Konzepte

HCI

NetApp
October 11, 2024

Inhalt

Konzepte

Produktübersicht über NetApp HCI

NetApp HCI wurde als Hybrid-Cloud-Infrastruktur für die Ansprüche von Unternehmen entwickelt, kombiniert Storage, Computing, Netzwerke und Hypervisor – und erweitert diese Ressourcen um Funktionen für Public und Private Clouds.

Die disaggregierte Hybrid-Cloud-Infrastruktur von NetApp ermöglicht eine unabhängige Skalierung von Computing- und Storage und passt sich mühelos an Workloads mit garantierter Performance an.

- Erfüllt Anforderungen einer Hybrid-Multi-Cloud
- Compute und Storage skalieren unabhängig voneinander
- Vereinfachte Orchestrierung von Datenservices in Hybrid-Multi-Clouds

Komponenten von NetApp HCI

Hier eine Übersicht über die verschiedenen Komponenten der NetApp HCI Umgebung:

- NetApp HCI stellt Storage- und Computing-Ressourcen bereit. Sie verwenden den **NetApp Deployment Engine** Assistenten zur Implementierung von NetApp HCI. Rechenknoten werden nach erfolgreicher Implementierung als ESXi-Hosts angezeigt und können in VMware vSphere Web Client gemanagt werden.
- **Managementservices** oder Mikroservices umfassen den Active IQ Collector, QoSSIOC für das vCenter Plug-in und den mNode Service; sie werden häufig als Service-Bundles aktualisiert. Ab Element 11.3 werden **Management Services** auf dem Management-Node gehostet, wodurch sich ausgewählte Software-Services außerhalb der Hauptversionen schneller aktualisieren lassen. Der **Management Node** (mNode) ist eine virtuelle Maschine, die parallel zu einem oder mehreren auf Element Software basierenden Speicherclustern läuft. 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.

  Erfahren Sie mehr über "Management Services-Releases".

- **Mit NetApp Hybrid Cloud Control** können Sie NetApp HCI managen. Sie können Management Services aktualisieren, Ihr System erweitern, Protokolle erfassen und Ihre Installation mit NetApp SolidFire Active IQ überwachen. Sie melden sich bei NetApp Hybrid Cloud Control an, indem Sie die IP-Adresse des Management-Node nutzen.
- Das **NetApp Element Plug-in für vCenter Server** ist ein Web-basiertes Tool, das in die vSphere-Benutzeroberfläche integriert ist. Das Plug-in ist eine erweiterbare und skalierbare, benutzerfreundliche Schnittstelle für VMware vSphere, mit der Storage Cluster mit **NetApp Element Software** gemanagt und überwacht werden können. Das Plug-in stellt eine Alternative zur Element UI dar. Über die Plug-in-Benutzeroberfläche können Cluster ermittelt und konfiguriert sowie Storage von der Cluster-Kapazität gemanagt, überwacht und zugewiesen werden, um Datastores und virtuelle Datastores (für virtuelle Volumes) zu konfigurieren. Ein Cluster wird im Netzwerk als einzelne lokale Gruppe angezeigt, die Hosts und Administratoren durch virtuelle IP-Adressen repräsentiert wird. Sie können auch Cluster-Aktivitäten mit Echtzeitberichten überwachen, einschließlich Fehler- und Warnmeldungen für alle Ereignisse, die während der Ausführung verschiedener Vorgänge auftreten können.

Erfahren Sie mehr über "NetApp Element Plug-in für vCenter Server".

- Standardmäßig sendet NetApp HCI Performance- und Alarmstatistiken an den **NetApp SolidFire Active IQ** Service. Im Rahmen des normalen Support-Vertrags überwacht NetApp Support diese Daten und warnt Sie vor Performance-Engpässen oder potenziellen Systemproblemen. Sie müssen ein NetApp Support-Konto erstellen, wenn Sie noch kein Konto haben (auch wenn Sie ein bestehendes SolidFire Active IQ-Konto haben), damit Sie diesen Service nutzen können.

  Erfahren Sie mehr über "NetApp SolidFire Active IQ".

