



Clustereinstellungen konfigurieren

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/de-de/element-software-128/storage/task_system_manage_cluster_enable_and_disable_encryption_for_a_cluster.html on November 12, 2025. Always check docs.netapp.com for the latest.

Inhalt

Clustereinstellungen konfigurieren	1
Aktivieren und Deaktivieren der Verschlüsselung ruhender Daten für einen Cluster	1
Überprüfen Sie den Status der ruhenden Verschlüsselung.	1
Aktivieren Sie die hardwarebasierte Verschlüsselung ruhender Daten	2
Aktivieren Sie die softwarebasierte Verschlüsselung ruhender Daten	2
Hardwarebasierte Verschlüsselung im Ruhezustand deaktivieren	2
Legen Sie den Schwellenwert für die Clusterauslastung fest.	2
Weitere Informationen	3
Volumenlastausgleich aktivieren und deaktivieren.	3
Weitere Informationen	3
Supportzugriff aktivieren und deaktivieren	3
Banner „Nutzungsbedingungen“ verwalten	4
Aktivieren Sie das Banner „Nutzungsbedingungen“	4
Bearbeiten Sie das Banner „Nutzungsbedingungen“	4
Banner „Nutzungsbedingungen“ deaktivieren	4
Stellen Sie das Netzwerkzeitprotokoll ein.	5
Konfigurieren Sie die Network Time Protocol-Server, die der Cluster abfragen soll.	5
Konfigurieren Sie den Cluster so, dass er auf NTP-Broadcasts lauscht.	6
SNMP verwalten	6
Erfahren Sie mehr über SNMP	6
Konfigurieren Sie einen SNMP-Anforderer	7
Konfigurieren eines SNMP-USM-Benutzers	7
SNMP-Traps konfigurieren	8
Anzeigen von Daten verwalteter Objekte mithilfe von Managementinformationsdatenbankdateien	8
Laufwerke verwalten	9
Laufwerksdetails	9
Weitere Informationen	10
Knoten verwalten	10
Knoten verwalten	10
Füge einem Cluster einen Knoten hinzu.	10
Node-Versionierung und Kompatibilität	11
Clusterkapazität in einer gemischten Knotenumgebung	12
Knotendetails anzeigen	13
Details zu Fibre-Channel-Anschlüssen anzeigen	14
Weitere Informationen	14
Virtuelle Netzwerke verwalten	14
Virtuelle Netzwerke verwalten	14
Fügen Sie ein virtuelles Netzwerk hinzu	15
Virtuelles Routing und Weiterleitung aktivieren	16
Bearbeiten eines virtuellen Netzwerks	17
VRF-VLANs bearbeiten	17
Löschen eines virtuellen Netzwerks	18

Clustereinstellungen konfigurieren

Aktivieren und Deaktivieren der Verschlüsselung ruhender Daten für einen Cluster

Mit SolidFire -Clustern können Sie alle ruhenden Daten, die auf Cluster-Laufwerken gespeichert sind, verschlüsseln. Sie können den clusterweiten Schutz von selbstverschlüsselnden Laufwerken (SED) mithilfe einer der folgenden Methoden aktivieren: "[Hardware- oder softwarebasierte Verschlüsselung ruhender Daten](#)" Die

Sie können die Hardwareverschlüsselung ruhender Daten über die Element-Benutzeroberfläche oder die API aktivieren. Die Aktivierung der Hardwareverschlüsselung ruhender Daten hat keinen Einfluss auf die Leistung oder Effizienz des Clusters. Die Softwareverschlüsselung ruhender Daten kann ausschließlich über die Element API aktiviert werden.

Die hardwarebasierte Verschlüsselung ruhender Daten ist bei der Clustererstellung nicht standardmäßig aktiviert und kann über die Element-Benutzeroberfläche aktiviert und deaktiviert werden.

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

Was du brauchst

- Sie verfügen über Cluster-Administratorrechte, um Verschlüsselungseinstellungen zu aktivieren oder zu ändern.
- Bei hardwarebasierter Verschlüsselung ruhender Daten haben Sie sichergestellt, dass sich der Cluster in einem fehlerfreien Zustand befindet, bevor Sie die Verschlüsselungseinstellungen ändern.
- Wenn Sie die Verschlüsselung deaktivieren, müssen zwei Knoten an einem Cluster beteiligt sein, um auf den Schlüssel zum Deaktivieren der Verschlüsselung auf einem Laufwerk zugreifen zu können.

Überprüfen Sie den Status der ruhenden Verschlüsselung.

Um den aktuellen Status der Verschlüsselung ruhender Daten und/oder der Softwareverschlüsselung ruhender Daten auf dem Cluster anzuzeigen, verwenden Sie die "[GetClusterInfo](#)" Verfahren. Sie können die "[GetSoftwareEncryptionAtRestInfo](#)" Methode zum Abrufen von Informationen, die der Cluster zur Verschlüsselung ruhender Daten verwendet.

 Das Element-Software-UI-Dashboard bei <https://<MVIP>> Aktuell wird nur der Verschlüsselungsstatus für hardwarebasierte Verschlüsselung angezeigt.

Optionen

- [Aktivieren Sie die hardwarebasierte Verschlüsselung ruhender Daten](#)
- [Aktivieren Sie die softwarebasierte Verschlüsselung ruhender Daten](#)
- [Hardwarebasierte Verschlüsselung im Ruhezustand deaktivieren](#)

Aktivieren Sie die hardwarebasierte Verschlüsselung ruhender Daten



Um die Verschlüsselung ruhender Daten mithilfe einer externen Schlüsselverwaltungskonfiguration zu aktivieren, müssen Sie die Verschlüsselung ruhender Daten über die "[API](#)" Die Durch Aktivierung über die vorhandene Element UI-Schaltfläche werden wieder intern generierte Schlüssel verwendet.

