhaft
- Grafische Darstellung der CPU-, Speichernutzung und Knotendrosselung
- Details zum Knoten, wie Seriennummer, Steckplatz im Gehäuse, Modell und Version der auf dem Speicherknoten ausgeführten NetApp Element -Software
- CPU- und speicherbezogene Informationen zu den virtuellen Maschinen

Um mehr über SolidFire Active IQ zu erfahren, siehe "SolidFire Active IQ Dokumentation" Die

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"
- **NetApp Supportseite › Tools für Active IQ**

Verwaltungsknoten für die Element-Software

Der"Managementknoten (mNode)" ist eine virtuelle Maschine, die parallel zu einem oder mehreren Element-Software-basierten Speicherclustern läuft. Es dient der Aktualisierung

und Bereitstellung von Systemdiensten, einschließlich Überwachung und Telemetrie, der Verwaltung von Clusterressourcen und -einstellungen, der Ausführung von Systemtests und -dienstprogrammen sowie der Ermöglichung des NetApp Supportzugriffs zur Fehlerbehebung.

Der Management-Knoten interagiert mit einem Speichercluster, um Managementaktionen durchzuführen, ist aber kein Mitglied des Speicherclusters. Die Management-Knoten sammeln regelmäßig Informationen über den Cluster mittels API-Aufrufen und melden diese Informationen an Active IQ zur Fernüberwachung (sofern aktiviert). Die Management-Knoten sind außerdem für die Koordinierung von Software-Upgrades der Cluster-Knoten zuständig.

Ab der Element-Version 11.3 fungiert der Management-Knoten als Microservice-Host, was schnellere Aktualisierungen ausgewählter Softwaredienste außerhalb von Hauptversionen ermöglicht. Diese Mikrodienste oder"Managementdienstleistungen" werden regelmäßig als Servicepakete aktualisiert.

Managementdienste für SolidFire All-Flash-Speicher

Ab der Element-Version 11.3 werden die **Verwaltungsdienste** auf dem"Verwaltungsknoten" Dies ermöglicht schnellere Aktualisierungen ausgewählter Softwaredienste außerhalb von Hauptversionen.

Die Management-Services bieten zentrale und erweiterte Verwaltungsfunktionen für SolidFire All-Flash-Speicher. Diese Dienstleistungen umfassen"NetApp Hybrid Cloud Control" , Active IQ Systemtelemetrie, Protokollierung und Service-Updates sowie der QoSSIOC-Dienst für das Element-Plug-in für vCenter.

Erfahren Sie mehr über"Management-Services-Releases" .

Nodes

Knoten sind Hardware- oder virtuelle Ressourcen, die zu einem Cluster zusammengefasst werden, um Blockspeicher- und Rechenkapazitäten bereitzustellen.

Die NetApp Element Software definiert verschiedene Knotenrollen für einen Cluster. Die Arten von Knotenrollen sind folgende:

- Verwaltungsknoten
- Speicherknoten
- Fibre Channel-Knoten

Knotenzuständevariieren je nach Clusterzugehörigkeit.

Verwaltungsknoten

Ein Management-Knoten ist eine virtuelle Maschine, die zur Aktualisierung und Bereitstellung von Systemdiensten wie Überwachung und Telemetrie, zur Verwaltung von Clusterressourcen und -einstellungen, zur Ausführung von Systemtests und -dienstprogrammen sowie zur Ermöglichung des NetApp Supportzugriffs für die Fehlerbehebung verwendet wird."Mehr erfahren"

Speicherknoten

Ein SolidFire -Speicherknoten ist ein Server, der eine Sammlung von Laufwerken enthält, die über die Bond10G-Netzwerkschnittstelle miteinander kommunizieren. Die Laufwerke im Knoten enthalten Block- und Metadatenspeicher für die Datenspeicherung und Datenverwaltung. Jeder Knoten enthält ein Werksabbild der NetApp Element -Software.

Speicherknoten weisen folgende Eigenschaften auf:

- Jeder Knoten hat einen eindeutigen Namen. Wird kein Knotenname von einem Administrator angegeben, wird standardmäßig SF-XXXX verwendet, wobei XXXX vier vom System generierte Zufallszeichen sind.
- Jeder Knoten verfügt über einen eigenen, leistungsstarken, nichtflüchtigen Direktzugriffsspeicher (NVRAM) als Schreibcache, um die Gesamtleistung des Systems zu verbessern und die Schreiblatenz zu reduzieren.
- Jeder Knoten ist mit zwei Netzwerken verbunden, einem Speichernetzwerk und einem Verwaltungsnetzwerk, die jeweils über zwei unabhängige Verbindungen für Redundanz und Leistung verfügen. Jeder Knoten benötigt eine IP-Adresse in jedem Netzwerk.
- Sie können einen Cluster mit neuen Speicherknoten erstellen oder einem bestehenden Cluster Speicherknoten hinzufügen, um die Speicherkapazität und die Leistung zu erhöhen.
- Sie können jederzeit Knoten zum Cluster hinzufügen oder daraus entfernen, ohne den Dienst zu unterbrechen.

Fibre Channel-Knoten

SolidFire Fibre Channel-Knoten bieten Konnektivität zu einem Fibre Channel-Switch, an den Sie Fibre Channel-Clients anschließen können. Fibre Channel-Knoten fungieren als Protokollkonverter zwischen den Fibre Channel- und iSCSI-Protokollen; dies ermöglicht es Ihnen, Fibre Channel-Konnektivität zu jedem neuen oder bestehenden SolidFire Cluster hinzuzufügen.

Fibre-Channel-Knoten weisen folgende Eigenschaften auf:

- Fibre-Channel-Switches verwalten den Zustand des Fabric und sorgen so für optimierte Verbindungen.
- Der Datenverkehr zwischen zwei Ports fließt ausschließlich über die Switches; er wird nicht an andere Ports weitergeleitet.
- Der Ausfall eines Ports ist ein isoliertes Problem und beeinträchtigt nicht den Betrieb anderer Ports.
- In einem Fabric können mehrere Portpaare gleichzeitig kommunizieren.

Betriebszustände der Knoten

Ein Knoten kann sich je nach Konfigurationsebene in einem von mehreren Zuständen befinden.

- **Verfügbar**

  Der Knoten hat keinen zugeordneten Clusternamen und ist noch nicht Teil eines Clusters.

- **Ausstehend**

  Der Knoten ist konfiguriert und kann einem bestimmten Cluster hinzugefügt werden.

  Für den Zugriff auf den Knoten ist keine Authentifizierung erforderlich.

- **Aktivierungsstatus ausstehend**

  Das System ist dabei, kompatible Element-Software auf dem Knoten zu installieren. Nach Abschluss des Vorgangs wechselt der Knoten in den aktiven Zustand.

- **Aktiv**

  Der Knoten ist Teil eines Clusters.

  Zur Änderung des Knotens ist eine Authentifizierung erforderlich.

In jedem dieser Zustände sind einige Felder schreibgeschützt.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

Cluster

Ein Cluster ist das Herzstück eines SolidFire -Speichersystems und besteht aus einer Sammlung von Knoten. Um die Speichereffizienzvorteile von SolidFire nutzen zu können, müssen Sie mindestens vier Knoten in einem Cluster haben. Ein Cluster erscheint im Netzwerk als eine einzige logische Gruppe und kann dann als Blockspeicher angesprochen werden.