NetApp HCI-URLs

Im Folgenden finden Sie die allgemeinen URLs, die Sie mit NetApp HCI verwenden:

URL	Beschreibung
`https://[IPv4 address of Bond1G interface on a storage node]`	Rufen Sie den Assistenten für die NetApp-Bereitstellungsmodul auf, um NetApp HCI zu installieren und zu konfigurieren. "Weitere Informationen ."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	Sie haben Zugriff auf NetApp Hybrid Cloud Control, um Upgrades, Erweiterungen und Monitoring Ihrer NetApp HCI Installation und Update-Managementservices durchzuführen. "Weitere Informationen ."
`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://<ManagementNodeIP>:9443`	Registrieren Sie das vCenter Plug-in-Paket im vSphere Web Client.
`https://activeiq.solidfire.com`	Überwachen Sie Ihre Daten und erhalten Sie Warnmeldungen zu Performance-Engpässen oder potenziellen Systemproblemen.
`https://<ManagementNodeIP>/mnode`	Managementservices müssen mithilfe der REST-API-UI vom Managementknoten manuell aktualisiert werden.
`https://[storage cluster MVIP address]`	Zugreifen auf die Benutzeroberfläche der NetApp Element Software

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Benutzerkonten

Um auf Storage-Ressourcen in Ihrem System zuzugreifen, müssen Sie Benutzerkonten einrichten.

Benutzerkontenverwaltung

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.

Mit NetApp Hybrid Cloud Control lassen sich folgende Account-Typen erstellen und verwalten:

- Administratorkonten für das Storage-Cluster
- Autoritäre Benutzerkonten
- Volume-Konten, nur für den Storage Cluster spezifisch, auf dem sie erstellt wurden.

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 Cluster-Administratorkonten verwalten, indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Kennwort für den Cluster-Administrator ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Weitere Informationen finden Sie im "SolidFire und Element Documentation Center".

Autoritäre Benutzerkonten

Autorisierte 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.

Weitere Informationen

- "Benutzerkonten verwalten"
- "Informationen zu Clustern"
- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Documentation Center"

Datensicherung

Begriffe der NetApp HCI Datensicherung umfassen verschiedene Arten von Remote-Replizierung, Volume Snapshots, Volume-Klonen, Sicherungsdomänen und

Hochverfügbarkeit mit der Double Helix Technologie.

Die NetApp HCI Datensicherung umfasst folgende Konzepte:

- Typen der Remote-Replizierung
- Volume Snapshots zur Datensicherung
- Volume-Klone
- Backup- und Restore-Prozess – Übersicht für SolidFire Storage
- 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

Siehe "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.

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 SolidFire Cluster auf einem externen Objektspeicher oder auf einem anderen SolidFire 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.

Backup- und Restore-Prozess – Übersicht für SolidFire 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 Sicherungsdomäne ist ein Node oder eine Gruppe von Nodes, die so gruppiert werden, dass ein Teil oder sogar alle Knoten ausfallen könnten, ohne dass die Datenverfügbarkeit beeinträchtigt wird. Sicherungsdomänen ermöglichen die automatische Selbstreparatur eines Storage-Clusters beim Verlust eines Chassis (Chassis-Affinität) oder einer gesamten Domäne (Chassis-Gruppe).

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 Sicherungsdomäne.
- Auf Chassis-Ebene befinden sich nur Nodes, die sich ein Chassis teilen, in derselben Schutzdomäne.
  - 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.

Sie können das NetApp Element-Plug-in für vCenter Server manuell "Aktivieren Sie die Überwachung von Schutzdomänen" verwenden. Sie können einen Schutz-Domain-Schwellenwert basierend auf Node- oder Chassis-Domänen auswählen.

Wenn ein neues Cluster erstellt wird, sollten Storage-Nodes genutzt werden, die sich in einem gemeinsamen Chassis befinden, sollte mithilfe der Sicherungs-Domains-Funktion ein Design für Ausfallschutz auf Chassis-Ebene in Betracht gezogen werden.

Sie können ein benutzerdefiniertes Schutz-Domain-Layout definieren, in dem jeder Knoten einer und nur einer benutzerdefinierten Schutzdomäne zugeordnet ist. Standardmäßig wird jeder Knoten derselben benutzerdefinierten Standard-Schutzdomäne zugewiesen.

Siehe "SolidFire und Element 12.2 Documentation Center".