1. Wählen Sie in der Element-Benutzeroberfläche **Cluster > Einstellungen**.
2. Wählen Sie **Verschlüsselung ruhender Daten** aktivieren.

Aktivieren Sie die softwarebasierte Verschlüsselung ruhender Daten



Die Softwareverschlüsselung ruhender Daten kann nicht deaktiviert werden, nachdem sie auf dem Cluster aktiviert wurde.

1. Führen Sie während der Clustererstellung Folgendes aus: "[Methode zum Erstellen von Clustern](#)" mit `enableSoftwareEncryptionAtRest` eingestellt auf `true` Die

Hardwarebasierte Verschlüsselung im Ruhezustand deaktivieren

1. Wählen Sie in der Element-Benutzeroberfläche **Cluster > Einstellungen**.
2. Wählen Sie **Verschlüsselung ruhender Daten** deaktivieren.

Weitere Informationen

- "[SolidFire und Element-Softwaredokumentation](#)"
- "[Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte](#)"

Legen Sie den Schwellenwert für die Clusterauslastung fest.

Sie können den Schwellenwert, ab dem das System eine Warnung wegen Überfüllung eines Blockclusters ausgibt, mit den folgenden Schritten ändern. Darüber hinaus können Sie mit der `ModifyClusterFullThreshold` API-Methode die Stufe ändern, ab der das System eine Block- oder Metadatenwarnung generiert.

Was du brauchst

Sie benötigen Cluster-Administratorrechte.

Schritte

1. Klicken Sie auf **Cluster > Einstellungen**.
2. Im Abschnitt „Cluster Full Settings“ geben Sie einen Prozentsatz für **Warnmeldung ausgeben, wenn _% der Kapazität vor dem Ausfall eines Knotens verbleiben, bevor Helix sich nicht mehr erholen kann** ein.
3. Klicken Sie auf **Änderungen speichern**.

Weitere Informationen

"Wie werden die Blockraumschwellenwerte für das Element berechnet?"

Volumenlastausgleich aktivieren und deaktivieren

Ab Element 12.8 können Sie Volume Load Balancing verwenden, um Volumes auf Knoten basierend auf den tatsächlichen IOPS jedes Volumes anstatt der in der QoS-Richtlinie konfigurierten minimalen IOPS zu verteilen. Sie können die Volume Load Balancing-Funktion, die standardmäßig deaktiviert ist, über die Element-Benutzeroberfläche oder die API aktivieren und deaktivieren.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Ändern Sie im Abschnitt „Clusterspezifisch“ den Status für die Volumenlastverteilung:

Volumenlastausgleich aktivieren

Wählen Sie **Lastverteilung auf Basis der tatsächlichen IOPS aktivieren** und bestätigen Sie Ihre Auswahl.

Lastverteilung für Volumes deaktivieren:

Wählen Sie **Lastverteilung auf Basis tatsächlicher IOPS deaktivieren** und bestätigen Sie Ihre Auswahl.

3. Optional können Sie unter **Berichterstellung > Übersicht** die Statusänderung für Saldo auf Basis tatsächlicher IOPS bestätigen. Möglicherweise müssen Sie in den Cluster-Health-Informationen nach unten scrollen, um den Status anzuzeigen.

Weitere Informationen

- ["Aktivieren Sie den Volumenlastausgleich über die API."](#)
- ["Deaktivieren Sie die Volumenlastverteilung über die API."](#)
- ["Volumen-QoS-Richtlinien erstellen und verwalten"](#)

Supportzugriff aktivieren und deaktivieren

Sie können den Supportzugriff aktivieren, um dem NetApp Supportpersonal vorübergehend über SSH Zugriff auf die Speicherknoten zur Fehlerbehebung zu gewähren.

Sie benötigen Cluster-Administratorrechte, um den Supportzugriff zu ändern.

1. Klicken Sie auf **Cluster > Einstellungen**.
2. Im Abschnitt „Supportzugriff aktivieren/deaktivieren“ geben Sie die Dauer (in Stunden) ein, für die der Support Zugriff haben soll.
3. Klicken Sie auf **Supportzugriff aktivieren**.

4. **Optional:** Um den Supportzugriff zu deaktivieren, klicken Sie auf **Supportzugriff deaktivieren**.

Banner „Nutzungsbedingungen“ verwalten“

Sie können ein Banner aktivieren, bearbeiten oder konfigurieren, das eine Nachricht für den Benutzer enthält.

Optionen

[Aktivieren Sie das Banner „Nutzungsbedingungen“.](#) [Bearbeiten Sie das Banner „Nutzungsbedingungen“.](#)
[Banner „Nutzungsbedingungen“ deaktivieren](#)

Aktivieren Sie das Banner „Nutzungsbedingungen“.

Sie können ein Banner mit den Nutzungsbedingungen aktivieren, das beim Anmelden eines Benutzers an der Element-Benutzeroberfläche angezeigt wird. Wenn der Benutzer auf das Banner klickt, erscheint ein Textdialogfeld mit der Nachricht, die Sie für den Cluster konfiguriert haben. Das Banner kann jederzeit ausgeblendet werden.

Sie benötigen Cluster-Administratorrechte, um die Nutzungsbedingungen-Funktionalität zu aktivieren.

1. Klicken Sie auf **Benutzer > Nutzungsbedingungen**.
2. Geben Sie im Formular **Nutzungsbedingungen** den Text ein, der im Dialogfeld „Nutzungsbedingungen“ angezeigt werden soll.



Die maximale Zeichenanzahl beträgt 4096.

3. Klicken Sie auf **Aktivieren**.

Bearbeiten Sie das Banner „Nutzungsbedingungen“.