Beim Erstellen eines neuen Clusters wird ein Knoten als Kommunikationsinhaber für den Cluster initialisiert und die Netzwerkkommunikation für jeden Knoten im Cluster eingerichtet. Dieser Vorgang wird für jeden neuen Cluster nur einmal durchgeführt. Sie können einen Cluster über die Element-Benutzeroberfläche oder die API erstellen.

Sie können einen Cluster skalieren, indem Sie zusätzliche Knoten hinzufügen. Beim Hinzufügen eines neuen Knotens kommt es zu keiner Unterbrechung des Dienstes, und der Cluster nutzt automatisch die Leistung und Kapazität des neuen Knotens.

Administratoren und Hosts können über virtuelle IP-Adressen auf den Cluster zugreifen. Jeder Knoten im Cluster kann die virtuellen IP-Adressen hosten. Die Management Virtual IP (MVIP) ermöglicht die Clusterverwaltung über eine 1GbE-Verbindung, während die Storage Virtual IP (SVIP) den Hostzugriff auf den Speicher über eine 10GbE-Verbindung ermöglicht. Diese virtuellen IP-Adressen ermöglichen konsistente Verbindungen unabhängig von der Größe oder Zusammensetzung eines SolidFire Clusters. Wenn ein Knoten, der eine virtuelle IP-Adresse hostet, ausfällt, übernimmt ein anderer Knoten im Cluster die Hosting der virtuellen IP-Adresse.

> Ab Element Version 11.0 können Knoten mit IPv4-, IPv6- oder beiden Adressen für ihr Managementnetzwerk konfiguriert werden. Dies gilt sowohl für Speicherknoten als auch für Verwaltungsknoten, mit Ausnahme des Verwaltungsknotens 11.3 und höher, der IPv6 nicht unterstützt. Bei der Erstellung eines Clusters kann nur eine einzige IPv4- oder IPv6-Adresse für den MVIP verwendet werden, und der entsprechende Adresstyp muss auf allen Knoten konfiguriert sein.

Mehr zu Clustern

- Autoritative Speichercluster
- Drittelregel
- Ungenutzte Kapazität
- Speichereffizienz
- Speichercluster-Quorum

Autoritative Speichercluster

Der autoritative Speichercluster ist der Speichercluster, den NetApp Hybrid Cloud Control zur Authentifizierung von Benutzern verwendet.

Wenn Ihr Management-Knoten nur über einen Speichercluster verfügt, dann ist dieser der autoritative Cluster. Wenn Ihr Management-Knoten über zwei oder mehr Speichercluster verfügt, wird einer dieser Cluster als autoritativer Cluster festgelegt, und nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden. Um herauszufinden, welcher Cluster der maßgebliche Cluster ist, können Sie Folgendes verwenden: `GET /mnode/about` API. In der Antwort wird die IP-Adresse in der `token_url` Das Feld ist die Management Virtual IP Address (MVIP) des autoritativen Speicherclusters. Wenn Sie versuchen, sich als Benutzer, der nicht zum autoritativen Cluster gehört, bei NetApp Hybrid Cloud Control anzumelden, schlägt der Anmeldeversuch fehl.

Viele Funktionen von NetApp Hybrid Cloud Control sind für die Zusammenarbeit mit mehreren Speicherclustern ausgelegt, jedoch gibt es Einschränkungen bei der Authentifizierung und Autorisierung. Die Einschränkung bei der Authentifizierung und Autorisierung besteht darin, dass der Benutzer des autoritativen Clusters Aktionen auf anderen Clustern ausführen kann, die mit NetApp Hybrid Cloud Control verbunden sind, selbst wenn er kein Benutzer auf den anderen Speicherclustern ist.

Bevor Sie mit der Verwaltung mehrerer Speichercluster fortfahren, sollten Sie sicherstellen, dass die auf den autoritativen Clustern definierten Benutzer auch auf allen anderen Speicherclustern mit denselben Berechtigungen definiert sind. Sie können Benutzer über die"Element-Software-Benutzeroberfläche" Die

Sehen"Speichercluster-Assets erstellen und verwalten" Weitere Informationen zur Arbeit mit Management-Node-Speichercluster-Assets finden Sie hier.

Drittelregel

Wenn Sie verschiedene Speicherknotentypen in einem NetApp SolidFire -Speichercluster mischen, darf kein einzelner Speicherknoten mehr als 33 % der gesamten Speicherclusterkapazität enthalten.

Ungenutzte Kapazität

Wenn ein neu hinzugefügter Knoten mehr als 50 Prozent der gesamten Clusterkapazität ausmacht, wird ein Teil der Kapazität dieses Knotens unbrauchbar gemacht ("gestrandet"), damit er der Kapazitätsregel entspricht. Dies bleibt so lange der Fall, bis zusätzliche Speicherkapazität geschaffen wird. Wird ein sehr großer Knoten hinzugefügt, der ebenfalls gegen die Kapazitätsregel verstößt, so ist der zuvor gestrandete Knoten nicht mehr gestrandet, während der neu hinzugefügte Knoten gestrandet wird. Um dies zu vermeiden, sollten Kapazitäten immer paarweise addiert werden. Wenn ein Knoten ausfällt, wird ein entsprechender Clusterfehler ausgelöst.

Speichereffizienz

Netapp SolidFire -Speichercluster nutzen Deduplizierung, Komprimierung und Thin Provisioning, um den für die Speicherung eines Volumes benötigten physischen Speicherplatz zu reduzieren.

- **Kompression**

  Durch Komprimierung wird der für ein Volume benötigte physische Speicherplatz reduziert, indem Datenblöcke in Komprimierungsgruppen zusammengefasst werden, von denen jede als einzelner Block gespeichert wird.

- **Deducation**

  Durch das Verwerfen doppelter Datenblöcke wird der für ein Volume benötigte physische Speicherplatz reduziert.

- **Thin Provisioning**

  Ein Thin-Provisioned Volume oder LUN ist ein Volume, für das kein Speicherplatz im Voraus reserviert wird. Stattdessen wird der Speicherplatz dynamisch zugewiesen, je nach Bedarf. Freier Speicherplatz wird dem Speichersystem wieder zur Verfügung gestellt, wenn Daten im Volume oder der LUN gelöscht werden.

Speichercluster-Quorum

Die Element-Software erstellt aus ausgewählten Knoten einen Speichercluster, der eine replizierte Datenbank der Clusterkonfiguration verwaltet. Für die Aufrechterhaltung des Quorums und damit der Ausfallsicherheit des Clusters müssen mindestens drei Knoten am Cluster-Ensemble teilnehmen.

Sicherheit

Wenn Sie Ihr SolidFire All-Flash-Speichersystem verwenden, sind Ihre Daten durch branchenübliche Sicherheitsprotokolle geschützt.

Verschlüsselung ruhender Daten (Hardware)

Alle Laufwerke in den Speicherknoten sind zur Verschlüsselung fähig und nutzen die AES 256-Bit-Verschlüsselung auf Laufwerksebene. Jedes Laufwerk verfügt über einen eigenen Verschlüsselungsschlüssel, der bei der ersten Initialisierung des Laufwerks erstellt wird. Wenn Sie die Verschlüsselungsfunktion aktivieren, wird ein clusterweites Passwort erstellt, und Teile dieses Passworts werden dann an alle Knoten im Cluster verteilt. Kein einzelner Knoten speichert das vollständige Passwort. Das Passwort wird dann verwendet, um den gesamten Zugriff auf die Laufwerke zu schützen. Das Passwort wird zum Entsperren des Laufwerks benötigt und danach nur noch, wenn die Stromversorgung des Laufwerks unterbrochen oder das Laufwerk gesperrt wird.

