Dell PowerStore

Planungshandbuch

Version 4.x

Februar 2025
Rev. A12

DELL Technologies

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Inhaltsverzeichnis

Vorwort

Es werden regelmäßig neue Software- und Hardwareversionen veröffentlicht, um das Produkt kontinuierlich zu verbessern. Einige in diesem Dokument beschriebene Funktionen werden eventuell nicht von allen Versionen der von Ihnen derzeit verwendeten Software oder Hardware unterstützt. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu Produktfunktionen. Wenden Sie sich an Ihren Serviceanbieter, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

ANMERKUNG: Kunden mit PowerStore X-Modell: Die aktuellen technischen Handbücher und Leitfäden für Ihr Modell finden Sie in der *PowerStore 3.2.x-Dokumentation*, die Sie von der PowerStore-Dokumentationsseite dell.com/powerstoredocs herunterladen können.

Hier erhalten Sie Hilfe

Auf Support, Produkt- und Lizenzierungsinformationen kann wie folgt zugegriffen werden:

- **Produktinformationen**: Dokumentation oder Versionshinweise zum Produkt und den Funktionen finden Sie auf der PowerStore-Dokumentationsseite dell.com/powerstoredocs.
- **Troubleshooting**: Informationen zu Produkten, Softwareupdates, Lizenzierung und Service finden Sie auf Dell Support auf der entsprechenden Produktsupportseite.
- **Technischer Support**: Für technischen Support und Service-Requests gehen Sie zu Dell Support und rufen die Seite **Service-Requests** auf. Um einen Service-Request stellen zu können, müssen Sie über eine gültige Supportvereinbarung verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie einen gültigen Supportvertrag benötigen oder Fragen zu Ihrem Konto haben.

1

Einleitung

Verwenden Sie dieses Dokument, um den Installationsprozess besser zu verstehen und ihren Standort und Ihre Workstation auf eine erfolgreiche Implementierung von PowerStore vorzubereiten. In diesem Kapitel werden folgende Themen behandelt:

Themen:

Einführung in PowerStore

PowerStore erreicht ein neues Niveau an operativer Einfachheit und Agilität. Mithilfe einer containerbasierten Microservices-Architektur, fortschrittlichen Storage-Technologien und integriertem maschinellen Lernen kann die volle Leistungsfähigkeit Ihrer Daten ausgeschöpft werden. PowerStore ist eine vielseitige Plattform mit einem leistungsorientierten Design, die mehrdimensionale Skalierung, ständige Datenreduzierung und Unterstützung für Datenträger der nächsten Generation bietet.

PowerStore bringt die Einfachheit der Public Cloud in die On-Premise-Infrastruktur, rationalisiert den Betrieb mit einer integrierten Engine für maschinelles Lernen und nahtloser Automatisierung und bietet gleichzeitig vorausschauende Analysen zur Überwachung, Analyse und Fehlerbehebung der Umgebung. PowerStore ist äußerst anpassungsfähig und so flexibel, dass spezielle Workloads direkt auf der Appliance gehostet und die Infrastruktur ohne Unterbrechung modernisiert werden kann. Ihre Investitionen werden geschützt durch flexible Zahlungsoptionen und DIP-Upgrades.

Die PowerStore T-Modell und PowerStore Q-Modell Appliances sind Storage-zentriert und ermöglichen das Management und die Bereitstellung von Block- und Datei-Storage auf externen Hosts. Während der Erstkonfiguration können Sie eine Appliance für vereinten Storage (Block und Datei) oder für blockoptimierten Storage (nur Block) konfigurieren.

Die Appliances des Modells PowerStore Q sind mit Quad-Level-Cell (QLC)-SSDs mit hoher Kapazität bestückt. Die unterstützten QLC-SSDs haben geringere Kosten pro Gigabyte als die TLC-SSDs (Triple-Level Cell), die in PowerStore T-Modell-Appliances verwendet werden.

Appliances

Eine PowerStore-Appliance ist eine vorkonfigurierte Infrastrukturkomponente mit Speicher- und Rechenressourcen. Eine Appliance besteht aus:

- Basisgehäuse – Bietet Platz für bis zu 25 Laufwerke (mindestens sechs Laufwerke) und umfasst zwei Nodes für hohe Verfügbarkeit mit Data Protection, die auf allen Nodes implementiert ist.
- Erweiterungsgehäuse – Ermöglicht das Hinzufügen weiterer Laufwerke und die Steigerung der Storage-Kapazität für die Appliance. Sie können bis zu drei Erweiterungsgehäuse hinzufügen.
  - PowerStore 500T unterstützt NVMe-Erweiterungsgehäuse.
  - Alle anderen PowerStore-Modelle unterstützen NVMe-Erweiterungsgehäuse oder SAS-Erweiterungsgehäuse.

ANMERKUNG: NVMe-Erweiterungsgehäuses und SAS-Erweiterungsgehäuses in derselben Appliance können nicht kombiniert werden.

Gehen Sie zu **Hardware** > **Appliances**, um die Gesamtintegrität der Appliances im Cluster zu überprüfen und Supportmaterialien zum Troubleshooting für die Appliances zu sammeln.

Klicken Sie auf den Namen der Appliance, um die Seite **Appliance-Details** zu starten, auf der Sie die Kennzahlen, Warnmeldungen und Integritätsinformationen der Appliance und ihrer Komponenten prüfen können. Verwenden Sie die **Weitere Aktionen**-Optionen auf der Detailseite, um Supportmaterialien für die Appliance zu sammeln und kleinere Probleme zu lösen.

PowerStore-Cluster

Ein PowerStore-Cluster ist eine Gruppe von einer bis vier Appliances, die als zentrale Komponente für Ressourcenmanagement, Effizienz und Verfügbarkeit fungiert. Ein Cluster kann bis zu vier Appliances enthalten. In dieser Version können nur Appliances derselben Konfiguration in einem Cluster vorhanden sein.

In der folgenden Abbildung werden die Komponenten eines Clusters dargestellt:

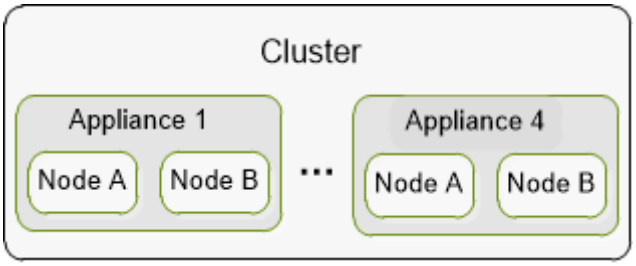

Abbildung 1. Clusterkomponenten

Ein Cluster bietet folgende Vorteile:

- Geringere Managementkomplexität
- Verbesserte Performance und Ressourceneffizienz: Compute- und Storage-Ressourcen werden in einem Cluster zusammengefasst und die Ressourcennutzung wird über die Appliances im Cluster ausgeglichen. Ressourcen werden neu ausgeglichen, um die Performance und Ressourcennutzung auf dem Cluster aufrechtzuerhalten und zu optimieren. Der Neuabgleich erfolgt basierend auf den Trends bei der Speicherplatznutzung und den Systemperformancebewertungen, die im Back-End stattfinden.
- Skalierbarkeit: Starten Sie mit einer kleinen Konfiguration und erweitern Sie das System später auf mehrere Appliances, um die Kapazität oder Performance zu steigern und die geschäftliche Nachfrage zu decken.

Um ein Cluster zu managen und zu konfigurieren, sind folgende Vorgänge nötig im PowerStore Manager:

- Überwachen und überprüfen Sie die aggregierten Kennzahlen für das Cluster auf der Seite **Dashboard**.
- Überprüfen und konfigurieren Sie die verschiedenen Einstellungen für das Cluster auf der Seite **Settings**.
- Fügen Sie Appliances zum Cluster hinzu oder entfernen Sie sie auf der Seite **Hardware**.

Planungs- und Installationsübersicht

Dieser Abschnitt enthält eine allgemeine Übersicht über die Schritte, die Sie von der Planung über die Installation bis hin zur Anmeldung bei der PowerStore Manager-Benutzeroberfläche planen sollten.

Bevor die Appliance eintrifft:

1. Führen Sie in Zusammenarbeit mit Ihren Infrastrukturadministratoren folgende Schritte durch:
   a. Konfigurieren Sie Ihren Netzwerk- und Managementswitch basierend auf den Empfehlungen im *PowerStore-Netzwerkleitfaden für die erstmalige Bereitstellung*.
   b. Erfassen Sie die netzwerkbezogenen Informationen, die Sie für die Erstkonfiguration des Clusters benötigen. Verwenden Sie das *PowerStore-Netzwerkleitfaden für die erstmalige Bereitstellung*, um diese Informationen zu erfassen und dann damit zu planen.
   c. Konfigurieren Sie die Netzwerkports, damit der Cluster sicher und effizient mit relevanten Hosts und Anwendungen kommunizieren kann. Weitere Informationen finden Sie unter Portnutzung.
2. PowerStore erfordert ein Rechenzentrum oder einen Serverraum, der mit gesteuerten elektrischen, Umgebungs-, Verkabelungs- und Sicherheitssystemen ausgestattet ist. Planen Sie den Standort, an dem die Appliances installiert werden sollen, sowie den Standort der Appliance-Komponenten (Basisgehäuse und Erweiterungsgehäuse) in einem Rack. Weitere Informationen finden Sie unter Standortplanung.
3. Richten Sie eine Workstation ein, mit der Sie die Appliances ermitteln und das Cluster konfigurieren können.
4. Bestimmen Sie die Toleranzstufe für Laufwerksfehler, die Sie auf den einzelnen Appliances festlegen möchten. Die Fehlertoleranzstufe für Laufwerke gibt die Anzahl der gleichzeitigen Laufwerksausfälle an, die die Appliance verkraften kann, ohne dass es zu einer Nichtverfügbarkeit von Daten oder Datenverlust kommt. Die Fehlertoleranzstufe für ein einzelnes Laufwerk erfüllt die Verfügbarkeitsanforderungen für alle Laufwerkstypen und Kapazitätspunkte, die Fehlertoleranzstufe für doppelte Laufwerke kann jedoch höhere Ausfallsicherheit und höheren Schutz bieten. Sie können die Fehlertoleranzstufe des Laufwerks nicht ändern, nachdem Sie sie festgelegt haben. Stellen Sie sicher, dass das Gehäuse die folgende Anzahl von SSD-Festplatten umfasst:

- Mindestens sechs Laufwerke für die Fehlertoleranz einzelner Laufwerke
- Sieben Laufwerke für die Fehlertoleranz doppelter Laufwerke

Wenn die Appliance eintrifft:

Lesen Sie den *PowerStore – Quick-Start-Handbuch* um:

1. Ihre Appliance (Basisgehäuse und Erweiterungsgehäuse) auszupacken und zu installieren
2. Die Gehäuse an das Netzwerk anzubinden und hochzufahren
3. Die Erstkonfiguration zu starten Weitere Informationen finden Sie im *PowerStore-Netzwerkleitfaden für die erstmalige Bereitstellung*.

Auch der *PowerStore – Installations- und Servicehandbuch* enthält Installationsanleitungen zum späteren Nachschlagen.

ANMERKUNG: Es wird empfohlen, entweder während der Erstkonfiguration oder nach der Anmeldung bei PowerStore Manager die Supportkonnektivität-Funktion zu aktivieren, um die Problemdiagnose zu beschleunigen, Troubleshooting durchzuführen und das Problem schneller zu beheben. Weitere Informationen finden Sie unter Supportkonnektivität.

Nach der Erstkonfiguration:

1. Melden Sie sich mit den Administratorzugangsdaten, die Sie während der Erstkonfiguration eingerichtet haben, beim PowerStore Manager an.
2. Konfigurieren Sie die Einstellungen für den Cluster und starten Sie die Bereitstellung von PowerStore Manager-Nutzerkonten, Storage-Ressourcen und Policies. Weitere Informationen zu den empfohlenen Schritten, wenn Sie sich zum ersten Mal beim PowerStore Manager anmelden, finden Sie im *PowerStore – Handbuch für die Einrichtung von PowerStore Manager*.

2

Standortplanung

Dieses Kapitel umfasst folgende Themen:

Themen:

Leitlinien für die Platzierung im Rack

Berücksichtigen Sie bei der Planung der Platzierung der Appliance-Komponenten die folgenden Leitlinien:

- Lassen Sie an der Unterseite des Racks 2 HE Platz für Wartung und die Netzkabelführung.
- Setzen Sie das Basisgehäuse ohne Erweiterungsgehäuse von unten beginnend bei der 3HE-Markierung ein.
- Setzen Sie die Basisgehäuse in der Reihenfolge von den Erweiterungsgehäuse mit den geringsten Verbindungen bis zu denen mit den meisten Verbindungen und dann in der Reihenfolge von den meisten Laufwerken bis zu den wenigsten nacheinander ein.
- Setzen Sie das Erweiterungsgehäuse, das mit dem ersten Basisgehäuse verbunden ist, direkt über dem Basisgehäuse ein.
- Die folgenden Basisgehäuse werden in umgekehrter Reihenfolge eingesetzt.

