Anforderungen

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/de-de/element-software-123/storage/concept_prereq_networking.html on November 19, 2025. Always check docs.netapp.com for the latest.

Inhalt

Anforderungen . . . 1
- Weitere Informationen . . . 1
- Netzwerkbetrieb . . . 1
  - Finden Sie weitere Informationen . . . 1
- Switch-Konfiguration für Cluster mit Element Software . . . 1
  - Finden Sie weitere Informationen . . . 3
- Anforderungen an Netzwerk-Ports . . . 3
  - Finden Sie weitere Informationen . . . 6

Anforderungen

Bevor Sie beginnen, sollten Sie die Voraussetzungen für die Bereitstellung der NetApp Element-Software, einschließlich Netzwerk- und Portanforderungen, prüfen.

- "Netzwerkanforderungen"
- "Switch-Konfiguration"
- "Anforderungen an Netzwerk-Ports"

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"

Netzwerkbetrieb

Das Netzwerk-Setup für ein SolidFire System besteht aus Switch- und Port-Anforderungen. Die Umsetzung davon hängt von Ihrem System ab.

Finden Sie weitere Informationen

- "Switch-Konfiguration für Cluster mit Element Software"
- "Anforderungen an Netzwerk-Ports"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Switch-Konfiguration für Cluster mit Element Software

Das NetApp Element Softwaresystem verfügt über bestimmte Switch-Anforderungen und Best Practices für eine optimale Storage-Performance.

Storage-Nodes benötigen je nach spezifischer Node-Hardware 10- oder 25-GbE-Ethernet-Switches für die Kommunikation von iSCSI-Storage-Services und zwischen Nodes innerhalb eines Clusters. 1GbE-Switches können für diese Arten von Datenverkehr verwendet werden:

- Management des Clusters und der Nodes
- Clusterinternen Managementdatenverkehr zwischen den Nodes
- Datenverkehr zwischen den Cluster-Knoten und der virtuellen Verwaltungsknoten

Best Practice: bei der Konfiguration von Ethernet-Switches für Cluster-Datenverkehr sollten Sie die folgenden Best Practices umsetzen:

- Für den Datenverkehr außerhalb des Storage-Systems im Cluster können Sie ein Paar 1-GbE-Switches implementieren, um Hochverfügbarkeit und Lastverteilung bereitzustellen.
- Auf den Storage-Netzwerk-Switches stellen Sie Switches paarweise bereit und konfigurieren und verwenden Jumbo Frames (eine MTU-Größe von 9216 Byte). So wird eine erfolgreiche Installation gewährleistet und Fehler im Speichernetzwerk aufgrund von fragmentierten Paketen vermieden.

Für die Elementbereitstellung sind mindestens zwei Netzwerksegmente erforderlich, eines für jeden der folgenden Verkehrstypen:

- Vereinfachtes
- Storage/Daten

Je nach den NetApp H-Series Storage-Node-Modellen und der geplanten Verkabelungskonfiguration können Sie diese Netzwerke mithilfe separater Switches physisch trennen oder sie über VLANs logisch trennen. Bei den meisten Implementierungen müssen diese Netzwerke jedoch durch VLANs logisch voneinander getrennt werden.

Storage-Nodes müssen vor, während und nach der Implementierung kommunizieren können.

Wenn Sie getrennte Managementnetzwerke für Storage-Nodes implementieren, stellen Sie sicher, dass diese Managementnetzwerke Netzwerkrouten zwischen ihnen haben. Diese Netzwerke müssen über Gateways verfügen, und es muss eine Route zwischen den Gateways vorhanden sein. Stellen Sie sicher, dass jedem neuen Node ein Gateway zugewiesen ist, um die Kommunikation zwischen den Nodes und Managementnetzwerken zu erleichtern.