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.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"

Cluster

Ein Cluster ist eine Gruppe von Nodes, die als Ganzes funktionieren und Storage- oder Computing-Ressourcen bereitstellen. Ab NetApp HCI 1.8 können Sie ein Storage-Cluster mit zwei Knoten haben. Ein Storage-Cluster wird im Netzwerk als einzelne logische Gruppe angezeigt und kann dann als Block-Storage genutzt werden.

Die Storage-Ebene in NetApp HCI wird durch NetApp Element bereitgestellt. Die Management-Ebene wird durch das NetApp Element Plug-in für vCenter Server bereitgestellt. Ein Storage-Node ist ein Server, der eine Sammlung von Laufwerken enthält, die über die Bond10G-Netzwerkschnittstelle miteinander kommunizieren. Jeder Storage Node ist mit zwei Netzwerken verbunden, Storage und Management, wobei jeder über zwei unabhängige Links verfügt, 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.

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.

Benutzer können mit NetApp Hybrid Cloud Control managen.

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 managen" über die Benutzeroberfläche der Element Software (Element Web UI).

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

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-Cluster mit zwei Nodes

Ab NetApp HCI 1.8 können Sie ein Storage-Cluster mit zwei Storage-Nodes einrichten.

- Sie können bestimmte Node-Typen verwenden, um das Storage-Cluster mit zwei Nodes zu bilden. Siehe "Versionshinweise zu NetApp HCI 1.8".

  In einem Cluster mit zwei Nodes sind die Storage-Nodes auf Nodes mit 480-GB- und 960-GB-Laufwerken begrenzt, und die Nodes müssen denselben Modelltyp aufweisen.

- Storage-Cluster mit zwei Nodes eignen sich am besten für kleinere Implementierungen mit Workloads, die nicht von hohen Anforderungen an Kapazität und Performance abhängig sind.
- Neben zwei Storage-Nodes enthält ein Storage-Cluster mit zwei Nodes auch zwei **NetApp HCI Witness**

Nodes.

Weitere Informationen zu "Witness Nodes"

- Sie können ein zwei-Node-Storage-Cluster auf ein Storage-Cluster mit drei Nodes skalieren. Die Ausfallsicherheit durch drei-Node-Cluster wird erhöht, da sich Storage-Node-Ausfälle automatisch beheben lassen.
- Storage-Cluster mit zwei Nodes bieten dieselben Sicherheitsfunktionen und Funktionen wie herkömmliche Storage-Cluster mit vier Nodes.
- Storage-Cluster mit zwei Nodes nutzen dieselben Netzwerke wie Storage-Cluster mit vier Nodes. Die Netzwerke werden während der NetApp HCI-Implementierung mit dem NetApp Deployment Engine Wizard eingerichtet.

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. Witness Nodes werden in einem Cluster mit zwei Knoten verwendet, um sicherzustellen, dass genügend Speicherknoten vorhanden sind, um ein gültiges Ensemble-Quorum zu bilden. Für die Erstellung eines Ensembles sind Storage Nodes vor Witness Nodes vorzuziehen. Für das Ensemble mit mindestens drei Nodes, das ein Storage Cluster mit zwei Nodes beinhaltet, werden zwei Storage-Nodes und ein Witness-Node verwendet.

In einem Ensemble mit drei Nodes mit zwei Storage-Nodes und einem Witness-Node wird bei einem Ausfall eines Storage-Node ein eingeschränkter Zustand des Clusters ausgeführt. Von den beiden Zeugenknoten kann nur einer im Ensemble aktiv sein. Der zweite Witness Node kann dem Ensemble nicht hinzugefügt werden, da er die Backup-Rolle ausführt. Das Cluster bleibt im eingeschränkten Zustand, bis der Offline-Storage-Node wieder in den Online-Status wechselt oder ein Ersatz-Node dem Cluster hinzugefügt wird.

Wenn ein Witness Node ausfällt, schließt sich der verbleibende Witness Node dem Ensemble zu einem Dreiknotenensemble an. Sie können einen neuen Witness Node bereitstellen, um den fehlgeschlagenen Witness Node zu ersetzen.