Weitere Informationen zu einem Beispiel für einen Rack-Platzplan finden Sie unter Arbeitsblätter für die Rackplatzplanung. Verwenden Sie dann das leere Arbeitsblatt, um die Appliances in Ihrem Cluster zu planen.

Technische Daten

Überprüfen Sie die technischen Daten zur Planung und Vorbereitung des Standorts, an dem Sie den PowerStore-Cluster installieren.

Abmessungen und Gewicht des Basisgehäuses

Tabelle 1. Abmessungen und Gewicht des Basisgehäuses

Abmessung	Wert
Gewicht (vollständig bestückt)	41,7 kg (92 lbs)
Vertikale Größe	2 NEMA-Einheiten
Höhe	8,64 cm (3,4")
Breite	44,45 cm (17,5")
Tiefe	79,5 cm (31,3")

Abmessungen und Gewicht des PowerStore 500T

Tabelle 2. Abmessungen und Gewicht des Basisgehäuses

Abmessung	Wert
Gewicht (vollständig bestückt)	37,4 kg
Vertikale Größe	2 NEMA-Einheiten
Höhe	8,64 cm (3,4")
Breite	44,45 cm (17,5")

Tabelle 2. Abmessungen und Gewicht des Basisgehäuses (fortgesetzt)

Abmessung	Wert
Tiefe	79,5 cm (31,3")

ANMERKUNG: Bei dieser Gewichtsangabe sind die Montageschienen nicht berücksichtigt. Rechnen Sie 3,6 kg (8 lbs) für einen Satz Schienen ein.

Abmessungen und Gewicht des SAS-Erweiterungsgehäuses

Tabelle 3. Abmessungen und Gewicht des SAS-Erweiterungsgehäuses

Abmessung	Wert
Gewicht (vollständig bestückt)	34,98 kg (77,11 lb)
Vertikale Größe	2 NEMA-Einheiten
Höhe	8,64 cm (3,4")
Breite	44,45 cm (17,5")
Tiefe	34,29 cm (13,5")

Abmessungen und Gewicht des NVMe-Erweiterungsgehäuses

Tabelle 4. Abmessungen und Gewicht des NVMe-Erweiterungsgehäuses

Abmessung	Wert
Gewicht (vollständig bestückt)	26,08 kg (ohne Kabelführungsarme oder Montageschienen)
Vertikale Größe	2 NEMA-Einheiten
Höhe	8,89 cm
Breite	43,18 cm
Tiefe	65,30cm (25,71")
Tiefe mit Kabelführungsarmen	84,86 cm

Stromversorgungsanforderungen des Basisgehäuses

Die Anforderungen an die Stromversorgung hängen ab von der Systemkonfiguration, dem Laden und den Umgebungsbedingungen. Die folgende Tabelle beschreibt die maximal zu erwartende Leistungsaufnahme. Um die Stromverbrauchswerte für Ihre spezifische Umgebung zu schätzen, verwenden Sie den Dell Power Calculator.

Tabelle 5. Anforderungen an die Stromversorgung für x000-Modelle

Voraussetzung	1000T	3000T	5000T	7000T	9000T
Maximale Eingangsleistung	240 VAC ± 10 %, einphasig Für 100 bis 120 V ist ein vom Kunden bereitgestellter Aufwärtstransformator erforderlich.				
Wechselstrom (maximaler Betrieb bei 200 VAC)	6,7 A	8,1 A	9,0 A	9,3 A	10,4 A
Stromverbrauch (maximaler Betrieb bei 200 VAC)	1385 VA (1316 W)	1629,6 VA (1597 W)	1792,9 VA (1757 W)	1868,4 VA (1831 W)	2088,8 VA (2047 W)
Wärmeabgabe (maximaler Betrieb)	4,37 x 10^6 J/h (4.490 BTU/h)	5,74 x 10^6 J/h (5.449 BTU/h)	6,32 x 10^6 J/h (5.995 BTU/h)	6,59 x 10^6 J/h (6.248 BTU/h)	7,37 x 10^6 J/h (6.985 BTU/h)
Stromanschlusstyp	Gerätestecker IEC320-C14 oder IEC320-C20 je Netzteil			Gerätestecker IEC320-C20 je Netzteil	
Normale Eingangsfrequenz	47 Hz – 63 Hz				
Maximaler Einschaltstrom	45 Apk „kalter“ Spitzenstrom pro Kabel bei beliebiger Spannung				
Netzsicherung	20-A-Sicherung je Netzteil, einpolig				
Überbrückung bei Stromausfall	min. 10 ms				
Stromverteilung	±5 % der Volllast zwischen Netzteilen				
Einschaltspitzenstrom	120 Apk „heißer“ Spitzenstrom pro Kabel bei beliebiger Spannung				

Tabelle 6. Anforderungen an die Stromversorgung für x200-Modelle

Voraussetzung	1200T	3200T	3200Q	5200T	9200T
Maximale Eingangsleistung	240 VAC ± 10 %, einphasig Für 100 bis 120 V ist ein vom Kunden bereitgestellter Aufwärtstransformator erforderlich.				
Wechselstrom (maximaler Betrieb bei 200 VAC)	6,5 A	7,1 A	7,7 A	8,8 A	9,8 A
Stromverbrauch (maximaler Betrieb bei 200 VAC)	1297,2 VA (1271,3 W)	1422 VA (1393,6 W)	1535,8 VA (1505,1 W)	1769,8 VA (1734,4 W)	1958,6 VA (1919,4 W)
Wärmeabgabe (maximaler Betrieb)	4,58 x 10^6 J/h (4.338 BTU/h)	5,02 x 10^6 J/h (4.755 BTU/h)	5,42 x 10^6 J/h (5.136 BTU/h)	6,24 x 10^6 J/h (5.918 BTU/h)	6,91 x 10^6 J/h (6.549 BTU/h)
Stromanschlusstyp	Gerätestecker IEC320-C14 oder IEC320-C20 je Netzteil				Gerätestecker IEC320-C20 je Netzteil
Normale Eingangsfrequenz	47 Hz – 63 Hz				

Tabelle 6. Anforderungen an die Stromversorgung für x200-Modelle (fortgesetzt)

Voraussetzung	1200T	3200T	3200Q	5200T	9200T
Maximaler Einschaltstrom	45 Apk „kalter“ Spitzenstrom pro Kabel bei beliebiger Spannung				
Netzsicherung	20-A-Sicherung je Netzteil, einpolig				
Überbrückung bei Stromausfall	min. 10 ms				
Stromverteilung	±5 % der Volllast zwischen Netzteilen				
Einschaltspitzenstrom	120 Apk „heißer“ Spitzenstrom pro Kabel bei beliebiger Spannung				

Tabelle 7. Herunterfahren bei hoher Umgebungstemperatur

Umgebungstemperatur	Hardwarefehler	Auswirkungen
Über 45 °C	Keine	Eine nicht kritische Warnung wird erzeugt.
Über 50 °C	Keine	Kritische Warnmeldung erzeugt. Das System wird nach Ablauf des Timers von fünf Minuten heruntergefahren. Wenn die Temperatur auf weniger als 45 °C (113 °F) zurückgeht, schaltet sich das System ein.
Alle	Die drei heißesten Laufwerke haben eine Durchschnittstemperatur von 50 °C (122 °F).	Das System wird nach Ablauf des Timers von fünf Minuten heruntergefahren.
Alle	Zwei Lüfter fehlerhaft	Das System wird nach Ablauf des Timers von fünf Minuten heruntergefahren.

Stromversorgungsanforderungen des PowerStore 500T

Die Anforderungen an die Stromversorgung hängen ab von der Systemkonfiguration, dem Laden und den Umgebungsbedingungen. Die nachstehende Tabelle enthält Worst-Case-Daten. Um die Stromverbrauchswerte für Ihre spezifische Umgebung zu schätzen, verwenden Sie den Dell Power Calculator.

Tabelle 8. Stromanforderungen für Wechselstrom

Voraussetzung	PowerStore 500T
Maximale Eingangsleistung	100 bis 240 V Wechselstrom ±10 %, einphasig
Wechselstrom (maximaler Betrieb)	max. 10 A bei 100 V Wechselstrom
	max. 5 A bei 200 V Wechselstrom
Stromverbrauch (maximaler Betrieb bei 200 VAC)	1004,1 VA (984 W)
Wärmeabgabe (maximaler Betrieb bei 200 VAC)	3,54 x 10^6 J/h (3358 BTU/h)
Wechselstromanschlusstyp (hohe Netzleistung)	Gerätestecker IEC320-C14 je Netzteil (200 VAC)
Wechselstromanschlusstyp (geringe Netzleistung)	Gerätestecker IEC320-C20 je Netzteil (100 VAC)
Normale Eingangsfrequenz	47 bis 63 Hz
Maximaler Einschaltstrom	45 Apk „kalter“ Spitzenstrom pro Kabel bei beliebiger Spannung
Schutz vor elektrostatischer Entladung (AC)	20-A-Sicherung je Netzteil, einpolig
Überbrückung bei Stromausfall	min. 10 ms
Stromverteilung	±5 % der Volllast zwischen Netzteilen
Einschaltspitzenstrom	120 Apk „heißer“ Spitzenstrom pro Kabel bei beliebiger Spannung

Tabelle 9. Stromanforderungen für Gleichstrom

Voraussetzung	PowerStore 500T
Netzspannung	-39 bis -72 DC
Gleichstrom (maximaler Betrieb)	max. 28,2 W bei -39 V Gleichstrom
	max. 22,9 W bei -48 V Gleichstrom
	max. 15,3 W bei -72 V Gleichstrom
Stromverbrauch (maximaler Betrieb)	1100 W
Wärmeabgabe (maximaler Betrieb bei 200 VAC)	3,96 x 10^6 J/h (3753 BTU/h)
Stromanschlusstyp	Positronics PLBH3W3M4B0A1/AA
Maximaler Einschaltstrom	40 A Spitze
Schutz vor elektrostatischer Entladung (DC)	50-A-Sicherung in jedem Netzteil
Überbrückung bei Stromausfall	min. 1 ms bei -50-V-Eingang
Stromverteilung	±5 % der Volllast zwischen Netzteilen

Stromversorgungsanforderungen des SAS-Erweiterungsgehäuses

Die Anforderungen an die Stromversorgung hängen ab von der Systemkonfiguration, dem Laden und den Umgebungsbedingungen. Die folgende Tabelle beschreibt die maximal zu erwartende Leistungsaufnahme. Um die Stromverbrauchswerte für Ihre spezifische Umgebung zu schätzen, verwenden Sie den Dell Power Calculator.

Tabelle 10. Stromversorgung

Voraussetzung	Beschreibung
Netzspannung	100 bis 240 V Wechselstrom ±10 %, einphasig, 47 bis 63 Hz
Wechselstrom (maximaler Betrieb)	max. 3,32 A bei 100 V Wechselstrom
	max. 1,66 A bei 200 V Wechselstrom
Stromverbrauch (maximaler Betrieb)	max. 308 VA (319 W) bei 100 V Wechselstrom
	max. 332 VA (315 W) bei 200 V Wechselstrom
Leistungsfaktor	min. 0,95 bei Volllast, 100 V / 200 V
Wärmeabgabe (maximaler Betrieb)	1,11 x 10^6 J/h max. (1.088 BTU/h) bei 100 VAC
	1,20 x 10^6 J/Std., (1.075 BTU/Std.) bei 200 V Wechselstrom
Einschaltstrom	max. 30 A für ½ Leitungszyklus pro Kabel bei 240 V Wechselstrom
Einschaltspitzenstrom	max. 40 A Spitzenstrom pro Kabel bei beliebiger Spannung
Netzsicherung	15-A-Sicherung je Netzteil, Phase und Nullleiter
Stromanschlusstyp	Gerätestecker IEC320-C14 je Netzteil
Überbrückung bei Stromausfall	Mind. 12 Millisekunden
Stromverteilung	± 5 % der Volllast zwischen Netzteilen

Stromversorgungsanforderungen des NVMe-Erweiterungsgehäuses

Die Anforderungen an die Stromversorgung hängen ab von der Systemkonfiguration, dem Laden und den Umgebungsbedingungen. Die folgende Tabelle beschreibt die maximal zu erwartende Leistungsaufnahme. Um die Stromverbrauchswerte für Ihre spezifische Umgebung zu schätzen, verwenden Sie den Dell Power Calculator.