Für NetApp Element ist Folgendes erforderlich:

- Alle mit NetApp H-Series Storage-Nodes verbundenen Switch-Ports müssen als Spanning Tree Edge Ports konfiguriert sein.
  - Bei Cisco Switches, je nach Switch-Modell, Softwareversion und Porttyp, können Sie dies mit einem der folgenden Befehle ausführen:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - Auf Mellanox-Switches kann dies mit dem durchgeführt werden `spanning-tree port type edge` Befehl.
- Die Switches, die Storage-Datenverkehr verarbeiten, müssen Geschwindigkeiten von mindestens 10 GbE pro Port unterstützen (bis zu 25 GbE pro Port wird unterstützt).
- Die Switches, die Managementdatenverkehr verarbeiten, müssen Geschwindigkeiten von mindestens 1 GbE pro Port unterstützen.
- Sie müssen Jumbo Frames an den Switch-Ports konfigurieren, die Storage Traffic verarbeiten. Für eine erfolgreiche Installation müssen Hosts 9000-Byte-Pakete lückenlos versenden können.
- Die Netzwerklatenz zwischen allen Storage-Nodes sollte 2 ms nicht überschreiten.

Einige Nodes bieten zusätzliche Out-of-Band-Managementfunktionen über einen dedizierten Management-Port. NetApp H300S, H500S und H700S Nodes ermöglichen auch IPMI-Zugriff über Port A Als Best Practice wird empfohlen, das Remote-Management durch die Konfiguration von Out-of-Band-Management für alle Nodes in Ihrer Umgebung zu vereinfachen.

Finden Sie weitere Informationen

- "Netzwerk- und Switch-Anforderungen des NetApp HCI"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Anforderungen an Netzwerk-Ports

Möglicherweise müssen Sie die folgenden TCP- und UDP-Ports über die Edge-Firewall Ihres Rechenzentrums zulassen, damit Sie das System Remote verwalten und Clients außerhalb Ihres Rechenzentrums die Verbindung zu Ressourcen ermöglichen können. Einige dieser Ports sind je nach Nutzung des Systems möglicherweise nicht erforderlich.

Alle Ports sind TCP, sofern nicht anders angegeben, und alle TCP-Ports müssen die Dreiwege-Handshake-Kommunikation zwischen dem NetApp-Supportserver, dem Verwaltungsknoten und den Knoten unterstützen, auf denen die Element-Software ausgeführt wird. Beispielsweise kommuniziert der Host auf einem Management-Knoten über TCP-Port 443 mit dem Host auf einem Speicher-Cluster-MVIP-Ziel, und der Ziel-Host kommuniziert über einen beliebigen Port zurück zum Quellhost.

Aktivieren Sie ICMP zwischen dem Managementknoten, Knoten mit Element Software und Cluster MVIP.

Die folgenden Abkürzungen werden in der Tabelle verwendet:

- MIP: Management-IP-Adresse, eine Adresse pro Node
- SIP: Speicher-IP-Adresse, eine Adresse pro Knoten
- MVIP: Management der virtuellen IP-Adresse
- SVIP: Virtuelle Speicher-IP-Adresse

Quelle	Ziel	Port	Beschreibung
ISCSI-Clients	Storage Cluster MVIP	443	(Optional) UI- und API-Zugriff
ISCSI-Clients	Storage Cluster SVIP	3260	ISCSI-Kommunikation des Clients
ISCSI-Clients	Speicherknoten SIP	3260	ISCSI-Kommunikation des Clients
Management-Node	`sfsupport.solidfire.com`	22	Reverse-SSH-Tunnel für den Support-Zugriff
Management-Node	MIP-Speicher-Node	22	SSH-Zugriff für die Unterstützung