Sie können den Text bearbeiten, den ein Benutzer sieht, wenn er das Anmeldebanner mit den Nutzungsbedingungen auswählt.

Was du brauchst

- Sie benötigen Cluster-Administratorrechte, um die Nutzungsbedingungen zu konfigurieren.
- Stellen Sie sicher, dass die Funktion „Nutzungsbedingungen“ aktiviert ist.

Schritte

1. Klicken Sie auf **Benutzer > Nutzungsbedingungen**.
2. Im Dialogfeld **Nutzungsbedingungen** können Sie den Text bearbeiten, der angezeigt werden soll.



Die maximale Zeichenanzahl beträgt 4096.

3. Klicken Sie auf **Änderungen speichern**.

Banner „Nutzungsbedingungen“ deaktivieren

Sie können das Banner mit den Nutzungsbedingungen deaktivieren. Wenn das Banner deaktiviert ist, wird der Benutzer bei der Nutzung der Element-Benutzeroberfläche nicht mehr aufgefordert, die Nutzungsbedingungen zu akzeptieren.

Was du brauchst

- Sie benötigen Cluster-Administratorrechte, um die Nutzungsbedingungen zu konfigurieren.
- Stellen Sie sicher, dass die Nutzungsbedingungen aktiviert sind.

Schritte

1. Klicken Sie auf **Benutzer > Nutzungsbedingungen**.
2. Klicken Sie auf **Deaktivieren**.

Stellen Sie das Netzwerkzeitprotokoll ein.

Konfigurieren Sie die Network Time Protocol-Server, die der Cluster abfragen soll.

Sie können jeden Knoten in einem Cluster anweisen, einen Network Time Protocol (NTP)-Server nach Aktualisierungen abzufragen. Der Cluster kontaktiert ausschließlich konfigurierte Server und fordert von diesen NTP-Informationen an.

Das NTP wird verwendet, um Uhren über ein Netzwerk zu synchronisieren. Die Anbindung an einen internen oder externen NTP-Server sollte Teil der initialen Cluster-Einrichtung sein.

Konfigurieren Sie NTP auf dem Cluster so, dass es auf einen lokalen NTP-Server verweist. Sie können die IP-Adresse oder den FQDN-Hostnamen verwenden. Der standardmäßige NTP-Server, der bei der Clustererstellung festgelegt wird, ist us.pool.ntp.org; eine Verbindung zu dieser Website kann jedoch je nach physischem Standort des SolidFire Clusters nicht immer hergestellt werden.

Die Verwendung des FQDN hängt davon ab, ob die DNS-Einstellungen des jeweiligen Speicherknotens vorhanden und betriebsbereit sind. Konfigurieren Sie dazu die DNS-Server auf jedem Speicherknoten und stellen Sie sicher, dass die Ports geöffnet sind, indem Sie die Seite „Netzwerkportanforderungen“ überprüfen.

Sie können bis zu fünf verschiedene NTP-Server eingeben.



Sie können sowohl IPv4- als auch IPv6-Adressen verwenden.

Was du brauchst

Sie benötigen Cluster-Administratorrechte, um diese Einstellung zu konfigurieren.

Schritte

1. Konfigurieren Sie eine Liste von IPs und/oder FQDNs in den Servereinstellungen.
2. Stellen Sie sicher, dass die DNS-Einstellungen auf den Knoten korrekt konfiguriert sind.
3. Klicken Sie auf **Cluster > Einstellungen**.
4. Unter „Einstellungen für das Netzwerkzeitprotokoll“ wählen Sie **Nein**, wodurch die Standard-NTP-Konfiguration verwendet wird.
5. Klicken Sie auf **Änderungen speichern**.

Weitere Informationen

- ["Konfigurieren Sie den Cluster so, dass er auf NTP-Broadcasts lauscht."](#)
- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Konfigurieren Sie den Cluster so, dass er auf NTP-Broadcasts lauscht.

Durch die Verwendung des Broadcast-Modus können Sie jeden Knoten in einem Cluster anweisen, im Netzwerk auf NTP-Broadcast-Nachrichten (Network Time Protocol) von einem bestimmten Server zu achten.

Das NTP wird verwendet, um Uhren über ein Netzwerk zu synchronisieren. Die Anbindung an einen internen oder externen NTP-Server sollte Teil der initialen Cluster-Einrichtung sein.

Was du brauchst

- Sie benötigen Cluster-Administratorrechte, um diese Einstellung zu konfigurieren.
- Sie müssen einen NTP-Server in Ihrem Netzwerk als Broadcast-Server konfigurieren.

Schritte

1. Klicken Sie auf **Cluster > Einstellungen**.
2. Tragen Sie den oder die NTP-Server, die den Broadcast-Modus verwenden, in die Serverliste ein.
3. Unter „Einstellungen für das Netzwerkzeitprotokoll“ wählen Sie **Ja**, um einen Broadcast-Client zu verwenden.
4. Um den Broadcast-Client einzustellen, geben Sie im Feld **Server** den NTP-Server ein, den Sie im Broadcast-Modus konfiguriert haben.
5. Klicken Sie auf **Änderungen speichern**.

Weitere Informationen

- ["Konfigurieren Sie die Network Time Protocol-Server, die der Cluster abfragen soll."](#)
- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

SNMP verwalten

Erfahren Sie mehr über SNMP

Sie können das Simple Network Management Protocol (SNMP) in Ihrem Cluster konfigurieren.

Sie können einen SNMP-Anforderer auswählen, die zu verwendende SNMP-Version festlegen, den Benutzer des SNMP User-based Security Model (USM) identifizieren und Traps konfigurieren, um den SolidFire Cluster zu überwachen. Sie können auch Managementinformationsdatenbankdateien einsehen und darauf zugreifen.