Tabelle 11. Stromversorgung

Voraussetzung	Beschreibung
Netzspannung	100 bis 240 V Wechselstrom ±10 %, einphasig, 47 bis 63 Hz
Wechselstrom (maximaler Betrieb)	max. 6,49 A bei 100 V Wechselstrom
	max. 3,31 A bei 200 V Wechselstrom
Stromverbrauch (maximaler Betrieb bei 200 VAC)	663 VA (630 W)
Leistungsfaktor	min. 0,92 bei Volllast, 100 V/200 V
Wärmeabgabe (maximaler Betrieb bei 200 VAC)	2,27 x 10^6 J/hr (2.150 BTU/h)
Einschaltstrom	max. 82 A für ½ Leitungszyklus pro Kabel bei 200 V Wechselstrom
Einschaltspitzenstrom	Max. 100 A für bis zu 125 uSec
Netzsicherung	15-A-Sicherung je Netzteil, Phase und Nullleiter
Stromanschlusstyp	Gerätestecker IEC320-C14 je Netzteil
Überbrückung bei Stromausfall	Mind. 10 Millisekunden
Stromverteilung	+/- 5 % der Volllast zwischen Netzteilen

Betriebsumgebungsbeschränkungen

Tabelle 12. Betriebsumgebungsbeschränkungen

Limit Type	Einschränkung
Temperatur	5 bis 35 °C normal, 35 bis 40 °C für 10 % der Zeit
Luftfeuchtigkeit	–12 °C Taupunkt und 8 bis 85 % RH (nicht kondensierend)
Temperaturgradient (Festplatte)	20 °C/Std.
Höhenanpassung	Normal: Tiefere Temperatur 1 °C je 300 m über 950 m
	Unwahrscheinlich: Tiefere Temperatur 1 °C je 175 m über 950 m

Anforderungen bei Transport und Lagerung

VORSICHT: Systeme und Komponenten dürfen keinen Temperatur- und Feuchtigkeitsschwankungen ausgesetzt werden, die wahrscheinlich zu Kondensation in oder an diesem System oder dieser Komponente führen. Bei der Transport- und Lagertemperatur darf ein Gefälle von 25 °C/Std. (45 °F/Std.) nicht überschritten werden.

Tabelle 13. Anforderungen bei Transport und Lagerung

Voraussetzung	Beschreibung
Umgebungstemperatur	-40 °C bis +65 °C (-40° F bis 149° F)
Temperaturgefälle	25 °C/Std. (45 °F/Std.)
Relative Luftfeuchtigkeit	10 % bis 90 %, nicht kondensierend
Höhe über NN	–50 ft bis 35000 ft (-16 m bis 10600 m)
Lagerungszeit ohne Stromversorgung	Bei der Lagerung ohne Stromversorgung sollten sechs aufeinanderfolgende Monate nicht überschritten werden.

Luftstrom im Basisgehäuse

Das Basisgehäuse verwendet einen adaptiven Kühlungsalgorithmus, der die Lüftergeschwindigkeit steigert bzw. reduziert, wenn die Einheit Änderungen bei der externen Umgebungstemperatur feststellt. Der Abluftstrom steigt mit der Umgebungstemperatur und der Lüftergeschwindigkeit und verhält sich innerhalb der empfohlen Betriebsparameter in etwa linear. Beachten Sie, dass die Daten in der Tabelle unten typische Werte darstellen und ohne vordere/hintere Schranktüren gemessen wurden, die potenziell die Luftzirkulation von der Vorder- zur Rückseite reduzieren würden.

Tabelle 14. Luftstrom im Basisgehäuse

Max. Luftstrom in m³/min	Min. Luftstrom in m³/min	Max. Stromverbrauch (Watt)
165 m³/min	50 m³/min	850 W

Wiederherstellung der Umgebungswerte

Wenn das System die maximale Umgebungstemperatur um ca. 10 °C überschreitet, beginnt ein geregeltes Herunterfahren der Nodesen im System. Die im Cache befindlichen Daten werden gespeichert und anschließend erfolgt das Herunterfahren. LCCs (Link Control Cards) in jedem Erweiterungsgehäuse des Systems werden heruntergefahren, die Laufwerke bleiben jedoch aktiv.

Wenn das System erkennt, dass die Temperatur auf einen akzeptablen Wert gesunken ist, wird die Stromversorgung der Basisgehäuse wiederhergestellt und die LCCs versorgen ihre Laufwerke wieder mit Strom.

Anforderungen an die Luftqualität

Die Produkte sind für die Anforderungen des Environmental Standard Handbook der American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) und die neueste Version der Thermal Guidelines for Data Processing Environments, Second Edition, ASHRAE 2009b, ausgelegt.

Die Schränke sind am besten für Datacom-Umgebungen der Klasse 1 geeignet, bei denen streng kontrollierte Umgebungsparameter für Temperatur, Kondensationspunkt, relative Luftfeuchtigkeit und Luftqualität gelten. Diese Umgebungen mit geschäftskritischen Geräten sind in der Regel fehlertolerant – einschließlich der Klimaanlagen.

Die Sauberkeit im Rechenzentrum muss dem ISO-Standard 14664-1, Klasse 8, für besonderen Schutz vor Staub und Verunreinigungen entsprechen. Die Luftzufuhr im Rechenzentrum muss mit einem MERV-11-Filter oder besser gefiltert werden. Die Luft innerhalb des Rechenzentrums muss kontinuierlich mit einem MERV-8- oder besseren Filtersystem gefiltert werden. Darüber hinaus muss dafür gesorgt werden, dass keine leitenden Partikel wie Zinkpartikel in die Umgebung eindringen.

Die zulässige Luftfeuchtigkeit liegt bei 20 bis 80 %, nicht kondensierend, der empfohlene Bereich für die Betriebsumgebung liegt aber bei 40 bis 55 %. Bei Rechenzentren mit gasförmiger Kontaminierung wie hohem Schwefelgehalt werden niedrigere Temperaturen und eine niedrigere Luftfeuchtigkeit empfohlen, um die Gefahr der Korrosion und Beschädigung der Hardware zu minimieren. Allgemein müssen die Luftfeuchtigkeitsfluktuationen im Rechenzentrum minimiert werden. Es wird außerdem empfohlen, im Rechenzentrum auf einen gegenüber der Umgebung erhöhten Luftdruck zu achten und Luftschleier an den Eingängen anzubringen, damit Schadstoffe in der Luft und Luftfeuchtigkeit nicht in die Umgebung eindringen können.

Bei Einrichtungen mit einer relativen Luftfeuchtigkeit unter 40 % wird die Verwendung von Erdungsbändern beim Kontakt mit den Geräten empfohlen, um eine elektrostatische Entladung zu vermeiden, die elektronische Geräte beschädigen kann.

Als Teil des kontinuierlichen Überwachungsprozesses der Korrosionsstärke der Umgebung wird empfohlen, Kupfer- und Silbercoupons (nach ISA 71.04-1985, Abschnitt 6.1 „Reactivity“) in für das Rechenzentrum repräsentativen Luftströmen zu platzieren. Die monatliche Reaktivitätsrate der Streifen sollte weniger als 300 Ångström betragen. Wenn die überwachte Reaktivitätsrate übermäßig hoch ist, sollte der Streifen auf Materialsorten analysiert werden, damit ein korrektiver Abhilfeprozess umgesetzt werden kann.

Empfehlung für Speicherzeit (stromlos): Überschreiten Sie nicht sechs aufeinanderfolgende Monate mit einem stromlosen Speicher.

Haftungsausschluss für Feuerunterdrückung

Im Computerraum müssen als zusätzliche Sicherheitsmaßnahme immer Brandschutzvorrichtungen vorhanden sein. Ein Brandschutzsystem liegt in der Verantwortung des Kunden. Gehen Sie bei der Auswahl der geeigneten Feuerlöschsysteme und -mittel für das Rechenzentrum sorgfältig vor. Sie sollten sich bei der Auswahl eines Brandschutzsystems, das einen angemessenen Schutz bietet, von einem Versicherungsvertreter, der Feuerwehr vor Ort oder einem Bauinspektor beraten lassen.

Die Geräte werden nach internen und externen Standards entwickelt und gefertigt, die für einen zuverlässigen Betrieb bestimmte Umgebungen erfordern. Dell trifft weder Aussagen zur Kompatibilität noch gibt Dell Empfehlungen zu Brandschutzsystemen. Storage-Geräte sollten nicht direkt im Gasentladungsstrom oder neben lauten Feueralarmsirenen positioniert werden, um Kräfte und Vibrationen zu minimieren, die die Systemintegrität beeinträchtigen können.

ANMERKUNG: Die vorstehenden Informationen werden ohne Gewähr zur Verfügung gestellt und stellen keinerlei Zusicherung, Haftung oder Verpflichtung auf Seiten unseres Unternehmens dar. Diese Informationen haben keinerlei Auswirkung auf den Umfang der Haftung in den allgemeinen Geschäftsbedingungen der grundlegenden Kaufvereinbarung zwischen dem Kunden und dem Hersteller.

Erschütterung und Vibration

Die Produkte wurden auf die Unempfindlichkeit gegenüber Erschütterungen und zufälligen Vibrationen verschiedener Intensitäten hin getestet.

Diese Intensitäten gelten für alle drei Achsen und sollten mit einem Beschleunigungsmesser an den Gerätegehäusen im Schrank gemessen werden und folgende Werte nicht überschreiten.

Tabelle 15. Reaktionsstufen der Plattform

Plattformzustand	Reaktionsmesswert
Erschütterung bei Nichtbetrieb	25 Gs für 3 Millisekunden
Erschütterung im Betrieb	6 Gs für 11 Millisekunden
Zufallsvibration bei Nichtbetrieb	0,40 Grms bei 5–500 Hz für 30 Minuten

Tabelle 15. Reaktionsstufen der Plattform (fortgesetzt)

Plattformzustand	Reaktionsmesswert
Zufallsvibration im Betrieb	0,21 Grms in einem Frequenzbereich zwischen 5 und 500 Hz für 10 Minuten

Systeme, die auf einem genehmigten Paket befestigt sind, werden Transporttests unterzogen, damit sie Erschütterungen und Vibrationen in ausschließlich vertikaler Richtung standhalten. Die Level dürfen die Werte in dieser Tabelle nicht überschreiten.

Tabelle 16. Messwerte des verpackten Systems

Zustand des verpackten Systems	Reaktionsmesswert
Transporterschütterung	10 Gs für 12 Millisekunden
Zufallsvibration bei Transport	0,28 Grms in einem Frequenzbereich zwischen 1 und 100 Hz für 4 Stunden

3

Lizenzierung und Workstation-Anforderungen

In diesem Kapitel werden folgende Themen behandelt:

Themen:

Lizenzierung von PowerStore

Die PowerStore-Lizenz wird automatisch abgerufen und auf allen Appliances in Ihrem Cluster während der Erstkonfiguration installiert. Sie enthält den Zugriff auf alle mit PowerStore verfügbaren Funktionen.

Wenn Sie während und nach der Erstkonfiguration automatisch Lizenzen abrufen möchten, stellen Sie sicher, dass der Port 443 offen ist. Der Cluster kommuniziert mit dem Lizenzverwaltungssystem (ELMS) von Dell über Port 443, um die Lizenzdatei abzurufen. Wenn es ein Problem beim Abruf der Lizenzdatei gibt, wird Ihr Cluster in einem 30-tägigen Testzeitraum betrieben. Das System versucht alle 24 Stunden, automatisch eine Lizenz abzurufen. Wenn Sie den Status Ihrer Lizenz überprüfen möchten, gehen Sie in PowerStore Manager zu **Settings** > **Licensing**. Ein Status **Active** zeigt an, dass alle Appliances im Cluster über eine gültige Lizenz verfügen.

Wenn Sie noch nicht über eine aktive Lizenz verfügen, können Sie auf der Seite **PowerStore Licensing** auf **Refresh** klicken, um zu versuchen, die Lizenz automatisch abzurufen. Oder klicken Sie auf **Install License**, um die Lizenz manuell zu installieren.

ANMERKUNG: Sie benötigen keine separate PowerStore-Lizenz, wenn Sie die PowerStore-Betriebsumgebungssoftware und Firmwareupgrades installieren.