"Aktivierung der Hardwareverschlüsselungsfunktion im Ruhezustand"hat keinen Einfluss auf die Leistung oder Effizienz des Clusters. Wird ein verschlüsseltes Laufwerk oder ein verschlüsselter Knoten mithilfe der Element API oder der Element UI aus der Clusterkonfiguration entfernt, wird die Verschlüsselung ruhender Daten auf den Laufwerken deaktiviert. Nach dem Ausbau des Laufwerks kann dieses mithilfe des sicheren Löschprogramms gelöscht werden. `SecureEraseDrives` API-Methode. Wird ein physisches Laufwerk oder ein Knoten zwangsweise entfernt, bleiben die Daten durch das clusterweite Passwort und die individuellen Verschlüsselungsschlüssel des Laufwerks geschützt.

Verschlüsselung ruhender Daten (Software)

Eine weitere Art der Verschlüsselung ruhender Daten, die Software-Verschlüsselung ruhender Daten, ermöglicht die Verschlüsselung aller Daten, die auf SSDs in einem Speichercluster geschrieben werden.

"Wenn aktiviert" Es verschlüsselt alle geschriebenen Daten und entschlüsselt alle gelesenen Daten automatisch in der Software. Die Softwareverschlüsselung ruhender Daten spiegelt die Hardware-Implementierung von Self-Encrypting Drive (SED) wider, um Datensicherheit auch ohne SED zu gewährleisten.

> Bei SolidFire All-Flash-Speicherclustern muss die Softwareverschlüsselung ruhender Daten während der Clustererstellung aktiviert werden und kann nach der Clustererstellung nicht mehr deaktiviert werden.

Sowohl software- als auch hardwarebasierte Verschlüsselung ruhender Daten kann unabhängig voneinander oder in Kombination miteinander verwendet werden.

Externes Schlüsselmanagement

Sie können die Element-Software so konfigurieren, dass sie einen KMIP-kompatiblen Schlüsselverwaltungsdienst (KMS) eines Drittanbieters zur Verwaltung der Verschlüsselungsschlüssel des Speicherclusters verwendet. Wenn Sie diese Funktion aktivieren, wird der clusterweite Laufwerkszugriffspasswort-Verschlüsselungsschlüssel des Speicherclusters von einem von Ihnen angegebenen KMS verwaltet.

Element kann die folgenden Schlüsselverwaltungsdienste nutzen:

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

Weitere Informationen zur Konfiguration der externen Schlüsselverwaltung finden Sie unter"die ersten Schritte zur externen Schlüsselverwaltung" Dokumentation.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ermöglicht es Ihnen, von Benutzern zu verlangen, mehrere Arten von Nachweisen vorzulegen, um sich beim Anmelden an der NetApp Element Web-UI oder der Storage-Node-UI zu authentifizieren. Sie können Element so konfigurieren, dass bei der Integration mit Ihrem bestehenden Benutzerverwaltungssystem und Identitätsanbieter nur Multi-Faktor-Authentifizierung akzeptiert wird. Element kann so konfiguriert werden, dass es sich in einen bestehenden SAML 2.0-Identitätsanbieter integriert, der mehrere Authentifizierungsmethoden erzwingen kann, wie z. B. Passwort und SMS, Passwort und E-Mail oder andere Methoden.

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

Informationen zur Konfiguration der Multi-Faktor-Authentifizierung finden Sie unter "die Multi-Faktor-Authentifizierung aktivieren" Dokumentation.

FIPS 140-2 für HTTPS und Verschlüsselung ruhender Daten

NetApp SolidFire -Speichercluster unterstützen eine Verschlüsselung, die den Anforderungen des Federal Information Processing Standard (FIPS) 140-2 für kryptografische Module entspricht. Sie können die FIPS 140-2-Konformität auf Ihrem SolidFire -Cluster sowohl für die HTTPS-Kommunikation als auch für die

Laufwerksverschlüsselung aktivieren.

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

Weitere Informationen zur Vorbereitung eines neuen Speicherclusters für die FIPS 140-2-Verschlüsselung finden Sie unter"Erstellen Sie einen Cluster, der FIPS-Laufwerke unterstützt." Die

Weitere Informationen zur Aktivierung von FIPS 140-2 auf einem bestehenden, vorbereiteten Cluster finden Sie unter"die EnableFeature Element API" Die

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

Konten und Berechtigungen

Um Speicherressourcen auf Ihrem System zu verwalten und den Zugriff darauf zu ermöglichen, müssen Sie Konten für Systemressourcen einrichten.

Mit Element Storage können Sie die folgenden Kontotypen erstellen und verwalten:

- Administrator-Benutzerkonten für den Speichercluster
- Benutzerkonten für den Zugriff auf Speichervolumes
- Autorisierte Cluster-Benutzerkonten für NetApp Hybrid Cloud Control

Administratorkonten für Speichercluster

In einem Speichercluster, auf dem die NetApp Element -Software ausgeführt wird, können zwei Arten von Administratorkonten existieren:

- **Primäres Cluster-Administratorkonto**: Dieses Administratorkonto wird bei der Erstellung des Clusters erstellt. Dieses Konto ist das primäre Administratorkonto mit dem höchsten Zugriffsniveau auf den Cluster. Dieses Konto ist vergleichbar mit einem Root-Benutzer in einem Linux-System. Sie können das Passwort für dieses Administratorkonto ändern.
- **Cluster-Administratorkonto**: Sie können einem Cluster-Administratorkonto einen begrenzten administrativen Zugriff gewähren, um bestimmte Aufgaben innerhalb eines Clusters auszuführen. Die jedem Cluster-Administratorkonto zugewiesenen Anmeldeinformationen werden zur Authentifizierung von API- und Element-UI-Anfragen innerhalb des Speichersystems verwendet.

> Um über die Benutzeroberfläche pro Knoten auf aktive Knoten in einem Cluster zuzugreifen, ist ein lokales (nicht-LDAP-)Cluster-Administratorkonto erforderlich. Für den Zugriff auf einen Knoten, der noch nicht Teil eines Clusters ist, werden keine Kontodaten benötigt.

Du kannst"Cluster-Administratorkonten verwalten" durch Erstellen, Löschen und Bearbeiten von Cluster-

Administratorkonten, Ändern des Cluster-Administratorpassworts und Konfigurieren von LDAP-Einstellungen zur Verwaltung des Systemzugriffs für Benutzer.

Benutzerkonten

Benutzerkonten dienen der Steuerung des Zugriffs auf die Speicherressourcen in einem softwarebasierten NetApp Element Netzwerk. Für die Erstellung eines Volumes ist mindestens ein Benutzerkonto erforderlich.

Wenn Sie ein Volume erstellen, wird es einem Konto zugewiesen. Wenn Sie ein virtuelles Volume erstellt haben, ist das Konto der Speichercontainer.