Sie können sowohl IPv4- als auch IPv6-Adressen verwenden.

SNMP-Details

Auf der SNMP-Seite des Cluster-Tabs können Sie die folgenden Informationen einsehen.

- **SNMP MIBs**

Die MIB-Dateien, die Sie ansehen oder herunterladen können.

- **Allgemeine SNMP-Einstellungen**

Sie können SNMP aktivieren oder deaktivieren. Nachdem Sie SNMP aktiviert haben, können Sie die gewünschte Version auswählen. Bei Version 2 können Sie Anforderer hinzufügen, und bei Version 3 können Sie USM-Benutzer einrichten.

- **SNMP-Trap-Einstellungen**

Sie können auswählen, welche Fallen Sie erfassen möchten. Sie können Host, Port und Community-String für jeden Trap-Empfänger festlegen.

Konfigurieren Sie einen SNMP-Anforderer

Wenn SNMP Version 2 aktiviert ist, können Sie einen Anforderer aktivieren oder deaktivieren und Anforderer so konfigurieren, dass sie autorisierte SNMP-Anfragen empfangen.

1. Klicken Sie auf Menü:Cluster[SNMP].
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.
3. Wählen Sie in der Liste **Version** die Option **Version 2** aus.
4. Geben Sie im Abschnitt **Anforderer** die **Community-Zeichenfolge** und die **Netzwerk**-Informationen ein.



Standardmäßig ist die Community-Zeichenfolge „public“ und das Netzwerk „localhost“. Sie können diese Standardeinstellungen ändern.

5. **Optional:** Um einen weiteren Anforderer hinzuzufügen, klicken Sie auf **Anforderer hinzufügen** und geben Sie die **Community-Zeichenfolge** und die **Netzwerk**-Informationen ein.
6. Klicken Sie auf **Änderungen speichern**.

Weitere Informationen

- [SNMP-Traps konfigurieren](#)
- [Anzeigen von Daten verwalteter Objekte mithilfe von Managementinformationsdatenbankdateien](#)

Konfigurieren eines SNMP-USM-Benutzers

Wenn Sie SNMP Version 3 aktivieren, müssen Sie einen USM-Benutzer konfigurieren, der autorisierte SNMP-Anfragen empfängt.

1. Klicken Sie auf **Cluster > SNMP**.
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.
3. Wählen Sie in der Liste **Version** die Option **Version 3** aus.
4. Im Abschnitt **USM-Benutzer** geben Sie bitte den Namen, das Passwort und die Passphrase ein.
5. **Optional:** Um einen weiteren USM-Benutzer hinzuzufügen, klicken Sie auf **USM-Benutzer hinzufügen** und geben Sie den Namen, das Passwort und die Passphrase ein.
6. Klicken Sie auf **Änderungen speichern**.

SNMP-Traps konfigurieren

Systemadministratoren können SNMP-Traps, auch Benachrichtigungen genannt, verwenden, um den Zustand des SolidFire Clusters zu überwachen.

Wenn SNMP-Traps aktiviert sind, generiert der SolidFire -Cluster Traps, die mit Ereignisprotokolleinträgen und Systemwarnungen verknüpft sind. Um SNMP-Benachrichtigungen zu erhalten, müssen Sie die zu generierenden Traps auswählen und die Empfänger der Trap-Informationen identifizieren. Standardmäßig werden keine Traps generiert.

1. Klicken Sie auf **Cluster > SNMP**.
2. Wählen Sie im Abschnitt **SNMP-Trap-Einstellungen** einen oder mehrere Trap-Typen aus, die das System generieren soll:
 - Cluster-Fehlerfallen
 - Clusteraufgelöste Fehlerfallen
 - Cluster-Ereignisfallen
3. Im Abschnitt **Trap-Empfänger** geben Sie die Host-, Port- und Community-String-Informationen für einen Empfänger ein.
4. **Optional:** Um einen weiteren Trap-Empfänger hinzuzufügen, klicken Sie auf **Trap-Empfänger hinzufügen** und geben Sie Host-, Port- und Community-String-Informationen ein.
5. Klicken Sie auf **Änderungen speichern**.

Anzeigen von Daten verwalteter Objekte mithilfe von Managementinformationsdatenbankdateien

Sie können die Management Information Base (MIB)-Dateien, die zur Definition der einzelnen verwalteten Objekte verwendet werden, anzeigen und herunterladen. Die SNMP-Funktion unterstützt den Lesezugriff auf die in der SolidFire-StorageCluster-MIB definierten Objekte.

Die in der MIB bereitgestellten statistischen Daten zeigen die Systemaktivität für Folgendes:

- Clusterstatistik
- Volumenstatistik
- Volumen nach Kontostatistik
- Knotenstatistiken
- Weitere Daten wie Berichte, Fehler und Systemereignisse

Das System unterstützt auch den Zugriff auf die MIB-Datei, die die oberen Zugriffspunkte (OIDs) für Produkte der SF-Serie enthält.

Schritte

1. Klicken Sie auf **Cluster > SNMP**.
2. Klicken Sie unter **SNMP MIBs** auf die MIB-Datei, die Sie herunterladen möchten.
3. Im sich öffnenden Download-Fenster können Sie die MIB-Datei öffnen oder speichern.

Laufwerke verwalten

Jeder Knoten enthält ein oder mehrere physische Laufwerke, die zur Speicherung eines Teils der Daten des Clusters verwendet werden. Der Cluster nutzt die Kapazität und Leistung des Laufwerks, nachdem das Laufwerk erfolgreich in den Cluster integriert wurde. Sie können die Element-Benutzeroberfläche zur Verwaltung von Laufwerken verwenden.