Automatische Reparatur und Fehlerbehandlung in Storage-Clustern mit zwei Nodes

Wenn eine Hardwarekomponente in einem Node ausfällt, der Teil eines herkömmlichen Clusters ist, kann der Cluster Daten ausgleichen, die sich auf der Komponente befinden, die zu anderen verfügbaren Nodes im Cluster ausgefallen ist. Diese Funktion zur automatischen Fehlerbehebung ist in einem Storage-Cluster mit zwei Nodes nicht verfügbar, da dem Cluster mindestens drei physische Storage-Nodes zur automatischen Fehlerbehebung zur Verfügung stehen müssen. Wenn ein Node in einem Cluster mit zwei Nodes ausfällt, muss im Cluster mit zwei Nodes keine zweite Kopie der Daten neu gebootet werden. Neue Schreibvorgänge werden für Blockdaten im verbleibenden aktiven Storage-Node repliziert. Wenn der ausgefallene Node ersetzt und zum Cluster hinzugefügt wird, werden die Daten zwischen den beiden physischen Storage-Nodes gleichmäßig verteilt.

Storage Cluster mit drei oder mehr Nodes

Die Erweiterung von zwei Storage-Nodes auf drei Storage-Nodes erhöht die Ausfallsicherheit des Clusters. Diese Lösung ermöglicht automatische Reparatur bei Node- und Laufwerksausfällen, bietet jedoch keine zusätzliche Kapazität. Sie können die Erweiterung mithilfe der "UI für die NetApp Hybrid Cloud Control". Bei der Erweiterung von einem Cluster mit zwei Nodes auf ein Cluster mit drei Nodes kann die Kapazität ungenutzt

bleiben (siehe Ungenutzte Kapazität). Der UI-Assistent zeigt vor der Installation Warnungen zu ungenutzte Kapazität an. Ein einziger Zeuge-Knoten ist weiterhin verfügbar, um das Ensemble-Quorum bei Ausfall eines Speicherknoten zu erhalten, wobei ein zweiter Zeuge-Knoten im Standby-Modus. Wenn Sie ein Storage-Cluster mit drei Nodes auf ein Cluster mit vier Nodes erweitern, werden die Kapazität und die Performance erhöht. In einem Cluster mit vier Nodes sind Witness Nodes nicht mehr erforderlich, um das Cluster-Quorum zu bilden. Sie können das System auf bis zu 64 Computing-Nodes und 40 Storage-Nodes erweitern.

Weitere Informationen

- "NetApp HCI Storage Cluster mit zwei Nodes – TR-4823"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Knoten

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

NetApp HCI und Element Software definiert verschiedene Node-Rollen für ein Cluster. Die vier Arten von Node-Rollen sind **Management Node**, **Storage Node**, **Compute Node** und **NetApp HCI Witness Nodes**.

Management-Node

Der Management-Node (manchmal als mNode abgekürzt) 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.

Der Management-Node ist eine Virtual Machine (VM), die parallel mit einem oder mehreren auf Element Software basierenden Storage-Clustern ausgeführt wird. Neben Upgrades bietet es Systemservices wie Monitoring und Telemetrie, Management von Cluster-Ressourcen und -Einstellungen, Tests und Utilities sowie NetApp Support-Zugang zur Fehlerbehebung. Ab Element 11.3 fungiert der Management Node als Microservice-Host, wodurch sich ausgewählte Softwareservices schneller außerhalb der Hauptversionen aktualisieren lassen. Diese Microservices und Managementservices, wie Active IQ Collector, QoSSIOC für das vCenter Plug-in und der Management-Node-Service, werden häufig als Service-Bundles aktualisiert.

Storage-Nodes

NetApp HCI Storage-Nodes sind Hardware, die die Storage-Ressourcen für ein NetApp HCI System bereitstellen. Laufwerke im Node enthalten Block- und Metadatenspeicherplatz für den Daten-Storage und das Datenmanagement. Jeder Node enthält ein Factory Image der NetApp Element Software. NetApp HCI Storage Nodes können mit dem NetApp Element Management-Erweiterungspunkt gemanagt werden.

Computing Nodes

NetApp HCI Computing-Nodes sind Hardware, die Computing-Ressourcen wie CPU, Arbeitsspeicher und Netzwerk bereitstellt, die für die Virtualisierung bei der NetApp HCI Installation erforderlich sind. Da auf jedem Server VMware ESXi ausgeführt wird, muss das Management der Computing-Nodes von NetApp HCI (Hinzufügen oder Entfernen von Hosts) außerhalb des Plug-ins im Menü Hosts und Cluster in vSphere erfolgen. Unabhängig davon, ob es sich um ein Storage-Cluster mit vier Nodes oder ein Storage-Cluster mit zwei Nodes handelt, bleibt die Mindestanzahl an Computing-Nodes bei NetApp HCI Implementierungen

erhalten.