Hier einige weitere Überlegungen:

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

Autorisierte Cluster-Benutzerkonten

Autorisierte Cluster-Benutzerkonten können sich gegenüber jedem Speichermedium authentifizieren, das mit der NetApp Hybrid Cloud Control-Instanz von Knoten und Clustern verknüpft ist. Mit diesem Konto können Sie Volumes, Accounts, Zugriffsgruppen und mehr clusterübergreifend verwalten.

Autorisierte Benutzerkonten werden über die Option „Benutzerverwaltung“ im Menü oben rechts in NetApp Hybrid Cloud Control verwaltet.

Der"autoritativer Speichercluster" ist der Speichercluster, den NetApp Hybrid Cloud Control zur Authentifizierung von Benutzern verwendet.

Alle Benutzer, die auf dem autoritativen Speichercluster erstellt wurden, können sich bei NetApp Hybrid Cloud Control anmelden. Benutzer, die auf anderen Speicherclustern erstellt wurden, können sich nicht bei Hybrid Cloud Control anmelden.

- Wenn Ihr Management-Knoten nur über einen Speichercluster verfügt, dann ist dieser der autoritative Cluster.
- Wenn Ihr Management-Knoten über zwei oder mehr Speichercluster verfügt, wird einer dieser Cluster als autoritativer Cluster festgelegt, und nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden.

Viele Funktionen von NetApp Hybrid Cloud Control sind zwar mit mehreren Speicherclustern kompatibel, jedoch gibt es bei der Authentifizierung und Autorisierung notwendige Einschränkungen. Die Einschränkung bei der Authentifizierung und Autorisierung besteht darin, dass Benutzer des autoritativen Clusters Aktionen auf anderen Clustern ausführen können, die mit NetApp Hybrid Cloud Control verbunden sind, selbst wenn sie auf den anderen Speicherclustern keine Benutzer sind. Bevor Sie mit der Verwaltung mehrerer Speichercluster fortfahren, sollten Sie sicherstellen, dass die auf den autoritativen Clustern definierten Benutzer auch auf allen anderen Speicherclustern mit denselben Berechtigungen definiert sind. Sie können Benutzer über NetApp Hybrid Cloud Control verwalten.

Volumenkonten

Volumespezifische Konten sind nur auf den Speichercluster beschränkt, auf dem sie erstellt wurden. Mit

diesen Konten können Sie Berechtigungen für bestimmte Volumes im gesamten Netzwerk festlegen, sie haben jedoch keine Auswirkungen außerhalb dieser Volumes.

Die Verwaltung der Volumenkonten erfolgt in der Tabelle „NetApp Hybrid Cloud Control Volumes“.

Storage

Bände

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

Mit Element Storage können Sie Volumes für Benutzerkonten erstellen, anzeigen, bearbeiten, löschen, klonen, sichern oder wiederherstellen. Sie können auch jedes einzelne Volume in einem Cluster verwalten und Volumes in Volume-Zugriffsgruppen hinzufügen oder entfernen.

Persistente Datenträger

Persistente Volumes ermöglichen es, Konfigurationsdaten des Management-Knotens auf einem bestimmten Speichercluster anstatt lokal auf einer VM zu speichern, sodass die Daten im Falle eines Verlusts oder einer Entfernung des Management-Knotens erhalten bleiben können. Persistente Volumes sind eine optionale, aber empfehlenswerte Konfiguration für Management-Knoten.

Eine Option zum Aktivieren persistenter Volumes ist in den Installations- und Upgrade-Skripten enthalten, wenn"Bereitstellung eines neuen Managementknotens" Die Persistente Volumes sind Volumes auf einem Element-Software-basierten Speichercluster, die Konfigurationsinformationen des Management-Knotens für die Host-Management-Knoten-VM enthalten, die über die Lebensdauer der VM hinaus bestehen bleiben. Wenn der Management-Knoten verloren geht, kann eine Ersatz-Management-Knoten-VM die Verbindung wiederherstellen und die Konfigurationsdaten der verloren gegangenen VM wiederherstellen.

Die Funktion für persistente Volumes erstellt, sofern sie während der Installation oder des Upgrades aktiviert ist, automatisch mehrere Volumes. Diese Volumes können, wie alle Element-Software-basierten Volumes, je nach Präferenz und Installation über die Element-Software-Weboberfläche, das NetApp Element Plug-in für vCenter Server oder die API angezeigt werden. Persistente Volumes müssen über eine iSCSI-Verbindung zum Management-Knoten betriebsbereit sein, um aktuelle Konfigurationsdaten zu erhalten, die für die Wiederherstellung verwendet werden können.

> ⓘ Persistente Volumes, die mit Verwaltungsdiensten verknüpft sind, werden während der Installation oder des Upgrades erstellt und einem neuen Konto zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder das zugehörige Konto nicht.

Virtuelle Volumes (vVols)

vSphere Virtual Volumes ist ein Speicherparadigma für VMware, das einen Großteil der Speicherverwaltung für vSphere vom Speichersystem zu VMware vCenter verlagert. Mit virtuellen Volumes (vVols) können Sie Speicherplatz entsprechend den Anforderungen einzelner virtueller Maschinen zuweisen.

Bindungen

Der NetApp Element -Cluster wählt einen optimalen Protokollendpunkt aus, erstellt eine Bindung, die den ESXi-Host und das virtuelle Volume mit dem Protokollendpunkt verknüpft, und gibt die Bindung an den ESXi-Host zurück. Nach der Bindung kann der ESXi-Host E/A-Operationen mit dem gebundenen virtuellen Volume durchführen.

Protokollendpunkte

VMware ESXi-Hosts verwenden logische E/A-Proxys, sogenannte Protokollendpunkte, zur Kommunikation mit virtuellen Volumes. ESXi-Hosts binden virtuelle Volumes an Protokollendpunkte, um E/A-Operationen durchzuführen. Wenn eine virtuelle Maschine auf dem Host eine E/A-Operation durchführt, leitet der zugehörige Protokollendpunkt die E/A an das virtuelle Volume weiter, mit dem sie gekoppelt ist.

Protokollendpunkte in einem NetApp Element -Cluster fungieren als SCSI-administrative logische Einheiten. Jeder Protokollendpunkt wird automatisch vom Cluster erstellt. Für jeden Knoten in einem Cluster wird ein entsprechender Protokollendpunkt erstellt. Ein Cluster mit vier Knoten verfügt beispielsweise über vier Protokollendpunkte.

iSCSI ist das einzige von der NetApp Element Software unterstützte Protokoll. Das Fibre Channel-Protokoll wird nicht unterstützt. Protokollendpunkte können von einem Benutzer weder gelöscht noch geändert werden, sind keinem Konto zugeordnet und können keiner Volume-Zugriffsgruppe hinzugefügt werden.

Lagerbehälter

Speichercontainer sind logische Konstrukte, die NetApp Element -Konten zugeordnet sind und für Berichtswesen und Ressourcenzuweisung verwendet werden. Sie bündeln die Rohspeicherkapazität oder aggregieren die Speicherkapazitäten, die das Speichersystem virtuellen Volumes bereitstellen kann. Ein in vSphere erstellter VVol-Datenspeicher wird einem einzelnen Speichercontainer zugeordnet. Ein einzelner Speichercontainer verfügt standardmäßig über alle verfügbaren Ressourcen des NetApp Element Clusters. Wenn eine detailliertere Steuerung für Mandantenfähigkeit erforderlich ist, können mehrere Speichercontainer erstellt werden.