Laufwerksdetails

Die Seite „Laufwerke“ auf der Registerkarte „Cluster“ bietet eine Liste der aktiven Laufwerke im Cluster. Sie können die Seite filtern, indem Sie eine der Registerkarten „Aktiv“, „Verfügbar“, „Entfernen“, „Löschen“ oder „Fehlgeschlagen“ auswählen.

Bei der ersten Initialisierung eines Clusters ist die Liste der aktiven Laufwerke leer. Sie können Laufwerke hinzufügen, die keinem Cluster zugewiesen sind und auf der Registerkarte „Verfügbar“ aufgeführt werden, nachdem ein neuer SolidFire -Cluster erstellt wurde.

Die folgenden Elemente werden in der Liste der aktiven Laufwerke angezeigt.

- **Laufwerks-ID**

Die dem Laufwerk zugewiesene fortlaufende Nummer.

- **Knoten-ID**

Die Knotennummer, die beim Hinzufügen des Knotens zum Cluster vergeben wird.

- **Knotename**

Der Name des Knotens, der das Laufwerk beherbergt.

- **Slot**

Die Steckplatznummer, an der sich das Laufwerk physisch befindet.

- **Kapazität**

Die Größe des Laufwerks in GB.

- **Seriennummer**

Die Seriennummer des Laufwerks.

- **Verbleibender Verschleiß**

Die Verschleißzustandsanzeige.

Das Speichersystem meldet den ungefähren Verschleißgrad, der auf jedem Solid-State-Drive (SSD) zum Schreiben und Löschen von Daten noch verfügbar ist. Ein Laufwerk, das 5 Prozent seiner vorgesehenen Schreib- und Löschzyklen verbraucht hat, weist noch einen Restverschleiß von 95 Prozent auf. Das System aktualisiert die Informationen zum Laufwerksverschleiß nicht automatisch; Sie können die Seite aktualisieren oder schließen und neu laden, um die Informationen zu aktualisieren.

- **Typ**

Die Art des Laufwerks. Der Typ kann entweder Block oder Metadaten sein.

Weitere Informationen

- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Knoten verwalten

Knoten verwalten

Sie können SolidFire -Speicher und Fibre-Channel-Knoten über die Seite „Knoten“ im Cluster-Tab verwalten.

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 zusätzlicher Speicherplatz 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.

Weitere Informationen

[Füge einem Cluster einen Knoten hinzu.](#)

Füge einem Cluster einen Knoten hinzu.

Sie können einem Cluster Knoten hinzufügen, wenn mehr Speicherplatz benötigt wird oder nachdem der Cluster bereits erstellt wurde. Die Knoten müssen bei der ersten Inbetriebnahme initial konfiguriert werden. Nach der Konfiguration des Knotens erscheint er in der Liste der ausstehenden Knoten und kann einem Cluster hinzugefügt werden.

Die Softwareversionen auf den einzelnen Knoten eines Clusters müssen kompatibel sein. Wenn Sie einem Cluster einen Knoten hinzufügen, installiert der Cluster bei Bedarf die Clusterversion der NetApp Element -Software auf dem neuen Knoten.

Sie können einem bestehenden Cluster Knoten mit kleinerer oder größerer Kapazität hinzufügen. Sie können einem Cluster größere Knotenkapazitäten hinzufügen, um ein Kapazitätswachstum zu ermöglichen. Größere Knoten, die einem Cluster mit kleineren Knoten hinzugefügt werden, müssen paarweise hinzugefügt werden. Dadurch bleibt genügend Platz für Double Helix, um die Daten zu verschieben, falls einer der größeren Knoten ausfällt. Sie können kleinere Knotenkapazitäten zu einem größeren Knotencluster hinzufügen, um die Leistung zu verbessern.



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 zusätzlicher Speicherplatz 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 der Clusterfehler strandedCapacity ausgelöst.

["NetApp Video: Skalierung nach Ihren Wünschen: Erweiterung eines SolidFire Clusters"](#)

Sie können Knoten zu NetApp HCI Appliances hinzufügen.

Schritte

1. Wählen Sie **Cluster > Knoten**.
2. Klicken Sie auf **Ausstehend**, um die Liste der ausstehenden Knoten anzuzeigen.

Sobald der Vorgang zum Hinzufügen von Knoten abgeschlossen ist, erscheinen diese in der Liste der aktiven Knoten. Bis dahin werden die ausstehenden Knoten in der Liste „Ausstehende Aktive“ angezeigt.

SolidFire installiert die Element-Softwareversion des Clusters auf den ausstehenden Knoten, wenn Sie diese einem Cluster hinzufügen. Dies kann einige Minuten dauern.

3. Führen Sie einen der folgenden Schritte aus:
 - Um einzelne Knoten hinzuzufügen, klicken Sie auf das **Aktionen**-Symbol des Knotens, den Sie hinzufügen möchten.
 - Um mehrere Knoten hinzuzufügen, wählen Sie die Kontrollkästchen der hinzuzufügenden Knoten aus und klicken Sie dann auf **Massenaktionen**. **Hinweis:** Falls auf dem hinzuzufügenden Knoten eine andere Version der Element-Software installiert ist als die auf dem Cluster laufende Version, aktualisiert der Cluster den Knoten asynchron auf die auf dem Cluster-Master laufende Version der Element-Software. Nach der Aktualisierung des Knotens fügt er sich automatisch dem Cluster hinzu. Während dieses asynchronen Prozesses befindet sich der Knoten im Zustand pendingActive.
4. Klicken Sie auf **Hinzufügen**.

Der Knoten erscheint in der Liste der aktiven Knoten.

Weitere Informationen

[Node-Versionierung und Kompatibilität](#)

Node-Versionierung und Kompatibilität

Die Knotenkompatibilität basiert auf der auf dem Knoten installierten Element-Softwareversion. Bei softwarebasierten Speicherclustern von Element wird ein Knoten automatisch auf die Element-Softwareversion im Cluster abgebildet, wenn Knoten und Cluster nicht kompatible Versionen aufweisen.