Workstation-Anforderungen

Verwenden Sie nach Abschluss des physischen Installationsprozesses eine Windows-basierte Workstation oder virtuelle Maschine, um die Appliances zu entdecken und mit der Erstkonfiguration zu beginnen. Informationen zu den Anforderungen an Workstations und virtuelle Maschinen finden Sie in der *Einfachen PowerStore-Supportmatrix*, die vom PowerStore Info Hub heruntergeladen werden kann.

4

Supportkonnektivität

In diesem Kapitel werden folgende Themen behandelt:

Themen:

Funktionsbeschreibung von Supportkonnektivität

Die folgenden Funktionen bieten eine Gewährleistung oder Abdeckung für die ProSupport Enterprise Suite:

ANMERKUNG: Secure Remote Services- und SupportAssist Enterprise-Funktionen sind nun Teil des sicheren Verbindungsgateways.

- Proaktive, automatisierte Problemerkennung, Fallerstellung und Benachrichtigung
- Beschleunigte Problemlösung durch Remotesupport und sichere bidirektionale Kommunikation zwischen Ihrem Serviceanbieter und Ihrer Storage-Umgebung
- Analysebasierte Empfehlungen für Support und Services

ANMERKUNG: Es wird dringend empfohlen, Supportkonnektivität zu aktivieren, um die Problemdiagnose zu beschleunigen, das Troubleshooting durchzuführen und eine kürzere Problemlösungszeit zu ermöglichen. Wenn Sie Supportkonnektivität nicht aktivieren, müssen Sie Informationen zur Appliance möglicherweise manuell erfassen, um Ihren Serviceanbieter beim Troubleshooting und bei der Behebung von Problemen mit der Appliance zu unterstützen. Außerdem muss Supportkonnektivität auf der Appliance aktiviert sein, damit Daten an Dell APEX AIOps Observability gesendet und die Verwendung der Anwendung für Cybersicherheit ermöglicht werden kann.

Vorabprüfung der Supportkonnektivität-Aktivierung

Bei PowerStoreOS-Betriebssystemversion 4.0 oder höher führt Supportkonnektivität eine Vorabprüfung als Teil des Aktivierungsprozesses durch. Die Vorabprüfung bestätigt proaktiv, ob sie für die Aktivierung bereit ist. Diese Vorabprüfungsfunktion identifiziert häufige Fehlkonfigurationen. Bei der Vorabprüfung wird Folgendes ermittelt:

- Die DNS-Konfiguration auf der Appliance kann erforderliche Hostnamen ordnungsgemäß auflösen.
- Für die direkte Verbindung sind die erforderlichen Netzwerkports offen, sodass die Appliance eine Verbindung zu den Back-end-Servern herstellen kann.
- Für die Verbindung über das sichere Verbindungsgateway sind die erforderlichen Netzwerkports offen, damit die Appliance die Backend-Server kontaktieren kann.
- Die Appliance kann gültige Zertifikate von den Dell Backend-Servern oder den Servern des sicheren Verbindungsgateways kopieren und speichern, um eine SSL-Verbindung herzustellen.
- Die Appliance verfügt über ausreichend verfügbaren Speicherplatz und führt keine Instanz von Supportkonnektivität aus.
- Die Appliance verfügt über die erforderlichen Zugangsdaten, die installiert sind, um eine erfolgreiche Verbindung zu ermöglichen.
- Beim Hinzufügen einer Appliance zu einem Cluster mit aktivierter Supportkonnektivität wird die Vorabprüfung auf der neuen Appliance ausgeführt, um zu überprüfen, ob auf der neuen Appliance ebenfalls Supportkonnektivität aktiviert werden kann.
- Beim Ändern der vorhandenen Supportkonnektivität-Konfiguration wird eine Teilmenge der definierten Tests ausgeführt, um zu überprüfen, ob die neue Konfiguration erfolgreich ist.

Wenn die Vorabprüfung feststellt, dass die Aktivierung von Supportkonnektivität fehlschlägt, bleibt sie deaktiviert. Außerdem werden Benachrichtigungen zusammen mit umsetzbaren Schritten zur Behebung von Problemen bereitgestellt, die während der Vorabprüfung erkannt wurden.

Die Vorabprüfung der Supportkonnektivität wird als Profil innerhalb der Systemintegritätsprüfungen implementiert. Die Registerkarte **Systemprüfungen** auf der Seite **Überwachung** in PowerStore Manager enthält eine zusätzliche Beschriftung und ein Wertpaar, das das Profil der letzten Systemprüfungsergebnisse basierend auf dem jeweiligen Profil anzeigt. **Systemprüfung ausführen** löst nur das Profil „Service-Engagement" aus. Andere Profile können jedoch durch andere Vorgänge oder Aktionen in PowerStore Manager ausgelöst werden. Wenn NutzerInnen beispielsweise Supportkonnektivität von PowerStore Manager über die Seite **Einstellungen** oder über den Assistenten für die Erstkonfiguration (Initial Configuration Wizard, ICW) aktiviert, werden auf der Registerkarte **Systemprüfungen** der Seite **Monitoring** die Ergebnisse der Systemprüfung angezeigt. Das Profil spiegelt Supportkonnektivität wider.

Wenn **Systemprüfung ausführen** ausgewählt ist, ändern sich die Werte für **Profil** und **Letzte Ausführung** und geben an, dass eine Systemprüfung ausgeführt wird. Sobald die Ergebnisse verfügbar sind, werden beide Werte aktualisiert, um das Profil „Service-Engagement" und den Wert der letzten Ausführung widerzuspiegeln. Die **Jobdetails** für PowerStore Manager geben die Ausgabe der aufgerufenen Systemprüfung an. Wenn während der Prüfung Fehler aufgetreten sind, werden diese in der Ausgabe der **Jobdetails** angezeigt.

ANMERKUNG: Die Vorabprüfung kann auch über das Servicskript `svc_health_check` aufgerufen werden. Außerdem enthält die REST API für `remote_support` die Option `precheck_override`, mit der Nutzer die Vorabprüfung von Supportkonnektivität überspringen können.

Supportkonnektivität und Sicherheit

Bei jedem Schritt des Remoteverbindungsprozesses von Supportkonnektivität kommen mehrere Sicherheitsebenen zum Tragen, die dafür sorgen, dass Sie und Ihr Serviceanbieter die Lösung ohne Sicherheitsbedenken nutzen können:

- Alle an Ihren Serviceanbieter gesendeten Benachrichtigungen werden von Ihrem Standort aus und niemals von einer externen Quelle gesendet und mit 256-Bit-AES-Verschlüsselung gesichert (AES = Advanced Encryption Standard).
- Die IP-basierte Architektur wird in Ihre vorhandene Infrastruktur integriert, wobei die Sicherheit Ihrer Umgebung erhalten bleibt.
- Die Kommunikation zwischen Ihrem Standort und dem Serviceanbieter erfolgt mit bilateraler Authentifizierung durch digitale Zertifikate.
- Unterstützt TLS 1.2
- Nur autorisierte Serviceanbieter mit einer gültigen Zwei-Faktor-Authentifizierung können die digitalen Zertifikate zur Anzeige einer Benachrichtigung von Ihrem Standort herunterladen.

Management von Supportkonnektivität

Sie können Supportkonnektivität mit PowerStore Manager oder mit der REST API managen. Sie können den Service aktivieren oder deaktivieren und die entsprechenden Informationen angeben, die für die ausgewählten Supportkonnektivität-Optionen erforderlich sind.

Supportkonnektivität Kommunikation

Supportkonnektivität kann nicht auf einem PowerStore-Cluster aktiviert werden, das mit IPv6 für das Managementnetzwerk konfiguriert wurde. Supportkonnektivität wird nicht über IPv6 unterstützt. Außerdem ist eine Neukonfiguration des Managementnetzwerks von IPv4 auf IPv6 nicht zulässig, wenn Supportkonnektivität auf einem Cluster konfiguriert ist.

ANMERKUNG: Damit Supportkonnektivität funktioniert, ist Zugriff auf einen DNS-Server erforderlich.

Der Verbindungsstatus von Supportkonnektivität zeigt den Status der Verbindung zwischen PowerStore und der Back-End-Support Services Ihres Serviceanbieters und die Servicequalität der Verbindung an. Der Verbindungsstatus wird über einen Zeitraum von fünf Minuten festgelegt und die Servicequalität der Verbindung wird über 24 Stunden festgelegt. Für den Verbindungsstatus kann basierend auf einer der Appliances im Cluster einer der folgenden Status angezeigt werden:

- `Unavailable` – Es sind keine Verbindungsdaten verfügbar. Sie haben möglicherweise den Kontakt zu einer Appliance verloren oder Supportkonnektivität wurde gerade aktiviert und es sind nicht genügend Daten vorhanden, um den Status zu bestimmen.
- `Disabled` – Supportkonnektivität wurde nicht aktiviert.
- `Not connected` – Die Verbindung wurde getrennt. Fünf aufeinanderfolgende KeepAlive-Ausfälle wurden erkannt.
- `Reconnecting` – PowerStore versucht, die Verbindung nach Verbindungsverlust wiederherzustellen. Fünf aufeinanderfolgende erfolgreiche KeepAlive-Anforderungen werden benötigt, um zu einem verbundenen Status zurückzukehren.

Für Verbindungsstatus kann basierend auf dem Durchschnitt aller Appliances im Cluster einer der folgenden Status angezeigt werden, wenn PowerStore mit den Support Services Ihres Serviceanbieters verbunden ist:

- `Evaluating` – Die Quality of Service für die Verbindung ist für die ersten 10 Stunden nach der ersten Initialisierung von Supportkonnektivität unbestimmt.

- `Good` – 80 % oder mehr der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.
- `Fair` – Zwischen 50 % und 80 % der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.
- `Poor` – Weniger als 50 % der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.

Supportkonnektivität-Remotesupport

Supportkonnektivität und seine Remotesupportfunktionen sind standardmäßig deaktiviert. Im Rahmen der Aktivierung von Supportkonnektivität und der Nutzung der Remote-Support-Services müssen Sie die Anwenderlizenzvereinbarung (End User License Agreement, EULA) akzeptieren. Andernfalls kann Supportkonnektivität nicht aktiviert werden und seine Remotesupportfunktion kann nicht verwendet werden. Sobald die Supportkonnektivität-EULA akzeptiert wurde, können Supportkonnektivität und seine Remotesupportfunktion konfiguriert werden.

Durch die Aktivierung der Remotesupportfunktion können von Ihrem Serviceanbieter autorisierte Supporttechniker sicher auf Ihr System zugreifen und Fehler beheben. Diese Funktion ermöglicht es den Supportmitarbeitern Ihres Serviceanbieters, sich remote beim System anzumelden, um eventuell auftretende Probleme zu beheben. Support-Mitarbeiter können sich per Remotezugriff über SSH oder PowerStore Manager bei Ihrem System anmelden. Ihr Supportvertrag legt fest, welche Aktionen und wann diese von den Mitarbeitern des Supports ausgeführt werden dürfen. Wenn Sie diese Funktion aktivieren, gewähren Sie Zugriff auf Ihr System, sodass die Fehlersuche und -behebung bei auftretenden Problemen erfolgen kann. Wenn z. B. Ereignisse wie ein Call Home, nicht verfügbare Daten oder Datenverluste oder andere außergewöhnliche Ereignisse auftreten, können die Servicemitarbeiter Ihres Serviceanbieters dank dieser Funktion schneller reagieren und die Probleme beheben.

Supportkonnektivität Optionen

Folgende Supportkonnektivität-Optionen sind verfügbar, mit denen Appliance-Informationen an Ihren Serviceanbieter für ein Remote-Troubleshooting gesendet werden können:

- **Verbindung über sicheres Verbindungsgateway herstellen**: Diese Option ist für zentralisierte Supportkonnektivität-Anwendungen vorgesehen, bei denen die Software des sicheren Verbindungsgateways auf einem vom Kunden bereitgestellten Gatewayserver mit bidirektionaler Dateiübertragung ausgeführt wird, einschließlich:
  - Call Homes
  - Unterstützung für Dell APEX AIOps Observability und Cybersicherheit
  - Softwarebenachrichtigungen
  - Download der Betriebsumgebung und Firmware von Ihrem Serviceanbieter auf den Cluster

  Diese Option bietet auch Remotezugriff für die SupportmitarbeiterInnen Ihres Serviceanbieters. Der Gatewayserver ist der zentrale Einstiegs- und Ausstiegspunkt für alle IP-basierten Supportaktivitäten für die Appliances, die mit dem Gateway verknüpft sind.
- **Direkt verbinden**: Diese Option ist für verteilte Supportkonnektivität-Anwendungen vorgesehen, bei denen die Software des sicheren Verbindungsgateways auf einzelnen Appliances mit derselben bidirektionalen Dateiübertragung ausgeführt wird wie bei der Verbindung über einen Gatewayserver.