Witness Nodes

NetApp HCI Witness Nodes sind VMs, die auf Computing-Nodes parallel mit einem Element Software-basierten Storage-Cluster ausgeführt werden. Witness Nodes hosten keine Slice- oder Block-Services. Ein Witness Node ermöglicht bei Ausfall eines Storage-Nodes die Verfügbarkeit des Storage-Clusters. Sie können Witness Nodes auf dieselbe Weise managen und aktualisieren wie andere Storage Nodes. Ein Storage-Cluster kann bis zu vier Witness-Nodes enthalten. Ihr primärer Zweck ist es, sicherzustellen, dass genügend Clusterknoten vorhanden sind, um ein gültiges Ensemble-Quorum zu bilden.

Best Practice: Konfigurieren Sie die Witness Node VMs so konfigurieren Sie den lokalen Datastore des Computing-Nodes (Standardeinstellung: Nde) und konfigurieren Sie diese nicht auf Shared Storage, z. B. SolidFire Storage Volumes. Um eine automatische Migration der VMs zu verhindern, stellen Sie die Automatisierungsebene des Distributed Resource Scheduler (DRS) der Witness Node VM auf **deaktivierte** ein. Dadurch wird verhindert, dass beide Witness-Nodes auf demselben Computing-Node ausgeführt werden und eine Konfiguration mit einem Hochverfügbarkeitspaar (HA-Paar) erstellt wird.

Erfahren Sie mehr über "Ressourcenanforderungen Witness Node" und "Anforderungen an die IP-Adresse des Witness Node".

In einem Storage-Cluster mit zwei Nodes werden mindestens zwei Witness-Nodes für Redundanz bereitgestellt, falls ein Witness-Node ausfällt. Wenn der Installationsprozess von NetApp HCI Witness Nodes installiert, wird eine VM-Vorlage in VMware vCenter gespeichert, mit der Sie einen Witness-Node neu bereitstellen können, falls dieser versehentlich entfernt, verloren oder beschädigt wurde. Sie können auch die Vorlage verwenden, um einen Witness Node neu zu implementieren, wenn ein ausgefallener Computing-Node, der den Witness Node hostet, ersetzt werden muss. Anweisungen hierzu finden Sie im Abschnitt **Neuimplementierung Witness Nodes für zwei- und drei-Knoten-Speicher-Cluster** "Hier".

Weitere Informationen

- "NetApp HCI Storage Cluster mit zwei Nodes – TR-4823"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Storage

Wartungsmodus

Wenn Sie einen Storage Node für Wartungsarbeiten, wie z. B. Software-Upgrades oder Host-Reparaturen, offline schalten müssen, können Sie die Auswirkungen auf den Rest des Storage-Clusters durch Aktivierung des Wartungsmodus für diesen Node auf ein Minimum minimieren. Sie können den Wartungsmodus mit beiden Appliance-Nodes und SolidFire Enterprise SDS-Nodes verwenden.

Sie können einen Storage Node nur in den Wartungsmodus versetzen, wenn der Node in einem ordnungsgemäßen Zustand (keine Blockierung von Cluster-Fehlern) ist und das Storage Cluster einem Ausfall einzelner Nodes gegenüber tolerant ist. Sobald Sie den Wartungsmodus für einen gesunden und toleranten

Node aktivieren, wird der Node nicht sofort migriert. Er wird überwacht, bis die folgenden Bedingungen erfüllt sind:

- Für alle auf dem Node gehosteten Volumes ist ein Failover fehlgeschlagen
- Der Node hostet für ein Volume nicht mehr als primärer Node
- Jedem Failover eines Volumes wird ein temporärer Standby-Node zugewiesen

Nachdem diese Kriterien erfüllt sind, wird der Node in den Wartungsmodus versetzt. Wenn diese Kriterien innerhalb eines Zeitraums von 5 Minuten nicht erfüllt werden, wechselt der Node nicht in den Wartungsmodus.