Die folgende Liste beschreibt die Bedeutungsstufen der Software-Releases, aus denen sich die Software-Versionsnummer von Element zusammensetzt:

- **Wesentlich**

Die erste Zahl bezeichnet eine Softwareversion. Ein Knoten mit einer bestimmten Hauptkomponentennummer kann nicht zu einem Cluster hinzugefügt werden, der Knoten mit einer anderen Hauptpatchnummer enthält. Ebenso wenig kann ein Cluster mit Knoten unterschiedlicher Hauptversionen erstellt werden.

- **Unerheblich**

Die zweite Zahl kennzeichnet kleinere Softwarefunktionen oder Erweiterungen bestehender Softwarefunktionen, die in einer Hauptversion hinzugefügt wurden. Diese Komponente wird innerhalb einer Hauptversionskomponente inkrementiert, um anzuzeigen, dass diese inkrementelle Version nicht mit anderen inkrementellen Softwareversionen von Element mit einer anderen Nebenkomponente kompatibel ist. Beispielsweise ist Version 11.0 nicht mit Version 11.1 kompatibel, und Version 11.1 ist nicht mit Version 11.2 kompatibel.

- **Mikro**

Die dritte Zahl kennzeichnet einen kompatiblen Patch (inkrementelle Version) für die Element-Softwareversion, die durch die Komponenten major.minor repräsentiert wird. Beispielsweise ist Version 11.0.1 mit Version 11.0.2 kompatibel, und Version 11.0.2 ist mit Version 11.0.3 kompatibel.

Die Haupt- und Nebenversionsnummern müssen für die Kompatibilität übereinstimmen. Die Mikronummern müssen für die Kompatibilität nicht übereinstimmen.

Clusterkapazität in einer gemischten Knotenumgebung

In einem Cluster können verschiedene Knotentypen gemischt werden. Die SF-Serie 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 und die H-Serie können in einem Cluster koexistieren.

Die H-Serie besteht aus den Knoten H610S-1, H610S-2, H610S-4 und H410S. Diese Knoten sind sowohl 10GbE- als auch 25GbE-fähig.

Es empfiehlt sich, unverschlüsselte und verschlüsselte Knoten nicht zu vermischen. In einem gemischten Knotencluster darf kein Knoten größer als 33 Prozent der gesamten Clusterkapazität sein. In einem Cluster mit vier SF-Series 4805-Knoten ist beispielsweise der größte Knoten, der einzeln hinzugefügt werden kann, ein SF-Series 9605. Die Clusterkapazitätsschwelle wird auf Basis des potenziellen Ausfalls des größten Knotens in dieser Situation berechnet.

Je nach Ihrer Element-Softwareversion werden die folgenden Speicherknoten der SF-Serie nicht unterstützt:

Beginnend mit...	Speicherknoten wird nicht unterstützt...
Element 12.8	<ul style="list-style-type: none">• SF4805• SF9605• SF19210• SF38410

Beginnend mit...	Speicherknoten wird nicht unterstützt...
Element 12.7	<ul style="list-style-type: none"> • SF2405 • SF9608
Element 12.0	<ul style="list-style-type: none"> • SF3010 • SF6010 • SF9010

Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Element-Version zu aktualisieren, wird eine Fehlermeldung angezeigt, die besagt, dass der Knoten von Element 12.x nicht unterstützt wird.

Knotendetails anzeigen

Sie können Details zu einzelnen Knoten anzeigen, wie z. B. Service-Tags, Laufwerksdetails und Grafiken zur Auslastung und Laufwerksstatistik. Auf der Seite „Knoten“ des Cluster-Tabs finden Sie die Spalte „Version“, in der Sie die Softwareversion jedes Knotens anzeigen können.

Schritte

1. Klicken Sie auf **Cluster > Knoten**.
2. Um die Details eines bestimmten Knotens anzuzeigen, klicken Sie auf das Symbol **Aktionen** für den Knoten.
3. Klicken Sie auf **Details anzeigen**.
4. Überprüfen Sie die Knotendetails:
 - **Knoten-ID**: Die vom System generierte ID für den Knoten.
 - **Knotenname**: Der Hostname des Knotens.
 - **Knotenrolle**: Die Rolle, die der Knoten im Cluster innehat. Mögliche Werte:
 - Cluster-Master: Der Knoten, der clusterweite administrative Aufgaben ausführt und den MVIP und SVIP enthält.
 - Ensemble-Knoten: Ein Knoten, der am Cluster teilnimmt. Je nach Clustergröße gibt es entweder 3 oder 5 Ensemble-Knoten.
 - Fibre Channel: Ein Knoten im Cluster.
 - **Knotentyp**: Der Modelltyp des Knotens.
 - **Aktive Laufwerke**: Die Anzahl der aktiven Laufwerke im Knoten.
 - **Knotenauslastung**: Der Prozentsatz der Knotenauslastung basierend auf nodeHeat. Der angezeigte Wert ist recentPrimaryTotalHeat als Prozentsatz. Verfügbar ab Element 12.8.
 - **Management IP**: Die Management-IP-Adresse (MIP), die dem Knoten für 1GbE- oder 10GbE-Netzwerkadministrationsaufgaben zugewiesen ist.
 - **Cluster-IP**: Die Cluster-IP-Adresse (CIP), die dem Knoten zugewiesen ist und für die Kommunikation zwischen Knoten im selben Cluster verwendet wird.
 - **Speicher-IP**: Die Speicher-IP-Adresse (SIP), die dem Knoten zugewiesen ist und für die iSCSI-Netzwerkerkennung und den gesamten Datennetzwerkverkehr verwendet wird.