Eine weitere Option, „Deaktiviert“, ist zwar verfügbar, wird aber nicht empfohlen. Wenn Sie diese Option auswählen, erhält Ihr Serviceanbieter keine Benachrichtigungen über Probleme mit der Appliance. Sie müssen Appliance-Informationen möglicherweise manuell sammeln, um Supportmitarbeiter beim Troubleshooting und bei der Behebung von Problemen mit der Appliance zu unterstützen.

Supportkonnektivität mithilfe der Option „Sicheres Verbindungsgateway“

Wenn Sie die Option **Verbindung über sicheres Verbindungsgateway herstellen** auswählen, wird Ihre Appliance zu anderen Appliances in einem sicheren Verbindungsgateway-Cluster hinzugefügt. Der Cluster befindet sich hinter einer einzigen, gemeinsamen, (zentralen) sicheren Verbindung zwischen den Servern Ihres Serviceanbieters und einem arrayexternen Gatewayserver. Der Gatewayserver ist der zentrale Einstiegs- und Ausstiegspunkt für alle IP-basierten Supportaktivitäten für die Appliances, die mit dem Gateway verknüpft sind.

Der Gatewayserver ist eine Lösung für Remotesupport, die auf einem oder mehreren vom Kunden bereitgestellten dedizierten Servern installiert ist. Die Option **Verbindung über sicheres Verbindungsgateway herstellen** unterstützt bis zu zwei Gatewayserver, einen als primären Server und einen als Backup. Der Gatewayserver fungiert als Kommunikationsbroker zwischen den zugehörigen Appliances und Ihrem Serviceanbieter.

Um Ihre Appliance für die Verwendung der Option **Verbindung über sicheres Verbindungsgateway herstellen** für Supportkonnektivität zu konfigurieren, müssen Sie die IP-Adresse für jeden Gatewayserver angeben. Portnummer 9443 ist die

Standardeinstellung und kann nicht geändert werden. Stellen Sie außerdem sicher, dass der Port zwischen dem Gatewayserver und der Appliance geöffnet ist.

ANMERKUNG: Der Gatewayserver muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können. Appliances können nur über den PowerStore Manager zum Gateway hinzugefügt werden. Wenn die Appliance vom Gatewayserver aus hinzugefügt wird, scheint sie verbunden zu sein, jedoch können Systeminformationen nicht erfolgreich gesendet werden.

Anforderungen für Supportkonnektivität bei Verwendung des Secure Connect Gateways

Die folgenden Anforderungen gelten für die Implementierung von **Verbindung über Secure Connect Gateway**Supportkonnektivität:

- Netzwerkverkehr (HTTPS) zwischen der Appliance und dem Server des sicheren Verbindungsgateways muss auf Port 9443 zugelassen sein. Lassen Sie den Zugriff auf die Ports 22, 443 und 8443 zwischen PowerStore und dem Secure Connect Gateway für PowerStore Manager und SSH-Zugriff zu. Legen Sie außerdem eine Ablehnungsregel zwischen der Appliance und dem ausgehenden Zugriff für die Ports 443 und 8443 fest, um sicherzustellen, dass die PowerStore-Appliance den Datenverkehr an den Secure Connect Gateway-Server weiterleitet.
- Der sichere Verbindungsgatewayserver muss Version 5.00.06.xy oder höher aufweisen.
- Stellen Sie sicher, dass auf dem PowerStore-Cluster PowerStoreOS Version 3.0 oder höher ausgeführt wird.

ANMERKUNG: Eine Appliance darf nie manuell zu einem Gatewayserver hinzugefügt oder von diesem entfernt werden. Eine Appliance darf nur PowerStore Manager hinzugefügt oder daraus entfernt werden.

Supportkonnektivität mit der Option „Direkt verbinden“

Für die Option **Direkt verbinden** wird das sichere Verbindungsgateway direkt auf jeder Appliance ausgeführt. In einem Cluster stellt jede Appliance eine eigene Verbindung zu Ihrem Serviceanbieter her. Der Datenverkehr wird nicht über die primäre Appliance in einem Cluster geroutet. Supportkonnektivität kann jedoch nur auf Clusterebene verwaltet werden, d. h. alle Änderungen werden auf alle Appliances im Cluster angewendet.

Aktivieren und konfigurieren Sie die Option **Direkt verbinden** auf der Seite **Supportkonnektivität**, die über **Einstellungen** aufgerufen werden kann und die in PowerStore Manager unter **Support** angezeigt wird. Diese Aktionen richten die Appliance so ein, dass eine sichere Verbindung zwischen ihr selbst und Ihrem Serviceanbieter verwendet wird.

Wenn Sie die Option **Direkt verbinden** auswählen und die Anwenderlizenzvereinbarung (End User License Agreement, EULA) akzeptieren, stellt die Appliance eine sichere Verbindung zwischen Ihnen und Ihrem Serviceanbieter her. Diese Option ermöglicht die Remotezugriff-Serviceverbindung für die Appliance zu und von Ihrem Serviceanbieter zusammen mit einer bidirektionalen Dateiübertragung. Gegebenenfalls können Sie die Verbindung von der Appliance zu einem zugehörigen Proxyserver (optional) konfigurieren.

Wenn eine neue Appliance zu einem vorhandenen Cluster hinzugefügt wird, erkennt sie die **Supportkonnektivität**-Clustereinstellungen und wird automatisch konfiguriert. Wenn die Option **Direkt verbinden** derzeit aktiviert ist, wird sie automatisch auf der neuen Appliance aktiviert. Es sind keine weiteren Aktionen erforderlich. Wenn die Option **Direkt verbinden** nicht aktiviert werden kann, verhindert dies nicht das Hinzufügen der Appliance.

Anforderungen für Supportkonnektivität bei Verwendung von Connect Directly

Die folgenden Anforderungen gelten für die Implementierung von **Connect Directly** Supportkonnektivität:

- Netzwerkdatenverkehr (HTTPS) muss auf den Ports 443 und 8443 (ausgehend) zu Ihrem Supportanbieter zulässig sein. Ein Fehler beim Öffnen von Port 8443 führt zu erheblichen Performanceeinbußen (30 bis 45 %). Ein Fehler beim Öffnen beider Ports führt möglicherweise zu einer Verzögerung bei der Behebung von Problemen mit dem Endgerät. Wenn die Verbindung einen Proxyserver verwendet, ist Port 3128 der Standardport, der verwendet wird, wenn der Port nicht angegeben und **Supportkonnektivität** mit **Connect Directly** aktiviert ist und eine Firewall zwischen dem Storage-System und dem Proxyserver verwendet wird. Wenn der Standardport oder nutzerdefinierte Port geschlossen ist, ist keine Kommunikation mit dem Storage-System über den Port möglich.

Konfigurieren von Supportkonnektivität

Sie können Supportkonnektivität mithilfe einer der folgenden Methoden für eine Appliance konfigurieren:

- Assistent für die Erstkonfiguration: eine Benutzeroberfläche, die Sie durch die anfängliche Einrichtung von PowerStore Manager führt und das System für die Verwendung vorbereitet.
- Supportkonnektivität – Eine Einstellungsseite, auf die Sie über PowerStore Manager zugreifen können (klicken Sie auf **Einstellungen** und wählen Sie unter **Support** die Option **Supportkonnektivität** aus).
- REST-API-Server – Eine Anwendungsschnittstelle, die REST-API-Anforderungen zum Konfigurieren der Einstellungen für die Supportkonnektivität empfangen kann. Weitere Informationen zur REST API finden Sie im *PowerStore REST API – Referenzhandbuch*.

Um den Status von Supportkonnektivität zu bestimmen, klicken Sie auf **Einstellungen** und wählen Sie unter **Support** die Option **Supportkonnektivität** in PowerStore Manager aus.

Konfigurieren der Ersteinrichtung von Supportkonnektivität

Voraussetzungen

ANMERKUNG: Die Supportkonnektivität kann auf einer PowerStore-Appliance oder einem Cluster, auf der STIG aktiviert ist, nicht aktiviert werden.

Um die Supportkonnektivität für die Option **Direkt verbinden** oder **Über sicheres Verbindungsgateway** zu aktivieren, ist ein uneingeschränkter Zugriff auf den Dell Support (esrs3-core.emc.com und esrs3-coredr.emc.com) über das Internet über HTTPS (für Nicht-Proxy-Umgebungen) erforderlich.

Wenn Ihre Firewall bei der Konfiguration von Supportkonnektivität zum Überprüfen von TLS-Zertifikaten konfiguriert ist, müssen die zugehörigen Zertifizierungsstellen-Zertifikatdateien der Liste vertrauenswürdiger Zertifizierungsstellen Ihrer Firewall hinzugefügt werden. Die folgenden erforderlichen Zertifikatdateien können über den entsprechenden Link heruntergeladen werden:

- Laden Sie die Zertifikatdatei DellSecureRemoteServicesRootCA.crt von Dell herunter.
- Laden Sie das Zertifikat ESRS2CA.cer-Zertifikatdatei von Dell herunter.

Info über diese Aufgabe

ANMERKUNG: Verwenden Sie dieses Verfahren nicht, wenn die Erstkonfiguration der Funktion durchgeführt und die entsprechende Anwenderlizenzvereinbarung (End User License Agreement, EULA) akzeptiert wurde.

Verwenden Sie PowerStore Manager zum Konfigurieren der Ersteinrichtung von Supportkonnektivität, indem Sie die folgenden Schritte ausführen:

ANMERKUNG: Bei PowerStoreOS OS 2.1 und späteren Versionen kann diese Funktion nur aktiviert werden, wenn unter **Support-Kontakte** die erforderlichen Informationen für **Pimärer Kontakt** angegeben werden. Außerdem müssen Sie nach einem erfolgreichen unterbrechungsfreien Upgrade ihre Browserregisterkarte aktualisieren oder schließen und wieder öffnen, um die neue Funktion anzuzeigen und zu verwenden. Andernfalls wird weiterhin die ältere Funktion angezeigt und verwendet.

Schritte

1. Klicken Sie auf **Einstellungen** und wählen Sie unter **Support** die Option **Supportkonnektivität** aus.
   Die Seite Supportkonnektivität wird angezeigt und **Support-Kontakt** ist ausgewählt.
2. Geben Sie die erforderlichen Informationen ein.

   ANMERKUNG: Die Felder **Vorname** und **Nachname** von **Primärer Kontakt** sind Pflichtfelder. Zudem muss das Feld **E-Mail-Adresse** oder **Telefon** für **Primärer Kontakt** ausgefüllt werden (mindestens eine dieser Angaben ist erforderlich). Die Angabe von Informationen für **Sekundärer Kontakt** ist optional. Ihre Kontaktinformationen für Supportkonnektivitätsind für eine schnelle Reaktion auf Supportprobleme wichtig und müssen genau und aktuell sein. Sie können auch die **Datenschutzerklärung** und den **Technologies Telemetrie-Hinweis** anzeigen, indem Sie auf den verwandten Link im Einführungstext von **Support-Kontakt** klicken.

3. Klicken Sie auf **Anwenden**, um die Informationen zu speichern.

   ANMERKUNG: Sie müssen auf **Anwenden** klicken, bevor Sie **Support-Kontakt** verlassen und **Verbindungstyp** auswählen können. Andernfalls wird eine Aufforderung angezeigt, in der Sie gefragt werden, ob Sie die Navigation abbrechen oder die eingegebenen Informationen verwerfen möchten.

4. Wählen Sie **Verbindungstyp** aus.

ANMERKUNG: Wenn die Ersteinrichtung von Supportkonnektivität nicht konfiguriert wurde, wird der Status als „Deaktiviert“ angezeigt.

5. Klicken Sie auf **Enabled/Disabled**, um mit der Aktivierung von Supportkonnektivität zu beginnen.

   ANMERKUNG: Bei PowerStoreOS-Betriebssystemversion 4.0 oder höheren Versionen führt Supportkonnektivität im Rahmen des Aktivierungsprozesses eine Vorabprüfung durch, um proaktiv zu bestätigen, dass es für die Aktivierung bereit ist. Wenn die Vorabprüfung feststellt, dass die Aktivierung von Supportkonnektivität fehlschlägt, bleibt sie deaktiviert. Außerdem werden Benachrichtigungen zusammen mit umsetzbaren Schritten zur Behebung von Problemen bereitgestellt, die während der Vorabprüfung erkannt wurden. Weitere Informationen zur Supportkonnektivität-Vorabprüfung finden Sie unter Vorabprüfung der Supportkonnektivität-Aktivierung.

   Die Seite Anwenderlizenzvereinbarung (End User License Agreement, EULA) wird angezeigt.
6. Klicken Sie auf **Accept**, um die EULA zu akzeptieren, und aktivieren Sie Supportkonnektivität.