Wenn Sie den Wartungsmodus für einen Storage-Node deaktivieren, wird der Node überwacht, bis die folgenden Bedingungen erfüllt sind:

- Alle Daten werden vollständig zum Node repliziert
- Alle blockierenden Cluster-Fehler werden behoben
- Alle temporären Standby-Node-Zuweisungen für die auf dem Node gehosteten Volumes wurden deaktiviert

Nachdem diese Kriterien erfüllt sind, wird der Node aus dem Wartungsmodus migriert. Wenn diese Kriterien nicht innerhalb einer Stunde erfüllt werden, kann der Node nicht in den Wartungsmodus wechseln.

Bei Verwendung der Element API werden die Status von Vorgängen im Wartungsmodus angezeigt:

- **Deaktiviert**: Es wurde keine Wartung angefordert.
- **FailedToRecover**: Der Knoten konnte nicht von der Wartung wiederherstellen.
- **RecoveringFromMaintenance**: Der Knoten wird gerade von der Wartung wiederhergestellt.
- **VorbereitungForMaintenance**: Es werden Maßnahmen ergriffen, damit ein Knoten die Wartung durchführen kann.
- **ReadyForMaintenance**: Der Knoten ist zur Wartung bereit.

Weitere Informationen

- "SolidFire und Element Documentation Center"

Volumes

Storage wird im NetApp Element System als Volumes bereitgestellt. Volumes sind Blockgeräte, auf die über das Netzwerk über iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Das NetApp Element Plug-in für vCenter Server 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.

Wenn Sie einen Management-Node für NetApp HCI mithilfe der NetApp Deployment Engine implementieren, werden persistente Volumes automatisch aktiviert und konfiguriert.

Eine Option zum Aktivieren persistenter Volumes ist in den Installations- und Upgrade-Skripten bei der Implementierung eines neuen Management-Node enthalten. 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.

Wenn die Funktion persistenter Volumes während der Installation oder eines Upgrades aktiviert ist, erstellt automatisch mehrere Volumes mit NetApp-HCI – Pre-Pend auf den Namen des zugewiesenen Clusters. 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

Weitere Informationen

- "Volumes managen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Volume-Zugriffsgruppen

Eine Volume-Zugriffsgruppe ist eine Sammlung von Volumes, auf die Benutzer entweder über iSCSI oder über Fibre Channel-Initiatoren zugreifen können.

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 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.

Weitere Informationen

- "Management von Volume-Zugriffsgruppen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

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.

Weitere Informationen

- "Verwalten von Initiatoren"
- "Volume-Zugriffsgruppen"
- "Management von Volume-Zugriffsgruppen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

NetApp HCI Lizenzierung

Wenn Sie NetApp HCI verwenden, werden je nach verwendetem System möglicherweise zusätzliche Lizenzen benötigt.

NetApp HCI und VMware vSphere Lizenzierung

Die VMware vSphere-Lizenzierung hängt von Ihrer Konfiguration ab:

Netzwerkoption	Lizenzierung
Option A: Zwei Kabel für Computing-Nodes mithilfe von VLAN-Tagging (alle Computing-Nodes)	Erfordert die Verwendung von vSphere Distributed Switch, für den eine Lizenz für VMware vSphere Enterprise Plus erforderlich ist
Option B: Sechs Kabel für Computing-Nodes mit getaggten VLANs (H410C 2RU 4-Node Computing-Node)	Bei dieser Konfiguration wird standardmäßig vSphere Standard Switch verwendet. Für die optionale Verwendung von vSphere Distributed Switch ist eine VMware Enterprise Plus-Lizenzierung erforderlich.
Option C: Sechs Kabel für Computing-Nodes mithilfe von nativen und getaggten VLANs (H410C, 2RU 4-Node Computing-Node)	Bei dieser Konfiguration wird standardmäßig vSphere Standard Switch verwendet. Für die optionale Verwendung von vSphere Distributed Switch ist eine VMware Enterprise Plus-Lizenzierung erforderlich.