- **Management VLAN ID:** Die virtuelle ID für das Management-LAN.
- **Storage VLAN ID:** Die virtuelle ID für das lokale Speichernetzwerk.
- **Version:** Die auf jedem Knoten laufende Softwareversion.
- **Replikationsport:** Der Port, der auf den Knoten für die Remote-Replikation verwendet wird.
- **Service Tag:** Die eindeutige Service-Tag-Nummer, die dem Knoten zugewiesen ist.
- **Benutzerdefinierte Schutzdomäne:** Die dem Knoten zugewiesene benutzerdefinierte Schutzdomäne.

Details zu Fibre-Channel-Anschlüsse anzeigen

Auf der Seite „FC-Ports“ können Sie Details zu Fibre-Channel-Ports wie Status, Name und Portadresse einsehen.

Informationen zu den Fibre Channel-Ports anzeigen, die mit dem Cluster verbunden sind.

Schritte

1. Klicken Sie auf **Cluster > FC-Ports**.
2. Um die Informationen auf dieser Seite zu filtern, klicken Sie auf **Filter**.
3. Überprüfen Sie die Details:
 - **Knoten-ID:** Der Knoten, der die Sitzung für die Verbindung hostet.
 - **Knotenname:** Vom System generierter Knotenname.
 - **Steckplatz:** Steckplatznummer, an der sich der Fibre Channel-Anschluss befindet.
 - **HBA-Anschluss:** Physischer Anschluss am Fibre Channel Host Bus Adapter (HBA).
 - **WWNN:** Der weltweite Knotenname.
 - **WWPN:** Der weltweite Zielhafenname.
 - **Switch WWN:** Weltweite Bezeichnung für den Fibre-Channel-Switch.
 - **Hafenstatus:** Aktueller Status des Hafens.
 - **nPort ID:** Die Knotenport-ID im Fibre Channel-Fabric.
 - **Geschwindigkeit:** Die ausgehandelte Fibre-Channel-Geschwindigkeit. Folgende Werte sind möglich:
 - 4Gbps
 - 8Gbps
 - 16Gbps

Weitere Informationen

- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Virtuelle Netzwerke verwalten

Virtuelle Netzwerke verwalten

Virtuelle Netzwerke in SolidFire -Speichern ermöglichen es, den Datenverkehr zwischen

mehreren Clients, die sich in separaten logischen Netzwerken befinden, mit einem Cluster zu verbinden. Die Verbindungen zum Cluster werden im Netzwerk-Stack durch VLAN-Tagging getrennt.

Weitere Informationen

- [Fügen Sie ein virtuelles Netzwerk hinzu](#)
- [Virtuelles Routing und Weiterleitung aktivieren](#)
- [Bearbeiten eines virtuellen Netzwerks](#)
- [VRF-VLANS bearbeiten](#)
- [Löschen eines virtuellen Netzwerks](#)

Fügen Sie ein virtuelles Netzwerk hinzu

Sie können einer Clusterkonfiguration ein neues virtuelles Netzwerk hinzufügen, um eine Multi-Tenant-Umgebungsverbindung zu einem Cluster zu ermöglichen, auf dem die Element-Software ausgeführt wird.

Was du brauchst

- Ermitteln Sie den IP-Adressblock, der den virtuellen Netzwerken auf den Clusterknoten zugewiesen werden soll.
- Identifizieren Sie eine Storage-Network-IP-Adresse (SVIP), die als Endpunkt für den gesamten NetApp Element Speicherdatenverkehr verwendet werden soll.



Bei dieser Konfiguration müssen Sie folgende Kriterien berücksichtigen:

- Bei VLANs ohne VRF-Unterstützung müssen sich die Initiatoren im selben Subnetz wie der SVIP befinden.
- Bei VRF-fähigen VLANs müssen sich die Initiatoren nicht im selben Subnetz wie der SVIP befinden, und Routing wird unterstützt.
- Der Standard-SVIP erfordert nicht, dass sich die Initiatoren im selben Subnetz wie der SVIP befinden, und Routing wird unterstützt.

Wenn ein virtuelles Netzwerk hinzugefügt wird, wird für jeden Knoten eine Schnittstelle erstellt, und jede benötigt eine virtuelle Netzwerk-IP-Adresse. Die Anzahl der IP-Adressen, die Sie beim Erstellen eines neuen virtuellen Netzwerks angeben, muss gleich oder größer als die Anzahl der Knoten im Cluster sein. Virtuelle Netzwerkadressen werden automatisch in großen Mengen bereitgestellt und einzelnen Knoten zugewiesen. Sie müssen den Knoten im Cluster keine virtuellen Netzwerkadressen manuell zuweisen.

Schritte

1. Klicken Sie auf **Cluster > Netzwerk**.
2. Klicken Sie auf **VLAN erstellen**.
3. Geben Sie im Dialogfeld **Neues VLAN erstellen** Werte in die folgenden Felder ein:
 - **VLAN-Name**
 - **VLAN-Tag**
 - **SVIP**
 - **Netzmaske**

- (Optional) **Beschreibung**

4. Geben Sie die **Start-IP-Adresse** für den IP-Adressbereich in **IP-Adressblöcken** ein.
5. Geben Sie die **Größe** des IP-Adressbereichs als Anzahl der in den Block aufzunehmenden IP-Adressen ein.
6. Klicken Sie auf **Block hinzufügen**, um einen nicht zusammenhängenden Block von IP-Adressen für dieses VLAN hinzuzufügen.
7. Klicken Sie auf **VLAN erstellen**.