Quelle	Ziel	Port	Beschreibung
Management-Node	DNS-Server	53 TCP/UDP	DNS-Suche
Management-Node	MIP-Speicher-Node	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	Storage Cluster MVIP	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	`monitoring.solidfire.com`	443	Berichterstellung für den Storage-Cluster an Active IQ
Management-Node	Storage Cluster MVIP	443	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	repo.netapp.com	443	Zugriff auf Komponenten, die für die Installation/Aktualisierung einer On-Premises-Implementierung erforderlich sind
Management-Node	BMC/IPMI für Storage-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
Management-Node	Witness Node	9442	Konfigurations-API-Service pro Node
Management-Node	VCenter Server	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.
SNMP-Server	Storage Cluster MVIP	161 UDP	SNMP-Abfrage
SNMP-Server	MIP-Speicher-Node	161 UDP	SNMP-Abfrage
BMC/IPMI für Storage-Node	Management-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
MIP-Speicher-Node	DNS-Server	53 TCP/UDP	DNS-Suche
MIP-Speicher-Node	Management-Node	80	Upgrades für Element Software
MIP-Speicher-Node	S3/Swift-Endpunkt	80	(Optional) HTTP-Kommunikation mit S3/Swift-Endpunkt für Backup und Recovery
MIP-Speicher-Node	NTP-Server	123 UDP	NTP

Quelle	Ziel	Port	Beschreibung
MIP-Speicher-Node	Management-Node	162 UDP	(Optional) SNMP-Traps
MIP-Speicher-Node	SNMP-Server	162 UDP	(Optional) SNMP-Traps
MIP-Speicher-Node	LDAP-Server	389 TCP/UDP	(Optional) LDAP-Suche
MIP-Speicher-Node	Management-Node	443	Upgrades der Element Storage-Firmware
MIP-Speicher-Node	Remote Storage Cluster MVIP	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
MIP-Speicher-Node	MIP für Remote-Storage-Node	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
MIP-Speicher-Node	S3/Swift-Endpunkt	443	(Optional) HTTPS-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery
MIP-Speicher-Node	Management-Node	514 TCP/UDP 10514 TCP/UDP	Syslog-Weiterleitung
MIP-Speicher-Node	Syslog-Server	514 TCP/UDP 10514 TCP/UDP	Syslog-Weiterleitung
MIP-Speicher-Node	LDAPS Server	636 TCP/UDP	LDAPS-Suche
MIP-Speicher-Node	MIP für Remote-Storage-Node	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung
Speicherknoten SIP	Remote-Speicherknoten SIP	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung
Speicherknoten SIP	Speicherknoten SIP	3260	ISCSI miteinander verbinden
Speicherknoten SIP	Remote-Speicherknoten SIP	4000 bis 4020	Remote-Replizierung: Node-to-Node-Datentransfer
System Administrator-PC	Management-Node	442	HTTPS-UI-Zugriff auf den Management-Node

Quelle	Ziel	Port	Beschreibung
System Administrator-PC	MIP-Speicher-Node	442	HTTPS-UI- und API-Zugriff auf Storage-Node
System Administrator-PC	Management-Node	443	HTTPS-UI- und API-Zugriff auf den Management-Node
System Administrator-PC	Storage Cluster MVIP	443	HTTPS-UI- und API-Zugriff auf das Storage-Cluster
System Administrator-PC	Storage Node Baseboard Management Controller (BMC)/Intelligent Platform Management Interface (IPMI) H410 und H600 Serien	443	HTTPS-UI- und API-Zugriff auf die Remote-Steuerung des Nodes
System Administrator-PC	MIP-Speicher-Node	443	Erstellung von HTTPS-Storage-Clustern, UI-Zugriff nach der Implementierung auf das Storage-Cluster
System Administrator-PC	Storage Node BMC/IPMI H410 und H600 Series	623 UDP	Remote Management Control Protocol-Port: Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
System Administrator-PC	Witness Node	8080	Witness Node pro Node Web-UI
VCenter Server	Storage Cluster MVIP	443	VCenter-Plug-in-API-Zugriff
VCenter Server	Remote-Plug-in	8333	Remote vCenter Plug-in Service
VCenter Server	Management-Node	8443	(Optional) vCenter Plug-in QoSSIOC-Service.
VCenter Server	Storage Cluster MVIP	8444	Zugriff auf vCenter VASA Provider (nur VVols)
VCenter Server	Management-Node	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.

Finden Sie weitere Informationen

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

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 VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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