   Supportkonnektivität kann geändert werden, dies wird jedoch nicht empfohlen. Wenn die EULA nicht akzeptiert wird, kann Supportkonnektivität nicht aktiviert werden.

   Die Schaltfläche **Aktiviert/Deaktiviert** sollte sich nach rechts verschieben und die Anzeige sollte sich in `Enabled` ändern. Der Verbindungsstatus ändert sich jedoch erst, nachdem Sie die erforderlichen Konfigurationsinformationen eingegeben und auf **Anwenden** geklickt haben.
7. Wählen Sie den zu verwendenden **Typ** der Option Supportkonnektivität aus der Liste aus.
8. Je nachdem, welche Supportkonnektivität-Option Sie ausgewählt haben, führen Sie danach einen der folgenden Schritte aus:
   - Für die Option **Verbindung über sicheres Verbindungsgateway herstellen**:
     - Geben Sie die IP-Adresse der einzelnen Gatewayserver, des primären Servers und ggf. des Backupservers an.

       ANMERKUNG: Jeder Gatewayserver muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können.

     - Port 9443 ist der Standardport und kann nicht geändert werden.
   - Für die Option **Direkt verbinden** :
     - Wenn für Ihre Netzwerkverbindung ein Proxyserver verwendet wird, geben Sie die IP-Adresse des Proxyservers an.

       ANMERKUNG: Der Proxyserver muss funktionsfähig sein, bevor Sie Ihre Appliance für seine Verwendung konfigurieren können.

     - Verwenden Sie die Steuerelemente, um die Nummer des Ports auszuwählen, der für die Verbindung mit dem Proxyserver in Ihrem Netzwerk verwendet werden soll.

       ANMERKUNG: Port 3128 ist der verwendete Standard, wenn der Port nicht angegeben und Supportkonnektivität mit **Direkt verbinden** aktiviert ist und eine Firewall zwischen der Appliance und einem Proxyserver eingesetzt wird. Wenn der Standard- oder nutzerdefinierte Port geschlossen ist, ist keine Kommunikation mit der Appliance über den Port möglich.
9. Je nachdem, welche Supportkonnektivität-Option Sie ausgewählt haben, führen Sie danach einen der folgenden Schritte aus:
   - Um die Option **Direkt verbinden** zu verwenden, fahren Sie mit dem nächsten Schritt fort.
   - Wählen Sie für die Option **Verbindung über sicheres Verbindungsgateway herstellen** die Option **Verbindung testen** für jeden konfigurierten Gatewayserver aus, um den Status der Verbindung zum Gatewayserver zu überprüfen.

   ANMERKUNG: Wenn der Konnektivitätsstatus im Status `Transitioning` bleibt und sich nach einigen Minuten nicht ändert (nach der Zeit, die zum Testen der Verbindung erforderlich sein sollte), wenden Sie sich an Ihren Serviceanbieter.
10. Das Kontrollkästchen **Mit Dell APEX AIOps Observability verbinden** ist standardmäßig aktiviert. Wenn Sie nicht möchten, dass Dateien an Dell APEX AIOps Observability gesendet werden und die Anwendung für Cybersicherheit verwenden können, deaktivieren Sie das Kontrollkästchen. Andernfalls lassen Sie das Kontrollkästchen aktiviert.
11. Das Kontrollkästchen **Remotesupport** ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass von Ihrem Serviceanbieter autorisierte Supporttechniker eine sichere Fehlerbehebung für Ihr System durchführen. Andernfalls lassen Sie das Kontrollkästchen aktiviert.
12. Wählen Sie **Testwarnmeldung senden**, um eine Testwarnmeldung an Ihren Serviceanbieter zu senden und die End-to-End-Konnektivität zu prüfen.
13. Wählen Sie **Anwenden** aus, um die Supportkonnektivität-Konfigurationsinformationen beizubehalten.

Managen von Supportkonnektivität-Einstellungen

Voraussetzungen

Supportkonnektivität wurde anfänglich konfiguriert und die entsprechende Anwenderlizenzvereinbarung (End User License Agreement, EULA) wurde akzeptiert.

Info über diese Aufgabe

Sie können die Konfigurationseinstellungen für **Support-Kontakt** und **Verbindungstyp** ändern, den Status der Funktion anzeigen, die Verbindung zu Ihrem Serviceanbieter testen und eine Testwarnmeldung an Ihren Serviceanbieter senden.

Schritte

1. Wählen Sie in PowerStore Manager **Einstellungen** und unter **Support Supportkonnektivität** aus.
   Die Supportkonnektivität-Seite wird angezeigt.
2. Um die Konfigurationseinstellungen von Supportkonnektivität zu ändern, führen Sie nach Bedarf eine oder mehrere der folgenden Aktionen aus:

   ANMERKUNG: Sie müssen auf **Anwenden** klicken, bevor Sie über **Support-Kontakt** oder **Verbindungstyp** navigieren können, nachdem Änderungen auf beiden Registerkarten vorgenommen wurden. Andernfalls wird eine Aufforderung angezeigt, in der Sie gefragt werden, ob die Navigationsverlagerung abgebrochen oder die eingegebenen Informationen verworfen werden sollen.

   - Ändern oder löschen Sie die Informationen für **Primärer Kontakt** oder **Sekundärer Kontakt** oder beides.

     ANMERKUNG: Bei PowerStoreOS OS 2.1 und späteren Versionen kann diese Funktion nur aktiviert werden, wenn die erforderlichen Informationen für **Pimärer Kontakt** angegeben werden. Außerdem können die Informationen für **Primärer Kontakt** nur gelöscht werden, wenn die Funktion deaktiviert ist. Die Felder **Vorname** und **Nachname** von **Primärer Kontakt** sind Pflichtfelder. Zudem muss das Feld **E-Mail-Adresse** oder **Telefon** für **Primärer Kontakt** ausgefüllt werden (mindestens eine dieser Angaben ist erforderlich). Die Angabe von Informationen für **Sekundärer Kontact** ist optional. Ihre Supportkonnektivität-Kontaktinformationen sind wichtig für eine schnelle Reaktion auf Supportprobleme und müssen genau und aktuell sein. Sie können auch die **Datenschutzerklärung** und den **Technologies Telemetrie-Hinweis** anzeigen, indem Sie auf den verwandten Link im Einführungstext von **Support-Kontakt** klicken.

   - Klicken Sie auf das Steuerelement **Enabled/Disabled**, um Supportkonnektivität zu aktivieren oder zu deaktivieren.

     ANMERKUNG: Der Verbindungsstatus ändert sich erst, nachdem Sie auf **Anwenden** geklickt haben.

     ANMERKUNG: Bei PowerStoreOS-Betriebssystemversion 4.0 oder höheren Versionen führt Supportkonnektivität im Rahmen des Aktivierungsprozesses eine Vorabprüfung durch, um proaktiv zu bestätigen, dass es für die Aktivierung bereit ist. Wenn die Vorabprüfung feststellt, dass die Aktivierung von Supportkonnektivität fehlschlägt, bleibt sie deaktiviert. Außerdem werden Benachrichtigungen zusammen mit umsetzbaren Schritten zur Behebung von Problemen bereitgestellt, die während der Vorabprüfung erkannt wurden. Weitere Informationen zur Supportkonnektivität-Vorabprüfung finden Sie unter Vorabprüfung der Supportkonnektivität-Aktivierung.

   - Ändern Sie die Option **Verbindungstyp**, die Sie verwenden möchten, und geben Sie alle erforderlichen Informationen an.
     - Für die Option **Verbindung über sicheres Verbindungsgateway herstellen**:
       - Geben Sie die IP-Adresse der einzelnen Gatewayserver, des primären Servers und ggf. des Backupservers an.

         ANMERKUNG: Jeder Gatewayserver muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können.

       - Port 9443 ist der Standardport und kann nicht geändert werden.
     - Für die Option **Direkt verbinden** :
       - Wenn für Ihre Netzwerkverbindung ein Proxyserver verwendet wird, geben Sie die IP-Adresse des Proxyservers an.

         ANMERKUNG: Der Proxyserver muss funktionsfähig sein, bevor Sie Ihre Appliance für seine Verwendung konfigurieren können.

       - Verwenden Sie die Steuerelemente, um die Nummer des Ports auszuwählen, der für die Verbindung mit dem Proxyserver in Ihrem Netzwerk verwendet werden soll.

ANMERKUNG: Wenn kein Port angegeben und Supportkonnektivität mit **Direkt verbinden** aktiviert ist und eine Firewall zwischen dem Storage-System und einem Proxyserver eingesetzt wird, ist der Standardport 3128. Wenn der Standardport oder nutzerdefinierte Port geschlossen ist, ist keine Kommunikation mit dem Storage-System über den Port möglich.

- Wählen Sie für die Option **Verbindung über sicheres Verbindungsgateway herstellen Verbindung testen** für die konfigurierten Gatewayserver aus, um den Status der Verbindung zu den Gatewayservern zu überprüfen.

  ANMERKUNG: Wenn der Konnektivitätsstatus im Status `Transitioning` bleibt und sich nach einigen Minuten nicht ändert (nach der Zeit, die zum Testen der Verbindung erforderlich sein sollte), wenden Sie sich an Ihren Serviceanbieter.

- Senden Sie eine Testwarnmeldung an Ihren Serviceanbieter, um die End-to-End-Konnektivität zu prüfen.
- Ändern Sie die Einstellung **Verbindung zu Dell APEX AIOps Observability**.

  ANMERKUNG: Um Dateien an Dell APEX AIOps Observability zu senden und die Cybersicherheitsanwendung verwenden zu können, aktivieren Sie das Kontrollkästchen. Deaktivieren Sie andernfalls das Kontrollkästchen.

- Ändern Sie die Einstellung für **Remotesupport**.

  ANMERKUNG: Wenn Sie zulassen möchten, dass von Ihrem Serviceanbieter autorisierte SupporttechnikerInnen eine sichere Fehlerbehebung für Ihr System durchführen, markieren Sie das Kontrollkästchen. Andernfalls deaktivieren Sie das Kontrollkästchen.

3. Wählen Sie **Anwenden** aus, um die Supportkonnektivität-Konfigurationsinformationen beizubehalten.

APEX AIOps Observability

Dell APEX AIOps Observability ist eine Cloud-basierte Anwendung, mit der NutzerInnen die Systemleistung nahezu in Echtzeit über mehrere PowerStore-Cluster hinweg überwachen und grundlegende Serviceaktionen durchführen können. Dell APEX AIOps Observability verwendet Protokolle, Systemkonfiguration, Warnmeldungen, Strom- und Temperaturkennzahlen, Performancekennzahlen, Kapazitätskennzahlen und Kapazitätsprognosedaten, die Supportkonnektivität von PowerStore-Clustern erfasst. Dell APEX AIOps Observability bietet Dashboard-Ansichten aller verbundenen Cluster, die wichtige Informationen anzeigen wie Performance, Kapazitätstrends und Kapazitätsprognosen. Dell APEX AIOps Observability bietet neben einer proaktiven Wartung, die NutzerInnen über Probleme informiert, bevor sie auftreten, auch einfache, geführte Fehlerkorrekturen.

ANMERKUNG: Supportkonnektivität muss auf dem Cluster aktiviert sein, um Daten an Dell APEX AIOps Observability zu senden.

NutzerInnen können Dell APEX AIOps Observability während der Konfiguration von PowerStore auf einem Supportkonnektivität-Cluster aktivieren. Die Unterstützung für Dell APEX AIOps Observability ist standardmäßig aktiviert, wenn eine Supportkonnektivität-Option aktiviert ist. Wenn Supportkonnektivität und Dell APEX AIOps Observability aktiviert sind, kann Dell APEX AIOps Observability direkt über PowerStore Manager gestartet werden.

ANMERKUNG: Sobald Dell APEX AIOps Observability aktiviert ist, kann Supportkonnektivität deaktiviert werden, ohne die Einstellung für Dell APEX AIOps Observability zu ändern. Ohne Supportkonnektivität werden keine Daten erfasst und an Dell APEX AIOps Observability gesendet, wenn Supportkonnektivität jedoch wieder aktiviert wird, erinnert sich das System an die Dell APEX AIOps Observability-Einstellung und nimmt das Senden von Daten an Dell APEX AIOps Observability sofort wieder auf. Die Deaktivierung des Dell APEX AIOps Observability-Supports deaktiviert nicht die Übertragung servicebezogener Telemetriedaten und proaktiver Datenerhebungen, die über Supportkonnektivität bereitgestellt werden.