Details zum virtuellen Netzwerk anzeigen

Schritte

1. Klicken Sie auf **Cluster > Netzwerk**.
2. Überprüfen Sie die Details.
 - **ID**: Eindeutige ID des VLAN-Netzwerks, die vom System zugewiesen wird.
 - **Name**: Eindeutiger, vom Benutzer vergebener Name für das VLAN-Netzwerk.
 - **VLAN-Tag**: VLAN-Tag, das bei der Erstellung des virtuellen Netzwerks zugewiesen wurde.
 - **SVIP**: Virtuelle Speicher-IP-Adresse, die dem virtuellen Netzwerk zugewiesen ist.
 - **Netzmaske**: Netzmaske für dieses virtuelle Netzwerk.
 - **Gateway**: Eindeutige IP-Adresse eines virtuellen Netzwerk-Gateways. VRF muss aktiviert sein.
 - **VRF aktiviert**: Gibt an, ob virtuelles Routing und Weiterleitung aktiviert ist oder nicht.
 - **Verwendete IP-Adressen**: Der Bereich der virtuellen Netzwerk-IP-Adressen, die für das virtuelle Netzwerk verwendet werden.

Virtuelles Routing und Weiterleitung aktivieren

Sie können Virtual Routing and Forwarding (VRF) aktivieren, wodurch mehrere Instanzen einer Routingtabelle in einem Router existieren und gleichzeitig funktionieren können. Diese Funktionalität ist nur für Speichernetzwerke verfügbar.

VRF kann nur beim Erstellen eines VLANs aktiviert werden. Wenn Sie wieder auf Nicht-VRF umstellen möchten, müssen Sie das VLAN löschen und neu erstellen.

1. Klicken Sie auf **Cluster > Netzwerk**.
2. Um VRF in einem neuen VLAN zu aktivieren, wählen Sie **VLAN erstellen**.
 - a. Geben Sie die relevanten Informationen für das neue VRF/VLAN ein. Siehe Hinzufügen eines virtuellen Netzwerks.
 - b. Aktivieren Sie das Kontrollkästchen **VRF aktivieren**.
 - c. **Optional**: Geben Sie ein Gateway ein.
3. Klicken Sie auf **VLAN erstellen**.

Weitere Informationen

[Fügen Sie ein virtuelles Netzwerk hinzu](#)

Bearbeiten eines virtuellen Netzwerks

Sie können VLAN-Attribute wie VLAN-Name, Netzmaske und Größe der IP-Adressblöcke ändern. Das VLAN-Tag und der SVIP können für ein VLAN nicht geändert werden. Das Gateway-Attribut ist kein gültiger Parameter für Nicht-VRF-VLANS.

Falls iSCSI-, Remote-Replikations- oder andere Netzwerk-Sitzungen bestehen, kann die Änderung fehlschlagen.

Bei der Verwaltung der Größe von VLAN-IP-Adressbereichen sollten Sie die folgenden Einschränkungen beachten:

- Sie können nur IP-Adressen aus dem ursprünglichen IP-Adressbereich entfernen, der Ihnen bei der Erstellung des VLAN zugewiesen wurde.
- Sie können einen IP-Adressblock entfernen, der nach dem ursprünglichen IP-Adressbereich hinzugefügt wurde, aber Sie können einen IP-Block nicht vergrößern, indem Sie IP-Adressen entfernen.
- Beim Versuch, IP-Adressen aus dem ursprünglichen IP-Adressbereich oder einem IP-Block zu entfernen, die von Knoten im Cluster verwendet werden, kann der Vorgang fehlschlagen.
- Bestimmte, bereits verwendete IP-Adressen können nicht anderen Knoten im Cluster neu zugewiesen werden.

Sie können einen IP-Adressbereich mit folgendem Verfahren hinzufügen:

1. Wählen Sie **Cluster > Netzwerk**.
2. Wählen Sie das Aktionssymbol für das VLAN aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VLAN ein.
5. Wählen Sie **Block hinzufügen**, um einen nicht zusammenhängenden Block von IP-Adressen für das virtuelle Netzwerk hinzuzufügen.
6. Wählen Sie **Änderungen speichern**.

Link zu den KB-Artikeln zur Fehlerbehebung

Hier finden Sie Artikel aus der Wissensdatenbank, die Ihnen bei der Fehlerbehebung im Zusammenhang mit der Verwaltung Ihrer VLAN-IP-Adressbereiche helfen.

- "[Warnung vor doppelter IP-Adresse nach dem Hinzufügen eines Speicherknotens in einem VLAN auf dem Element-Cluster](#)"
- "[Wie man in Element ermittelt, welche VLAN-IPs verwendet werden und welchen Knoten diese IPs zugewiesen sind.](#)"

VRF-VLANS bearbeiten

Sie können VRF-VLAN-Attribute wie VLAN-Name, Netzmaske, Gateway und IP-Adressbereiche ändern.

1. Klicken Sie auf **Cluster > Netzwerk**.
2. Klicken Sie auf das Aktionssymbol für das VLAN, das Sie bearbeiten möchten.
3. Klicken Sie auf **Bearbeiten**.

4. Geben Sie die neuen Attribute für das VRF-VLAN im Dialogfeld **VLAN bearbeiten** ein.
5. Klicken Sie auf **Änderungen speichern**.

Löschen eines virtuellen Netzwerks

Sie können ein virtuelles Netzwerkobjekt entfernen. Sie müssen die Adressblöcke einem anderen virtuellen Netzwerk hinzufügen, bevor Sie ein virtuelles Netzwerk entfernen.

1. Klicken Sie auf **Cluster > Netzwerk**.
2. Klicken Sie auf das Aktionssymbol für das VLAN, das Sie löschen möchten.
3. Klicken Sie auf **Löschen**.
4. Bestätigen Sie die Nachricht.

Weitere Informationen

[Bearbeiten eines virtuellen Netzwerks](#)

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.