Speichercontainer funktionieren wie herkömmliche Konten und können sowohl virtuelle als auch herkömmliche Volumes enthalten. Es werden maximal vier Speichercontainer pro Cluster unterstützt. Für die Nutzung der VVols-Funktionalität ist mindestens ein Speichercontainer erforderlich. Sie können Speichercontainer in vCenter während der Erstellung von VVols ermitteln.

VASA-Anbieter

Damit vSphere die vVol-Funktion im NetApp Element -Cluster erkennt, muss der vSphere-Administrator den NetApp Element VASA Provider bei vCenter registrieren. Der VASA-Provider ist der Out-of-Band-Steuerungspfad zwischen vSphere und dem Element-Cluster. Es ist verantwortlich für die Ausführung von Anfragen an den Element-Cluster im Auftrag von vSphere, wie z. B. das Erstellen von VMs, das Bereitstellen von VMs für vSphere und das Bekanntgeben von Speicherkapazitäten für vSphere.

Der VASA-Provider läuft als Teil des Cluster-Masters in der Element-Software. Der Cluster-Master ist ein hochverfügbarer Dienst, der bei Bedarf auf jeden beliebigen Knoten im Cluster ausweicht. Wenn der Cluster-Master ausfällt, wird der VASA-Provider mitverschoben, wodurch eine hohe Verfügbarkeit für den VASA-Provider gewährleistet wird. Alle Bereitstellungs- und Speicherverwaltungsaufgaben nutzen den VASA-Provider, der alle erforderlichen Änderungen am Element-Cluster vornimmt.

Bei Element 12.5 und älteren Versionen dürfen Sie nicht mehr als einen NetApp Element VASA-Provider bei einer einzelnen vCenter-Instanz registrieren. Wird ein zweiter NetApp Element VASA-Provider hinzugefügt, sind alle VVOL-Datenspeicher nicht mehr zugänglich.

Die VASA-Unterstützung für bis zu 10 vCenter-Instanzen ist als Upgrade-Patch verfügbar, sofern Sie bereits einen VASA-Anbieter bei Ihrem vCenter registriert haben. Zur Installation folgen Sie den Anweisungen im VASA39-Manifest und laden Sie die .tar.gz-Datei von der Website herunter."NetApp Software-Downloads" Website. Der NetApp Element VASA-Provider verwendet ein NetApp Zertifikat. Mit diesem Patch wird das Zertifikat von vCenter unverändert verwendet, um die Nutzung mehrerer vCenter-Instanzen für VASA und VVols zu unterstützen. Das Zertifikat darf nicht verändert werden. Benutzerdefinierte SSL-Zertifikate werden von VASA nicht unterstützt.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

Volumenzugriffsgruppen

Durch das Erstellen und Verwenden von Volume-Zugriffsgruppen können Sie den Zugriff auf eine Gruppe von Volumes steuern. Wenn Sie eine Gruppe von Volumes und eine Gruppe von Initiatoren mit einer Volume-Zugriffsgruppe verknüpfen, gewährt die Zugriffsgruppe diesen Initiatoren Zugriff auf diese Gruppe von Volumes.

Volume-Zugriffsgruppen in NetApp SolidFire -Speichern ermöglichen es iSCSI-Initiator-IQNs oder Fibre Channel-WWPNs, auf eine Sammlung von Volumes zuzugreifen. 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 Zugriff auf das Fibre Channel-Netzwerk für die Volumes in der Zugriffsgruppe.

Zugriffsgruppen für Datenträger unterliegen folgenden Beschränkungen:

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

Initiatoren

Initiatoren ermöglichen externen Clients den Zugriff auf Volumes in einem Cluster und dienen als Einstiegspunkt für die Kommunikation zwischen Clients und Volumes. Sie können Initiatoren für den CHAP-basierten Zugriff auf Speichervolumes anstelle des kontobasierten Zugriffs verwenden. Ein einzelner Initiator, der einer Volume-Zugriffsgruppe hinzugefügt wird, ermöglicht es den Mitgliedern der Volume-Zugriffsgruppe, auf alle der Gruppe hinzugefügten Speichervolumes zuzugreifen, ohne dass eine Authentifizierung erforderlich ist. Ein Initiator kann nur einer Zugriffsgruppe

angehören.

Datenschutz

Zu den Datenschutzfunktionen gehören Remote-Replikation, Volume-Snapshots, Volume-Klonen, Schutzdomänen und Hochverfügbarkeit mit Double-Helix-Technologie.

Der Datenschutz für Elementspeicher umfasst folgende Konzepte:

- Arten der Remote-Replikation
- Volume-Snapshots zum Datenschutz
- Volumenklone
- Übersicht über den Sicherungs- und Wiederherstellungsprozess für Element-Speicher
- Schutzdomänen
- Benutzerdefinierte Schutzdomänen
- Doppelhelix-Hochverfügbarkeit

Arten der Remote-Replikation

Die Remote-Replikation von Daten kann folgende Formen annehmen:

- Synchrone und asynchrone Replikation zwischen Clustern
- Snapshot-Replikation
- Replikation zwischen Element- und ONTAP -Clustern mit SnapMirror

Weitere Informationen finden Sie unter "TR-4741: NetApp Element Software-Remote-Replikation" Die

Synchrone und asynchrone Replikation zwischen Clustern

Bei Clustern, auf denen die NetApp Element Software läuft, ermöglicht die Echtzeitreplikation die schnelle Erstellung von Remote-Kopien der Volume-Daten.

Sie können einen Speichercluster mit bis zu vier anderen Speicherclustern koppeln. Sie können Volumendaten synchron oder asynchron von jedem der beiden Cluster eines Clusterpaares für Failover- und Failback-Szenarien replizieren.

Synchrone Replikation

Bei der synchronen Replikation werden Daten kontinuierlich vom Quellcluster zum Zielcluster repliziert. Dabei kommt es zu Latenzproblemen, Paketverlusten, Jitter und Bandbreitenbeschränkungen.

Die synchrone Replikation eignet sich für folgende Situationen:

- Replikation mehrerer Systeme über kurze Distanz
- Ein Katastrophenwiederherstellungsstandort, der sich geografisch in der Nähe des Ursprungsortes befindet
- Zeitkritische Anwendungen und der Schutz von Datenbanken
- Anwendungen zur Geschäftskontinuität, die erfordern, dass der sekundäre Standort als primärer Standort

fungiert, wenn der primäre Standort ausfällt

Asynchrone Replikation

Bei der asynchronen Replikation werden Daten kontinuierlich von einem Quellcluster in einen Zielcluster repliziert, ohne auf die Bestätigungen vom Zielcluster zu warten. Bei der asynchronen Replikation werden Schreibvorgänge dem Client (der Anwendung) erst bestätigt, nachdem sie im Quellcluster festgeschrieben wurden.

Die asynchrone Replikation eignet sich für folgende Situationen:

- Der Disaster-Recovery-Standort ist weit vom Quellstandort entfernt und die Anwendung verträgt keine durch das Netzwerk verursachten Latenzen.
- Es gibt Bandbreitenbeschränkungen im Netzwerk, das die Quell- und Zielcluster verbindet.

Snapshot-Replikation

Beim Snapshot-basierten Datenschutz werden geänderte Daten zu bestimmten Zeitpunkten in einen Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quellvolume sind nicht.