Systemzustand

ANMERKUNG: Diese Funktion ist nur anwendbar, wenn Supportkonnektivität auf dem Cluster aktiviert ist und eine bidirektionale Verbindung zwischen PowerStore und Dell APEX AIOps Observability besteht.

Die **Systemintegrität** wird auf der Registerkarte **Übersicht** der Seite **Dashboard** in PowerStore Manager angezeigt. Die Integritätsbewertung bietet einen Einblick in die Performance des Systems. Die Integritätsbewertung basiert auf PowerStore-Warnmeldungen, die in den Telemetriedaten gesendet werden. Die **Systemintegrität** umfasst neben Problemen und den zugehörigen Korrekturschritten auch fünf Attribute, die als Symbole für Komponenten, Konfiguration, Kapazität, Leistung bzw. Data Protection angezeigt werden.

Cybersicherheit

ANMERKUNG: Supportkonnektivität und Dell APEX AIOps Observability muss auf dem Storage-System aktiviert sein, um die Verwendung der Cybersicherheitsanwendung zu ermöglichen.

Cybersicherheit ist eine cloudbasiert Software-as-a-Service-Anwendung zur Analyse der Storage-Sicherheit. Sie bietet eine Sicherheitsbewertung und misst die allgemeine Risikoebene der Cybersicherheit von Appliances mithilfe intelligenter, umfassender und vorausschauender Analysen. Cybersicherheit verwendet Supportkonnektivität zum Sammeln von Systemprotokollen, Systemkonfigurationen, Sicherheitskonfigurationen und -einstellungen, Warnmeldungen und Performancekennzahlen von Ihrem PowerStore-System.

A

Portnutzung

In den folgenden Abschnitten sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt. Die Appliance dient unter verschiedenen Umständen als Netzwerkclient, zum Beispiel bei der Kommunikation mit einem vCenter Server. In diesen Fällen initiiert die Appliance die Kommunikation und die Netzwerkinfrastruktur muss diese Verbindungen unterstützen.

Themen:

Appliance-Netzwerkports

In der folgenden Tabelle sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt.

Tabelle 17. Appliance-Netzwerkports

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
22	SSH-Client	TCP	Benutzer-Workstation	Cluster-IP, Appliance-IP oder Node-IP	Eingehend	Wird für den SSH-Zugriff verwendet (falls aktiviert). Ist dieser Port geschlossen, sind Managementverbindungen über SSH nicht verfügbar. ● Remotezugriff (Call Home): Sowohl die Appliance-IP als auch die Cluster-IP sind registriert. Die Appliance-IP wird für den Zugriff auf bestimmte Appliances verwendet (wenn die Managementverbindung aktiv ist). ● Support- oder AußendiensttechnikerInnen: Node-IP für den Zugriff auf einen bestimmten Node.
25 oder 587	SMTP	TCP	Node-IP	Nutzerzugewiesene SMTP-Server-IP.	Ausgehend	Wird von der Appliance zum Senden von E-Mails verwendet. Ist dieser Port geschlossen, können keine E-Mail-Benachrichtigungen gesendet werden.
26	SSH-Client	TCP	Benutzer-Workstation	Cluster-IP, Appliance-IP oder Node-IP	Eingehend	SSH-Zugriff auf Port 22 wird auf diesen Port umgeleitet. Ist dieser Port geschlossen, sind Managementverbindungen über SSH nicht verfügbar.
53	DNS	TCP oder UDP	Node-IP	DNS-Server-IP	Ausgehend	Wird verwendet, um DNS-Abfragen an den DNS-Server zu übertragen. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht.
80, 8080, 3128	Supportkonnektivität	TCP	Node-IP	Nutzerzugewiesene Proxyserver-IP.	Ausgehend	Wird für die Supportkonnektivität-Proxyverbindung verwendet.
123	NTP	TCP oder UDP	Node-IP	Nutzerzugewiesene NTP-Server-IP	Ausgehend	NTP-Zeitsynchronisation. Ist dieser Port geschlossen, wird die Zeit zwischen Appliances nicht synchronisiert.
162 oder von 1024 bis 49151	SNMP	UDP	Node-IP	Nutzerzugewiesene SNMP-Server-IP	Ausgehend	SNMP-Kommunikation. Ist dieser Port geschlossen, werden keine Warnmeldungsmechanismen für das Storage-System gesendet, die auf SNMP basieren. Der Standardport für SNMP ist 162.
443	● HTTPS ● Blockreplikation ● Remotebackup	TCP	Node-IP	Cluster-IP	Bidirektional	Sicherer HTTP-Datenverkehr zu PowerStore Manager. Wird auch für die Blockreplikations-Managementkommunikation zwischen Clustern und die Remotebackup-Managementkommunikation zwischen PowerStore und PowerProtect Data Domain verwendet. Ist dieser Port geschlossen, ist keine Kommunikation mit der Appliance möglich.
514	Remote-Protokollierung	UDP	Node-IP	Remote-Syslog-Server-IP	Ausgehend	Wird von der Appliance zum Senden von Protokollmeldungen an Remote-Syslog-Server verwendet.

Tabelle 17. Appliance-Netzwerkports (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
						Ist dieser Port geschlossen, können keine Protokollmeldungen an Remote-Syslog-Server gesendet werden.
1468	Remote-Protokollierung	TCP	Node-IP	Remote-Syslog-Server-IP	Ausgehend	Wird von der Appliance zum Senden von Protokollmeldungen an Remote-Syslog-Server verwendet. Ist dieser Port geschlossen, können keine Protokollmeldungen an Remote-Syslog-Server gesendet werden.
2049	DD Boost/NFS	TCP	Storage-IP-Set mit Replikationszweck	DD Boost-Schnittstellen-IP des PowerProtect Data Domain-Systems	Ausgehend	Von DD Boost für Remotebackup verwendeter Hauptport.
2051	DD Boost	TCP	Data Domain-IP der Replikationsquelle	Replikationsendpunkt oder Ziel-Data Domain	Ausgehend	Der Port wird nur vom DD Boost-Protokoll verwendet, wenn die Replikation konfiguriert ist.
2052	DD Boost/NFS	TCP	Storage-IP-Set mit Replikationszweck	DD Boost-Schnittstellen-IP des PowerProtect Data Domain-Systems	Ausgehend	Wird vom DD Boost-Protokoll für Remotebackup verwendet.
3033	Importieren	TCP oder UDP	Import: Storage-IP des FE-Portsatzes mit Replikationszweck	Import: Managementadresse des Remotesystems	Ausgehend	Erforderlich für den Speicherimport von Legacy-EqualLogic Peer-Speicher und Dell Compellent Storage Center-Systemen.
3260	iSCSI	TCP	Replikation und Import: Storage-IP des FE-Portsatzes mit Replikationszweck	• Eingehender Hostzugriff: Storage-IP des FE-Ports mit iSCSI-Zweck, über den der Host zugreifen kann • Replikation: Storage-IP	• Eingehend für Host- und ESXi-Hostzugriff • Bidirektional für Replikation • Ausgehender Storage für den Import	Erforderlich, um den folgenden Zugriff auf iSCSI-Services bereitzustellen: • Externer Host-iSCSI-Zugriff • Externer oder in PowerStore integrierter ESXi-Host-iSCSI-Zugriff • Inter-Cluster-Zugriff für Replikation • Storage-Importzugriff von Legacy-EqualLogic Peer-Speicher, Dell Compellent Storage Center-, Unity- und VNX2-Systemen Ist der Port geschlossen, sind keine iSCSI-Services verfügbar. Wird von der Datenmobilität zur Unterstützung

Tabelle 17. Appliance-Netzwerkports (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
				des FE-Portsatzes mit Replikationszweck • Import: Storage-IP des FE-Ports, der für den eingehenden Hostzugriff festgelegt und im Remotesystem des Imports festgelegt ist.		einer angemessenen Replikationsperformance bei einer Verbindung mit niedriger Latenz verwendet.
3261	iSCSI-/Datenmobilität	TCP	Replikation: Storage-IP des FE-Portsatzes mit Replikationszweck	Replikation: Storage-IP des FE-Portsatzes mit Replikationszweck	Bidirektional für Replikation	Wird von der Datenmobilität zur Unterstützung einer angemessenen Replikationsperformance bei einer Verbindung mit hoher Latenz verwendet.
4420	NVMe über TCP I/O Controller	TCP	Host-IP	Eingehender Hostzugriff: Storage-IP des FE-Ports, der mit NVMe/TCP-Zweck festgelegt ist, über den der Host darauf zugreift	Eingehend für Host- und ESXi-Hostzugriff	Erforderlich, um den folgenden Zugriff auf NVMe/TCP-I/O-Controller-Services bereitzustellen: • Externer Host-NVMe-/TCP-Zugriff • NVMe/TCP-Zugriff auf externen oder in PowerStore integrierten ESXi-Host Wenn dieser Port geschlossen ist, sind die NVMe TCP I/O-Controller-Services nicht verfügbar.
5353	Multicast-DNS (mDNS)	UDP	Alle Storage-IPs mit NVMe/TCP-Zweck **ANMERKUNG:** Gilt für IPs aus dem Storage-Netzwerk,	Die Zieladresse ist die Multicast-IP-Adresse 224.0.0.251	Bidirektional	Multicast-DNS-Abfrage. Ist dieser Port geschlossen, funktioniert die mDNS-Namensauflösung nicht.

Tabelle 17. Appliance-Netzwerkports (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
			die mit NVMe-Erkennung = „Auto Discovery of CDC“ oder „Advertise DDC“ konfiguriert sind.			
5555	RSA SecurID-Authentifizierung	TCP	Cluster-IP	RSA SecurID-Server-IP	Ausgehend	Wird verwendet, um mit einem RSA Authentifizierungsserver zu kommunizieren, wenn die RSA SecureID-Authentifizierungsfunktion aktiviert ist. Wenn dieser Port geschlossen ist, funktioniert die Authentifizierung mit dem RSA SecurID Authentication-Server nicht. Der Standardport für RSA SecurID Authentication ist 5555.
8009	NVMe über TCP Erkennungs-Controller	TCP	Eingehender Hostzugriff: Storage-IP des FE-Ports, der mit NVMe/TCP-Zweck festgelegt ist, über den der Host darauf zugreift	Host-IP	Eingehend für Host- und ESXi-Hostzugriff	Für NVMe von Erkennung verwendet. Wenn dieser Port geschlossen ist, sind NVMe-TCP-Erkennungsservices nicht verfügbar.
8443	• VASA • Supportkonnektivität	TCP	• vCenter IP • Cluster-IP oder Appliance-IP	• Appliance IP • Dell Global Access Server	• Eingehend für VASA • Ausgehend für Supportkonnektivität	• Erforderlich für den VASA Vendor Provider für VASA 3.0. • Erforderlich für die zugehörigen Supportkonnektivität Connect Home-Funktionen.
8443, 50443, 55443 oder 60443	• Windows Import-Host-Agent • Linux Import-Host-Agent	TCP	Storage-IP	• Windows Import-Host-Agent-IP	Ausgehend	Einer dieser Ports muss geöffnet sein, wenn der Datenspeicher von Legacy-Speichersystemen importiert wird.

Tabelle 17. Appliance-Netzwerkports (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
	• VMware Import-Host-Agent			• Linux Import-Host-Agent-IP • VMware Import-Host-Agent-IP		
9443	Supportkonnektivität	TCP	Appliance IP	SupportAssist Gateway-IP	Ausgehend	Erforderlich für Supportkonnektivität REST API in Bezug auf Connect Home.
13333	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Niedrig
13334	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Low_Medium
13335	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Mittel
13336	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Medium_High
13337	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Hoch

Appliance-Netzwerkports in Bezug auf Dateien

In der folgenden Tabelle sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt, die sich auf Dateien beziehen.

ANMERKUNG: Ausgehende Ports sind kurzlebig.