NetApp HCI und ONTAP Select Lizenzierung

Falls Sie eine Version von ONTAP Select zur Verwendung in Verbindung mit einem erworbenen NetApp HCI System bereitgestellt wurden, gelten die folgenden zusätzlichen Einschränkungen:

- Die ONTAP Select Lizenz, die im Paket mit einem NetApp HCI Systemverkauf angeboten wird, darf nur in Verbindung mit den NetApp HCI Computing-Nodes verwendet werden.
- Der Storage für diese ONTAP Select Instanzen muss sich nur auf den NetApp HCI Storage-Nodes befinden.
- Die Verwendung von Computing-Nodes von Drittanbietern oder Storage-Nodes von Drittanbietern ist untersagt.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Maximale Konfigurationswerte für NetApp Hybrid Cloud Control

NetApp HCI umfasst NetApp Hybrid Cloud Control zur Vereinfachung von Computing-Lebenszyklus und Storage-Management. Die Lösung unterstützt Upgrades von Element Software auf Storage-Nodes für NetApp HCI und NetApp SolidFire Storage-Cluster sowie Firmware-Upgrades für NetApp HCI Computing-Nodes in NetApp HCI. Er ist standardmäßig auf den Management-Nodes in NetApp HCI verfügbar.

NetApp Hybrid Cloud Control kommuniziert nicht nur über die von NetApp bereitgestellten Hardware- und Software-Komponenten in einer NetApp HCI-Installation, sondern interagiert auch mit Komponenten anderer Anbieter in der Kundenumgebung wie VMware vCenter. NetApp stimmt die Funktionen von NetApp Hybrid Cloud Control und seine Interaktion mit diesen Drittanbieterkomponenten in der Kundenumgebung auf ein bestimmtes Maß ab. Für optimale Benutzerfreundlichkeit mit NetApp Hybrid Cloud Control empfiehlt NetApp, innerhalb verschiedener Konfigurationsmaxima zu bleiben.

Wenn Sie diese getesteten Grenzwerte überschreiten, treten möglicherweise Probleme mit NetApp Hybrid Cloud Control auf, z. B. eine langsamere Benutzeroberfläche, API-Antworten oder Funktionen, die nicht verfügbar sind. Wenn Sie NetApp für Produkt-Support mit NetApp Hybrid Cloud Control in Umgebungen einsetzen, die über die Konfigurationsmaxima hinausgehen, wird NetApp Support bitten, dass Sie die Konfiguration innerhalb der dokumentierten Konfigurationsmaxima ändern.

Konfigurationsmaxima

NetApp Hybrid Cloud Control unterstützt VMware vSphere-Umgebungen mit bis zu 100 ESXi-Hosts und 1000 virtuellen Maschinen (vergleichbar mit einer kleinen vCenter Server Appliance-Konfiguration).

NetApp HCI-Sicherheit

Beim Einsatz von NetApp HCI werden Ihre Daten durch branchenübliche Sicherheitsprotokolle gesichert.

Verschlüsselung für Storage-Nodes im Ruhezustand

NetApp HCI ermöglicht Ihnen die Verschlüsselung aller im Storage-Cluster gespeicherten Daten.

Alle Laufwerke in Storage-Nodes, die zu Verschlüsselung fähig sind, verwenden die AES-256-Bit-Verschlüsselung auf Laufwerksebene. Jedes Laufwerk verfügt über einen eigenen Verschlüsselungsschlüssel,

der beim ersten Initialized des Laufwerks erstellt wird. Wenn Sie die Verschlüsselungsfunktion aktivieren, wird ein Storage-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. Sie benötigen das Passwort, um das Laufwerk zu entsperren. Da das Laufwerk alle Daten verschlüsselt, sind Ihre Daten jederzeit sicher.

Wenn Sie die Verschlüsselung im Ruhezustand aktivieren, werden die Performance und die Effizienz des Storage-Clusters nicht beeinträchtigt. Wenn Sie ein verschlüsselungsfähiges Laufwerk oder Node mit der Element API oder der Element UI aus dem Storage-Cluster entfernen, werden die Laufwerke im Ruhezustand deaktiviert. Zudem werden die Laufwerke sicher gelöscht, sodass die zuvor auf diesen Laufwerken gespeicherten Daten geschützt sind. Nachdem Sie das Laufwerk entfernt haben, können Sie das Laufwerk mit der API-Methode sicher löschen `SecureEraseDrives`. Wenn Sie ein Laufwerk oder einen Node aus dem Speicher-Cluster entfernen, bleiben die Daten durch das Cluster-weite Passwort und die individuellen Verschlüsselungsschlüssel des Laufwerks geschützt.