Sie können die Häufigkeit der Snapshot-Replikationen festlegen.

Die Snapshot-Replikation hat keinen Einfluss auf die asynchrone oder synchrone Replikation.

Replikation zwischen Element- und ONTAP -Clustern mit SnapMirror

Mit der NetApp SnapMirror Technologie können Sie Snapshots, die mit der NetApp Element -Software erstellt wurden, für Zwecke der Notfallwiederherstellung auf ONTAP replizieren. In einer SnapMirror Beziehung ist Element der eine Endpunkt und ONTAP der andere.

SnapMirror ist eine Snapshot-Replikationstechnologie von NetApp , die die Notfallwiederherstellung erleichtert und für das Failover vom primären Speicher zum sekundären Speicher an einem geografisch entfernten Standort konzipiert ist. Die SnapMirror -Technologie erstellt eine Replik oder ein Spiegelbild der Arbeitsdaten im Sekundärspeicher, von dem aus Sie weiterhin Daten bereitstellen können, falls es am Primärstandort zu einem Ausfall kommt. Die Daten werden auf Volumenebene gespiegelt.

Die Beziehung zwischen dem Quellvolume im Primärspeicher und dem Zielvolume im Sekundärspeicher 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 per Peering verbunden sein. Eine Peer-Beziehung ermöglicht es Clustern und Volumes, Daten sicher auszutauschen.

SnapMirror läuft nativ auf den NetApp ONTAP -Controllern und ist in Element integriert, das auf NetApp HCI und SolidFire -Clustern läuft. Die Logik zur Steuerung von SnapMirror ist in der ONTAP -Software enthalten; daher muss bei allen SnapMirror -Beziehungen mindestens ein ONTAP -System zur Durchführung der Koordinierungsarbeiten einbezogen werden. Die Beziehungen zwischen Element- und ONTAP Clustern werden von den Benutzern primär über die Element-Benutzeroberfläche verwaltet; einige Verwaltungsaufgaben werden jedoch im NetApp ONTAP System Manager durchgeführt. Benutzer können SnapMirror auch über die CLI und die API verwalten, die beide in ONTAP und Element verfügbar sind.

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

Sie müssen die SnapMirror Funktionalität auf Clusterebene manuell mithilfe der Element-Software aktivieren. Die SnapMirror -Funktionalität ist standardmäßig deaktiviert und wird bei einer Neuinstallation oder einem Upgrade nicht automatisch aktiviert.

Nach der Aktivierung von SnapMirror können Sie SnapMirror Beziehungen über die Registerkarte „Datenschutz“ in der Element-Software erstellen.

Die NetApp Element Software ab Version 10.1 unterstützt die SnapMirror -Funktionalität zum Kopieren und Wiederherstellen von Snapshots mit ONTAP -Systemen.

Systeme, auf denen Element 10.1 oder höher läuft, enthalten Code, der direkt mit SnapMirror auf ONTAP -Systemen mit Version 9.3 oder höher kommunizieren kann. Die Element API bietet Methoden, um die SnapMirror Funktionalität auf Clustern, Volumes und Snapshots zu aktivieren. Darüber hinaus beinhaltet die Element-Benutzeroberfläche Funktionen zur Verwaltung von SnapMirror -Beziehungen zwischen der Element-Software und ONTAP -Systemen.

Ab Element 10.3 und ONTAP 9.4 können Sie in bestimmten Anwendungsfällen mit eingeschränkter Funktionalität von ONTAP Volumes auf Element-Volumes replizieren.

Weitere Informationen finden Sie unter "Replikation zwischen NetApp Element Software und ONTAP (ONTAP CLI)".

Volume-Snapshots zum Datenschutz

Ein Volume-Snapshot ist eine Momentaufnahme eines Volumes, die Sie später verwenden können, um ein Volume auf diesen spezifischen Zeitpunkt zurückzusetzen.

Snapshots ähneln zwar Volume-Klonen, sind aber lediglich Replikate der Volume-Metadaten, sodass man sie weder einbinden noch beschreiben kann. Das Erstellen eines Volume-Snapshots benötigt ebenfalls nur wenig Systemressourcen und Speicherplatz, wodurch die Snapshot-Erstellung schneller ist als das Klonen.

Sie können Snapshots auf einen Remote-Cluster replizieren und diese als Sicherungskopie des Volumes verwenden. Dies ermöglicht es Ihnen, ein Volume mithilfe des replizierten Snapshots auf einen bestimmten Zeitpunkt zurückzusetzen; Sie können auch eine Kopie eines Volumes aus einem replizierten Snapshot erstellen.

Sie können Snapshots von einem Element-Cluster in einem externen Objektspeicher oder in einem anderen Element-Cluster sichern. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, benötigen Sie eine Verbindung zum Objektspeicher, die Lese-/Schreibvorgänge ermöglicht.

Sie können einen Snapshot eines einzelnen Volumes oder mehrerer Volumes zum Schutz Ihrer Daten erstellen.

Volumenklone

Das Klonen eines einzelnen Datenträgers oder mehrerer Datenträger ist eine zeitpunktbezogene Kopie der Daten. Beim Klonen eines Volumes erstellt das System einen Snapshot des Volumes und anschließend eine Kopie der Daten, auf die im Snapshot verwiesen wird.

Dies ist ein asynchroner Prozess, und die benötigte Zeit hängt von der Größe des zu klonenden Volumes und der aktuellen Clusterlast ab.

Der Cluster unterstützt bis zu zwei laufende Klonanforderungen pro Volume gleichzeitig und bis zu acht aktive Volume-Klonvorgänge gleichzeitig. Anfragen, die diese Grenzen überschreiten, werden zur späteren Bearbeitung in eine Warteschlange gestellt.

Übersicht über den Sicherungs- und Wiederherstellungsprozess für Element-Speicher

Sie können Volumes auf anderen SolidFire -Speichern sichern und wiederherstellen, sowie auf sekundären Objektspeichern, die mit Amazon S3 oder OpenStack Swift kompatibel sind.

Sie können ein Volume an folgendem Ort sichern:

- Ein SolidFire Speichercluster
- Ein Amazon S3-Objektspeicher
- Ein OpenStack Swift-Objektspeicher

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifestinformationen aus dem ursprünglichen Sicherungsprozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire -Speichersystem gesichert wurde, sind keine Manifestinformationen erforderlich.

Schutzdomänen

Eine Schutzdomäne ist ein Knoten oder eine Gruppe von Knoten, die so zusammengefasst sind, dass ein Teil oder sogar die gesamte Domäne ausfallen kann, während die Datenverfügbarkeit erhalten bleibt. Schutzdomänen ermöglichen es einem Speichercluster, sich nach dem Verlust eines Chassis (Chassis-Affinität) oder einer gesamten Domäne (Gruppe von Chassis) automatisch zu erholen.

Sie können die Überwachung der Schutzdomäne manuell aktivieren, indem Sie den Erweiterungspunkt „NetApp Element Configuration“ im NetApp Element Plug-in für vCenter Server verwenden. Sie können einen Schwellenwert für die Schutzdomäne basierend auf Knoten- oder Chassisdomänen auswählen. Sie können die Überwachung der Schutzdomäne auch über die Element-API oder die Web-Benutzeroberfläche aktivieren.