Tabelle 18. Appliance-Netzwerkports in Bezug auf Dateien

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
20	FTP (Datenverkehr)	TCP	NAS-Server-Produktionsschnittstelle	Beliebige IP	Eingehend	Für FTP-Datenübertragung verwendeter Port. Dieser Port kann durch Aktivieren von FTP geöffnet werden. Authentifizierung wird auf Port 21 durchgeführt und vom FTP-Protokoll definiert.
21	FTP (Managementdatenverkehr)	TCP	IP-Adresse des Produktionsnetzwerks	IP-Adresse der Produktionsschnittstelle des NAS-Servers	Eingehend	Port 21 ist der Kontrollport, den der FTP-Service auf eingehende FTP-Anforderungen überwacht.
22	SFTP	TCP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend	Warnmeldungen über SFTP (FTP über SSH) SFTP ist ein Client-/Serverprotokoll. Nutzer können mithilfe von SFTP Dateiübertragungen auf einer Appliance im lokalen Subnetz durchführen. Ermöglicht auch eine ausgehende FTP-Kontrollverbindung. Ist der Port geschlossen, ist FTP nicht verfügbar.
53	DNS	TCP oder UDP	NAS-Server-Produktionsschnittstelle	DNS-Server-IP	Ausgehend	Wird verwendet, um DNS-Abfragen an den DNS-Server zu übertragen. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht. Erforderlich für SMB v1.
88	Kerberos	TCP oder UDP	NAS-Server-Produktionsschnittstelle	Kerberos-IP des NAS-Servers	Ausgehend	Erforderlich für Kerberos-Authentifizierungsservices.
111	RPC bind (für Namespaces für Dateidienste, andernfalls Hostservice)	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Bidirektional	Wird vom Standard-Portmapper oder dem rpcbind-Service geöffnet und ist ein zusätzlicher Appliance-Netzwerkservice. Er kann nicht beendet werden. Per Definition kann ein Clientsystem bei einer Netzwerkverbindung zum Port diesen abfragen. Es wird keine Authentifizierung durchgeführt.
123	NTP	UDP	NAS-Server-Produktionsschnittstelle	NTP-Server-IP	Ausgehend	NTP-Zeitsynchronisation. Ist dieser Port geschlossen, wird die Zeit zwischen Appliances nicht synchronisiert.
135	Microsoft RPC	TCP	IP-Adresse des Produktionsnetzwerks	NAS-Server-Produktionsschnittstelle	Eingehend	Mehrere Zwecke für Microsoft Client.
137	Microsoft Netbios WINS	UDP, TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend, Ausgehend	Der NetBIOS Name Service ist mit den Appliance-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion (Wins). Wenn dieser Port deaktiviert ist, deaktiviert er alle SMB-bezogenen Services.

Tabelle 18. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
138	Microsoft Netbios BROWSE	UDP	• Eingehend: IP des Produktionsnetzwerks • Ausgehend: Produktionsschnittstelle des NAS-Servers	Eingehend: IP-Adresse der nutzerkonfigurierten NAS-Serverdateischnittstelle	Eingehend	Der NetBIOS Datagram Service ist mit den Appliance-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Es wird nur der Service zum Durchsuchen verwendet. Wenn dieser Port deaktiviert ist, deaktiviert er die Funktion zum Durchsuchen.
139	Microsoft SMB	TCP	Eingehend: IP des Produktionsnetzwerks	Eingehend: IP-Adresse der nutzerkonfigurierten NAS-Serverdateischnittstelle	Bidirektional	Der NetBIOS Session Service ist mit den Appliance-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Wenn SMB-Services aktiviert sind, ist dieser Port geöffnet. Er ist für SMB v1 erforderlich.
162 oder von 1024 bis 49151	SNMP	UDP	NAS-Server-Produktionsschnittstelle	SNMP-Server-IP	Ausgehend	SNMP-Kommunikation. Ist dieser Port geschlossen, werden keine Warnmeldungsmechanismen für das Storage-System gesendet, die auf SNMP basieren. Der Standardport für SNMP ist 162.
389	LDAP	TCP oder UDP	NAS-Server-Produktionsschnittstelle	LDAP-Server-IP	Ausgehend	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar. Sicheres LDAP ist als Alternative konfigurierbar.
445	Microsoft SMB	TCP	IP-Adresse des Produktionsnetzwerks	Eingehend: IP-Adresse der nutzerkonfigurierten NAS-Serverdateischnittstelle	Eingehend	SMB (auf dem Domain Controller) und SMB-Verbindungsport für Windows 2000-Clients und höher. Clients mit befugtem Zugriff auf die SMB-Services der Appliance benötigen für den fortlaufenden Betrieb eine Netzwerkverbindung zum Port. Eine Deaktivierung dieses Ports deaktiviert alle SMB-bezogenen Services. Ist Port 139 ebenfalls deaktiviert, wird die SMB-Dateifreigabe deaktiviert.
464	Kerberos	TCP oder UDP	NAS-Server-Produktionsschnittstelle	Kerberos IP	Ausgehend	Erforderlich für Kerberos-Authentifizierungsservices und SMB.
514	Remote-Protokollierung	UDP	NAS-Server-Produktionsschnittstelle	Remote-Syslog-Server-IP	Ausgehend	Ermöglicht es der Appliance, Protokollmeldungen an Remote-Syslog-Server zu senden. Ist dieser Port geschlossen, können keine Protokollmeldungen an Remote-Syslog-Server gesendet werden.
636	LDAPS	TCP oder UDP	NAS-Server-Produktionsschnittstelle	LDAP-Server-IP	Ausgehend	Sichere LDAP-Abfragen. Ist dieser Port geschlossen, ist keine sichere LDAP-Authentifizierung verfügbar.

Tabelle 18. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
1234	NFS mountd	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Bidirektional	Verwendet für den Mount-Service, der eine Kernkomponente des NFS-Services (Versionen 2, 3 und 4) ist.
1468	Remote-Protokollierung	TCP	NAS-Server-Produktionsschnittstelle	Remote-Syslog-Server-IP	Ausgehend	Ermöglicht es der Appliance, Protokollmeldungen an Remote-Syslog-Server zu senden. Ist dieser Port geschlossen, können keine Protokollmeldungen an Remote-Syslog-Server gesendet werden.
2000	SSHD	TCP	IP des Servicecontainers	NAS-Serviceschnittstelle auf Node	Eingehend	SSHD für Wartung (optional)
2049	NFS I/O	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Bidirektional	Verwendet für die Bereitstellung von NFS-Services.
3268	LDAP	UDP	NAS-Server-Produktionsschnittstelle	LDAP-Server-IP	Ausgehend	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar.
3269	LDAPS	UDP	NAS-Server-Produktionsschnittstelle	LDAP-Server-IP	Ausgehend	Sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind sichere LDAP-Authentifizierungsabfragen nicht verfügbar.
4000	STATD für NFSv3	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Bidirektional	Wird zum Bereitstellen der statd-Services von NFS verwendet. statd ist der Dateisperrmonitor von NFS und arbeitet mit lockd, um Absturz- und Recovery-Funktionen für NFS zu bieten. Ist dieser Port geschlossen, sind NAS-statd-Services nicht verfügbar.
4001	NLMD für NFSv3	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Bidirektional	Wird zum Bereitstellen der lockd-Services von NFS verwendet. lockd ist der Dateisperr-Daemon von NFS. Er verarbeitet Sperranfragen von NFS-Clients und arbeitet mit dem statd-Daemon zusammen. Ist dieser Port geschlossen, sind NAS-lockd-Services nicht verfügbar.
4002	RQUOTAD für NFSv3	TCP oder UDP, UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend, Ausgehend	Verwendet für die Bereitstellung von NFS-rquotad-Services. Der rquotad-Daemon bietet Quota-Informationen für NFS-Clients, auf denen ein Dateisystem gemountet ist. Ist dieser Port geschlossen, sind NAS-rquotad-Services nicht verfügbar.

Tabelle 18. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
4003	XATTRPD (erweitertes Dateiattribut)	TCP oder UDP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend	Erforderlich für das Management von Dateiattributen in einer Umgebung mit mehreren Protokollen.
5086	Dateireplikation (Replikationsmanagementverkehr)	TCP	Node-IP	Node-IP	Bidirektional	Wird von der Managementkommunikation für die Dateireplikation von Dateidiensten zwischen Clustern verwendet.
10000	NDMP	TCP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend	• Ermöglicht die Kontrolle von Backup und Recovery eines NDMP (Network Data Management Protocol)-Servers über eine Netzwerkbackupanwendung ohne Installation von Drittanbietersoftware auf dem Server. In einer Appliance fungiert der NAS-Server als NDMP-Server. • Wenn kein NDMP-Bandsicherung verwendet wird, kann der NDMP-Service deaktiviert werden. • Der NDMP-Service wird über eine Kombination aus Nutzername und Kennwort authentifiziert. Der Benutzername ist konfigurierbar. In der NDMP-Dokumentation wird beschrieben, wie Sie das Kennwort für verschiedene Umgebungen konfigurieren.
[10500,10531]	Von NDMP reservierter Bereich für dynamische NDMP-Ports	TCP	IP-Adresse des Produktionsnetzwerks	Nutzerkonfigurierte IP-Adresse der NAS-Serverdateischnittstelle	Eingehend	Verwenden Sie für Drei-Wege-Backup/Restore-Sitzungen die NAS-Server Ports 10500 bis 10531.
12228	Virenschutzprüfservice	TCP	NAS-Server-Produktionsschnittstelle	IP-Adresse des Virenschutzservice	Ausgehend	Erforderlich für den Virenschutzprüfservice.
13333	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Niedrig
13334	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Low_Medium

Tabelle 18. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Dienst	Protokoll	IP des Quellgeräts	IP des Zielgeräts	Zugriffsrichtung	Beschreibung
13335	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Mittel
13336	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Medium_High
13337	Datenmobilität	TCP	Storage-IP-Set mit Replikationszweck	Storage-IP von Remote-PowerStore mit Replikationszweck	Bidirektional	Wird vom iBasic-Replikationsdatenverkehr auf Blockreplikationsnetzwerkschnittstellen für die Latenzeinstellung verwendet: Hoch

B

Arbeitsblätter für die Rackplatzplanung

Dieser Anhang umfasst folgende Arbeitsblätter:

Themen:

Beispielarbeitsblatt für die Rackplatzplanung

Tabelle 19. Beispielarbeitsblatt für die Rackplatzplanung

40 (1 HE)	Managementswitch (nur PowerStore T-Modell)	
39 (1 HE)	**Ethernetswitch 2**	
38 (1 HE)	**Ethernetswitch 1**	
35 / 36 (2 HE)		
33 / 34 (2 HE)		
31 / 32 (2 HE)		
29 / 30 (2 HE)		
27 / 28 (2 HE)		
25 / 26 (2 HE)		
23 / 24 (2 HE)	Basisgehäuse 5 (BE5) Mgmt-IP-Adresse: xxx.xx.xxx	**Appliance 5** (2 Erweiterungsgehäuse im Stapel, wechselnde Reihenfolge)
21 / 22 (2 HE)	Erweiterungsgehäuse (BE5-EE1)	
19 / 20 (2 HE)	Erweiterungsgehäuse (BE5-EE2)	
17 / 18 (2 HE)	Erweiterungsgehäuse (BE4-EE2)	**Appliance 4** (2 Erweiterungsgehäuse im Stapel, wechselnde Reihenfolge)
15 / 16 (2 HE)	Erweiterungsgehäuse (BE4-EE1)	
13 / 14 (2 HE)	Basisgehäuse 4 (BE4) Mgmt-IP-Adresse: xxx.xx.xxx	
11 / 12 (2 HE)	Basisgehäuse 3 (BE3) Mgmt-IP-Adresse: xxx.xx.xxx	**Appliance 3** (1 Erweiterungsgehäuse im Stapel)
09 / 10 (2 HE)	Erweiterungsgehäuse (BE3-EE1)	
07 / 08 (2 HE)	Erweiterungsgehäuse (BE2-EE1)	**Appliance 2** (1 Erweiterungsgehäuse im Stapel)
05 / 06 (2 HE)	Basisgehäuse 2 (BE2) Mgmt-IP-Adresse: xxx.xx.xxx	
03 / 04 (2 HE)	Basisgehäuse 1 (BE1) Mgmt-IP-Adresse: xxx.xx.xxx	**Appliance 1** (Kein Erweiterungsgehäuse im Stapel)
01 / 02 (2 HE)	**Reserviert für Wartung**	

Leeres Arbeitsblatt für die Rackplatzplanung

Tabelle 20. Leeres Arbeitsblatt für die Rackplatzplanung

40 (1 HE)	Managementswitch (nur PowerStore T-Modell)	
39 (1 HE)	**Ethernetswitch 2**	
38 (1 HE)	**Ethernetswitch 1**	
35 / 36 (2 HE)		
33 / 34 (2 HE)		
31 / 32 (2 HE)		
29 / 30 (2 HE)		
27 / 28 (2 HE)		
25 / 26 (2 HE)		
23 / 24 (2 HE)		
21 / 22 (2 HE)		
19 / 20 (2 HE)		
17 / 18 (2 HE)		
15 / 16 (2 HE)		
13 / 14 (2 HE)		
11 / 12 (2 HE)		
09 / 10 (2 HE)		
07 / 08 (2 HE)		
05 / 06 (2 HE)		
03 / 04 (2 HE)		
01 / 02 (2 HE)	**Reserviert für Wartung**	