Informationen zum Aktivieren und Deaktivieren der Verschlüsselung im Ruhezustand finden Sie "Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster" im SolidFire und Element Documentation Center.

Softwareverschlüsselung für Daten im Ruhezustand

Mithilfe der Softwareverschlüsselung können alle auf die SSDs in einem Storage-Cluster geschriebenen Daten verschlüsselt werden. Dies bietet eine primäre Verschlüsselungsschicht in SolidFire SDS-Nodes ohne Self-Encrypting Drives (SEDs).

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 unter "Erste Schritte mit External Key Management" im Dokumentationszentrum für SolidFire und Elemente.

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 unter "Aktivieren der Multi-Faktor-Authentifizierung" im SolidFire and Element Documentation Center.

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

NetApp SolidFire Storage-Cluster und NetApp HCI Systeme 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 NetApp HCI oder SolidFire Cluster sowohl für HTTPS-Kommunikation als auch für Laufwerkverschlüsselung 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 "Erstellung 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".

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

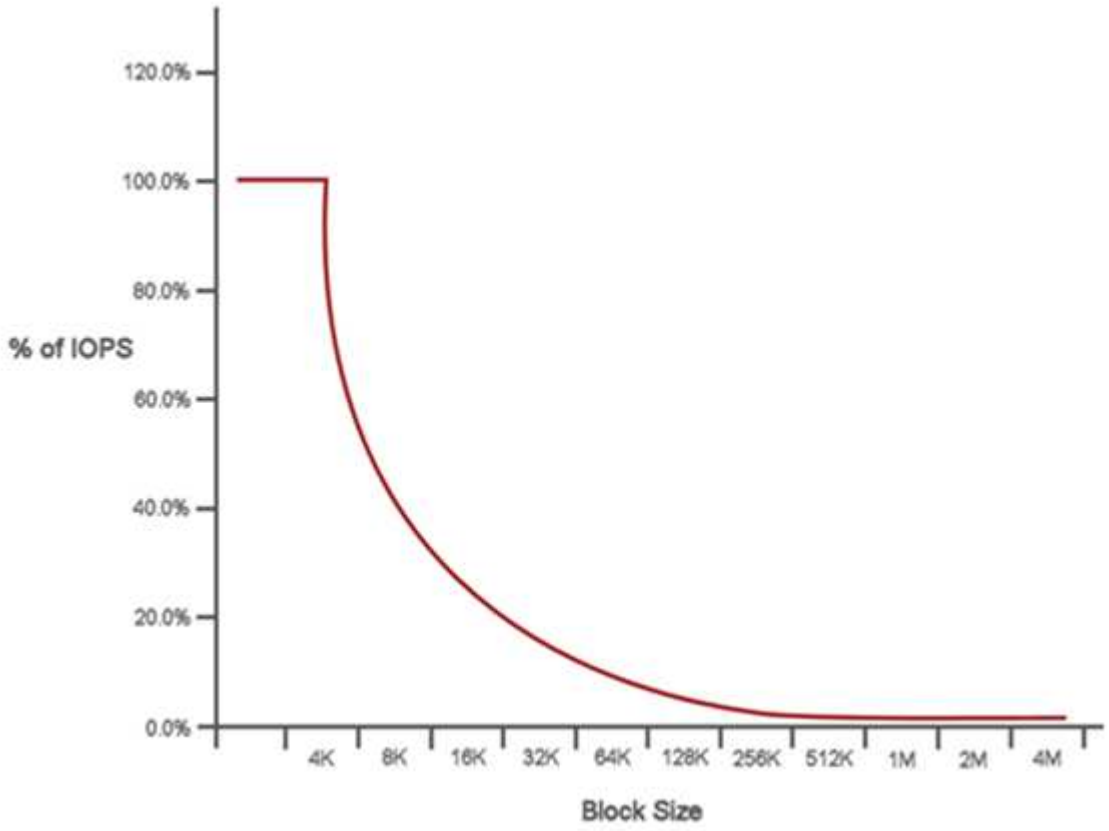
*Diese Schätzungen sind ungefähr. **Maximale IOPS und Burst IOPS können auf 200,000 gesetzt werden. Diese Einstellung ist jedoch nur erlaubt, die Performance eines Volumes effektiv zu nutzen. Die tatsächliche maximale Performance eines Volumes wird durch die Auslastung des Clusters und die Performance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

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"