Ein Schutzdomänen-Layout ordnet jedem Knoten eine bestimmte Schutzdomäne zu.

Es werden zwei verschiedene Schutzdomänen-Layouts unterstützt, die als Schutzdomänenebenen bezeichnet werden.

- Auf Knotenebene befindet sich jeder Knoten in seiner eigenen Schutzdomäne.
- Auf Chassis-Ebene befinden sich nur Knoten, die sich ein Chassis teilen, in derselben Schutzdomäne.
    - Das Chassis-Layout wird beim Hinzufügen des Knotens zum Cluster automatisch aus der Hardware ermittelt.
    - In einem Cluster, in dem sich jeder Knoten in einem separaten Gehäuse befindet, sind diese beiden Ebenen funktional identisch.

Wenn Sie einen neuen Cluster erstellen und Speicherknoten verwenden, die sich in einem gemeinsam genutzten Chassis befinden, sollten Sie die Implementierung eines Ausfallschutzes auf Chassis-Ebene mithilfe der Funktion „Schutzdomänen“ in Betracht ziehen.

Benutzerdefinierte Schutzdomänen

Sie können ein benutzerdefiniertes Schutzdomänen-Layout definieren, das zu Ihrem spezifischen Chassis- und Knoten-Layout passt, wobei jeder Knoten genau einer benutzerdefinierten Schutzdomäne zugeordnet ist. Standardmäßig ist jeder Knoten der gleichen benutzerdefinierten Standard-Schutzdomäne zugeordnet.

Wenn keine benutzerdefinierten Schutzdomänen zugewiesen sind:

- Der Clusterbetrieb ist davon nicht betroffen.
- Die benutzerdefinierte Stufe ist weder tolerant noch robust.

Wenn Sie benutzerdefinierte Schutzdomänen für einen Cluster konfigurieren, gibt es drei mögliche Schutzstufen, die Sie im Element-Web-UI-Dashboard einsehen können:

- Nicht geschützt: Der Speichercluster ist nicht gegen den Ausfall einer seiner benutzerdefinierten Schutzdomänen geschützt. Um dieses Problem zu beheben, fügen Sie dem Cluster zusätzliche Speicherkapazität hinzu oder konfigurieren Sie die benutzerdefinierten Schutzdomänen des Clusters neu, um den Cluster vor möglichem Datenverlust zu schützen.
- Fehlertolerant: Der Speichercluster verfügt über ausreichend freie Kapazität, um Datenverlust nach dem Ausfall einer seiner benutzerdefinierten Schutzdomänen zu verhindern.
- Fehlerresistent: Der Speichercluster verfügt über genügend freie Kapazität, um sich nach dem Ausfall einer seiner benutzerdefinierten Schutzdomänen selbst zu reparieren. Nach Abschluss des Heilungsprozesses ist der Cluster vor Datenverlust geschützt, falls weitere Domänen ausfallen sollten.

Wenn mehr als eine benutzerdefinierte Schutzdomäne zugewiesen ist, ordnet jedes Subsystem Duplikate separaten benutzerdefinierten Schutzdomänen zu. Falls dies nicht möglich ist, werden Duplikate separaten Knoten zugeordnet. Jedes Teilsystem (z. B. Bins, Slices, Protocol Endpoint Providers und Ensemble) führt dies unabhängig durch.

Sie können die Element-Benutzeroberfläche verwenden, um"Benutzerdefinierte Schutzdomänen konfigurieren" Alternativ können Sie die folgenden API-Methoden verwenden:

- "GetProtectionDomainLayout"- zeigt an, in welchem Chassis und welcher benutzerdefinierten Schutzdomäne sich jeder Knoten befindet.
- "SetProtectionDomainLayout"- ermöglicht die Zuweisung einer benutzerdefinierten Schutzdomäne zu jedem Knoten.

Doppelhelix-Hochverfügbarkeit

Die Double-Helix-Datensicherung ist eine Replikationsmethode, die mindestens zwei redundante Datenkopien auf alle Laufwerke eines Systems verteilt. Der Ansatz „RAID-los“ ermöglicht es einem System, mehrere gleichzeitig auftretende Ausfälle auf allen Ebenen des Speichersystems zu absorbieren und schnell zu beheben.

Leistung und Servicequalität

Ein SolidFire -Speichercluster ist in der Lage, Quality-of-Service-Parameter (QoS) auf Volume-Basis bereitzustellen. Sie können die Clusterleistung, gemessen in Eingängen und Ausgängen pro Sekunde (IOPS), mithilfe von drei konfigurierbaren Parametern, die QoS definieren, garantieren: Min IOPS, Max IOPS und Burst IOPS.

SolidFire Active IQ verfügt über eine QoS-Empfehlungsseite, die Hinweise zur optimalen Konfiguration und Einrichtung der QoS-Einstellungen bietet.

Servicequalitätsparameter

Die IOPS-Parameter werden wie folgt definiert:

- **Minimale IOPS** - Die Mindestanzahl an kontinuierlichen Eingaben und Ausgaben pro Sekunde (IOPS), die der Speichercluster einem Volume bereitstellt. Der für ein Volume konfigurierte Min IOPS-Wert ist die garantierte Leistungsstufe für ein Volume. Die Leistung sinkt nicht unter dieses Niveau.
- **Maximale IOPS** - Die maximale Anzahl an anhaltenden IOPS, die der Speichercluster einem Volume bereitstellt. Wenn die IOPS-Werte des Clusters kritisch hoch sind, wird dieses IOPS-Leistungsniveau nicht überschritten.
- **Burst IOPS** - Die maximale Anzahl an IOPS, die in einem kurzen Burst-Szenario zulässig ist. Wenn ein Volume unterhalb der maximalen IOPS läuft, werden Burst-Gutschriften angesammelt. Wenn die Leistungsanforderungen sehr hoch sind und bis zum Maximum ausgereizt werden, werden kurze IOPS-Spitzen auf dem Volume zugelassen.

  Die Element-Software verwendet Burst IOPS, wenn ein Cluster in einem Zustand geringer Cluster-IOPS-Auslastung läuft.

  Ein einzelnes Volume kann Burst-IOPS ansammeln und die Guthaben nutzen, um seine maximale IOPS-Leistung für eine festgelegte "Burst-Periode" bis zum Burst-IOPS-Niveau zu steigern. Ein Volumen kann für bis zu 60 Sekunden kurzzeitig auftreten, sofern der Cluster die Kapazität besitzt, diesen Kurzzeitausbruch zu verkraften. Einem Volume wird für jede Sekunde, in der es unterhalb seines Max IOPS-Limits läuft, eine Sekunde Burst-Guthaben gutgeschrieben (bis zu einem Maximum von 60 Sekunden).

  Die Burst-IOPS sind auf zwei Arten begrenzt:

  - Ein Volume kann seine maximale IOPS-Leistung für eine Anzahl von Sekunden überschreiten, die der Anzahl der Burst-Credits entspricht, die das Volume angesammelt hat.
  - Wenn ein Volume seinen Max-IOPS-Wert überschreitet, wird es durch seinen Burst-IOPS-Wert begrenzt. Daher überschreitet die Burst-IOPS-Zahl niemals den für das Volumen festgelegten Burst-IOPS-Wert.
- **Effektive maximale Bandbreite** - Die maximale Bandbreite wird berechnet, indem die Anzahl der IOPS (basierend auf der QoS-Kurve) mit der IO-Größe multipliziert wird.

  Beispiel: QoS-Parametereinstellungen von 100 Min IOPS, 1000 Max IOPS und 1500 Burst IOPS haben folgende Auswirkungen auf die Leistungsqualität:

  - Die Workloads können maximal 1000 IOPS erreichen und aufrechterhalten, bis es im Cluster zu einer Überlastung der Workloads hinsichtlich der IOPS kommt. Die IOPS werden dann schrittweise reduziert, bis die IOPS auf allen Volumes innerhalb der festgelegten QoS-Bereiche liegen und die Leistungskonflikte beseitigt sind.
  - Die Performance wird auf allen Volumes in Richtung des minimalen IOPS-Werts von 100 angestrebt. Die Werte fallen nicht unter den Min-IOPS-Wert, können aber bei nachlassender Arbeitslast über 100 IOPS bleiben.
  - Die Leistung beträgt über einen längeren Zeitraum nie mehr als 1000 IOPS oder weniger als 100 IOPS. Eine Leistung von 1500 IOPS (Burst IOPS) ist zulässig, jedoch nur für solche Volumes, die Burst-Guthaben durch Betrieb unterhalb der maximalen IOPS angesammelt haben, und nur für kurze Zeiträume. Die Spitzenwerte sind nie dauerhaft.

QoS-Wertgrenzen

Hier sind die möglichen Minimal- und Maximalwerte für QoS.

Parameter	Minimalwert	Standard	4 4KB	5 8 KB	6 16 KB	262 KB
Min IOPS	50	50	15.000	9.375*	5556*	385*

Parameter	Minimalwert	Standard	4 4KB	5 8 KB	6 16 KB	262 KB
Maximale IOPS	100	15.000	200.000**	125.000	74.074	5128
Burst IOPS	100	15.000	200.000**	125.000	74,074	5128

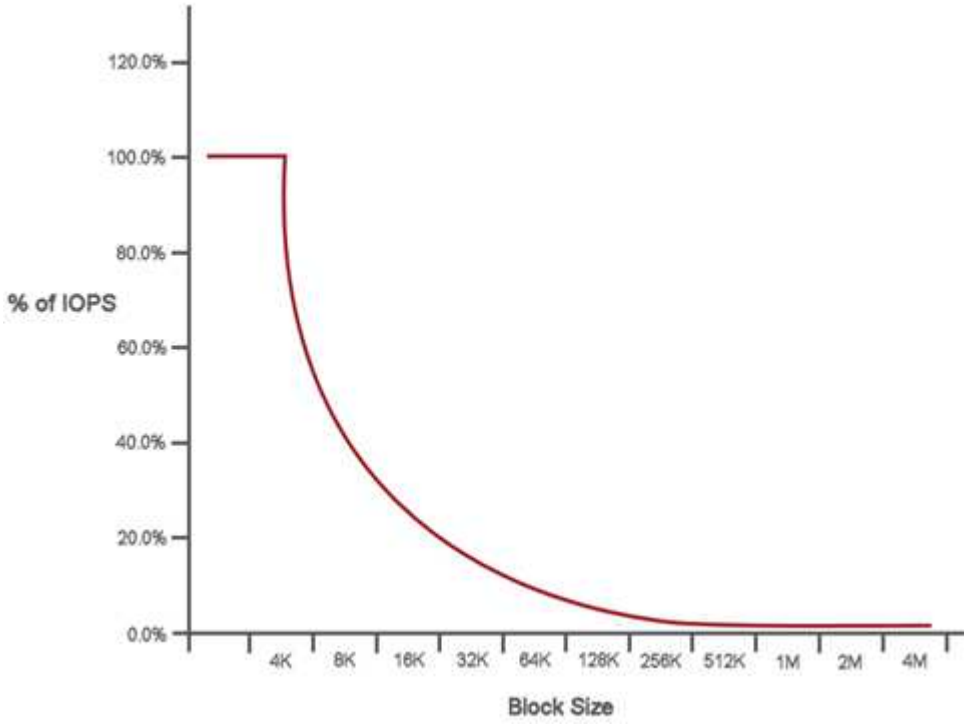
*Diese Schätzungen sind Näherungswerte. **Max IOPS und Burst IOPS können auf bis zu 200.000 eingestellt werden; diese Einstellung ist jedoch nur zulässig, um die Leistung eines Volumes effektiv freizugeben. Die maximale Leistung eines Volumes in der Praxis wird durch die Clusternutzung und die Leistung pro Knoten begrenzt.

QoS-Leistung

Die QoS-Leistungskurve zeigt den Zusammenhang zwischen Blockgröße und IOPS-Prozentsatz.

Blockgröße und Bandbreite haben einen direkten Einfluss auf die Anzahl der IOPS, die eine Anwendung erzielen kann. Die Element-Software berücksichtigt die empfangenen Blockgrößen, indem sie diese auf 4k normalisiert. Je nach Arbeitslast kann das System die Blockgrößen erhöhen. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das zur Verarbeitung der größeren Blockgrößen erforderlich ist. Mit zunehmender Bandbreite sinkt die Anzahl der IOPS, die das System erreichen kann.

Die QoS-Leistungskurve zeigt den Zusammenhang zwischen zunehmenden Blockgrößen und dem abnehmenden Prozentsatz der IOPS:



Wenn beispielsweise die Blockgröße 4k beträgt und die Bandbreite 4000 KBps, beträgt die IOPS-Zahl 1000. Wenn die Blockgröße auf 8k erhöht wird, erhöht sich die Bandbreite auf 5000 KBps, und die IOPS sinken auf 625. Durch die Berücksichtigung der Blockgröße stellt das System sicher, dass Arbeitslasten mit niedrigerer Priorität, die größere Blockgrößen verwenden, wie z. B. Backups und Hypervisor-Aktivitäten, nicht zu viel der Leistung beanspruchen, die für Datenverkehr mit höherer Priorität benötigt wird, der kleinere Blockgrößen verwendet.

QoS-Richtlinien

Eine QoS-Richtlinie ermöglicht es Ihnen, eine standardisierte Dienstgüteeinstellung zu erstellen und zu speichern, die auf viele Volumes angewendet werden kann.

QoS-Richtlinien eignen sich am besten für Serviceumgebungen, beispielsweise für Datenbank-, Anwendungs- oder Infrastrukturserver, die selten neu gestartet werden und einen konstanten, gleichberechtigten Zugriff auf den Speicher benötigen. Die individuelle Volume-QoS eignet sich am besten für VMs mit geringer Auslastung, wie z. B. virtuelle Desktops oder spezialisierte Kiosk-VMs, die täglich oder mehrmals täglich neu gestartet, eingeschaltet oder ausgeschaltet werden können.

QoS und QoS-Richtlinien sollten nicht zusammen verwendet werden. Wenn Sie QoS-Richtlinien verwenden, sollten Sie auf einem Volume keine benutzerdefinierten QoS-Einstellungen verwenden. Benutzerdefinierte QoS-Einstellungen überschreiben und passen die QoS-Richtlinienwerte für die Volumen-QoS-Einstellungen an.

Der ausgewählte Cluster muss Element 10.0 oder höher sein, um QoS-Richtlinien nutzen zu können; andernfalls stehen QoS-Richtlinienfunktionen nicht zur Verfügung.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"