

Fehlerbehebung bei Hyperflex-Problemen mit dem Datenspeicher in ESXi

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen:](#)

[Problem](#)

[Datenspeicher in vCenter nicht verfügbar](#)

[Datenspeicher in vCenter/CLI überhaupt nicht verfügbar](#)

[Lösung](#)

[Überprüfung der Netzwerkverfügbarkeit](#)

[IOvisor/SCVMclient/NFS Proxy-Statusprüfung](#)

[Cluster-UID auflösbar mit ESXi-Loopback-IP](#)

[Einträge in veralteten Datenspeichern unter /etc/vmware/esx.conf](#)

[Firewall-Regeln im ESXi überprüfen](#)

[Überprüfen Sie iptable Regeln auf dem SCVM.](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte beschrieben, die Sie zur Behebung von Problemen mit der HyperFlex-Datenspeicher-Mount verwenden können.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen:

Hyperflex-Datenspeicher werden standardmäßig in NFS v3 gemountet.

NFS (Network File System) ist ein Dateifreigabeprotokoll, das vom Hypervisor für die Kommunikation mit einem NAS-Server (Network Attached Storage) über ein standardmäßiges TCP/IP-Netzwerk verwendet wird.

Im Folgenden werden die in einer vSphere-Umgebung verwendeten NFS-Komponenten beschrieben:

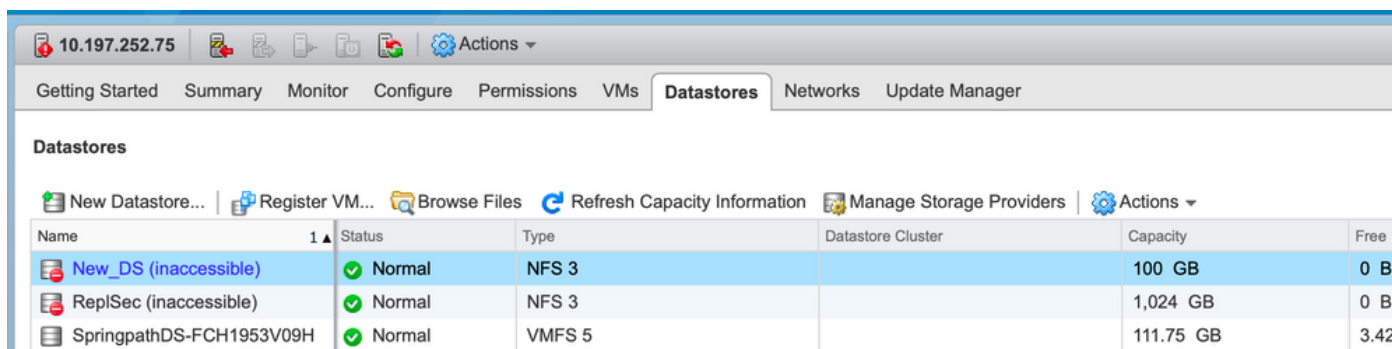
- **NFS-Server** - ein Speichergerät oder ein Server, der das NFS-Protokoll verwendet, um Dateien über das Netzwerk verfügbar zu machen. In der HyperFlex-Welt führt jedes Controller-VM eine NFS-Serverinstanz aus. Die NFS-Server-IP für die Datenspeicher ist die eth1:0-Schnittstellen-IP.
- **NFS-Datenspeicher** - eine gemeinsam genutzte Partition auf dem NFS-Server, die zum Speichern von Dateien für virtuelle Systeme verwendet werden kann.
- **NFS-Client** - ESXi enthält einen integrierten NFS-Client für den Zugriff auf NFS-Geräte.

Neben den regulären NFS-Komponenten ist auf dem ESXi eine VIB installiert, die IOVisor genannt wird. Diese VIB stellt einen NFS-Mount-Punkt (Network File System) bereit, sodass der ESXi-Hypervisor auf die virtuellen Festplatten zugreifen kann, die mit einzelnen virtuellen Systemen verbunden sind. Aus Sicht des Hypervisors wird sie einfach an ein Netzwerkdateisystem angefügt.

Problem

Die Symptome von Mount-Problemen können im ESXi-Host als Datenspeicher angezeigt werden, auf den nicht zugegriffen werden kann.

Datenspeicher in vCenter nicht verfügbar



Name	Status	Type	Datastore Cluster	Capacity	Free
New_DS (inaccessible)	Normal	NFS 3		100 GB	0 B
ReplSec (inaccessible)	Normal	NFS 3		1,024 GB	0 B
SpringpathDS-FCH1953V09H	Normal	VMFS 5		111.75 GB	3.42

Anmerkung: Wenn Ihre Datenspeicher in vCenter als nicht zugänglich angezeigt werden, werden sie in der ESX-CLI als nicht verfügbar angesehen. Das bedeutet, dass die Datenspeicher zuvor auf dem Host bereitgestellt wurden.

Überprüfen Sie die Datenspeicher über die CLI:

- SSH zum ESXi-Host, und geben Sie den Befehl ein:

```
[root@node1:~] esxcfg-nas -l
test1 is 10.197.252.106:test1 from 3203172317343203629-5043383143428344954 mounted unavailable
test2 is 10.197.252.106:test2 from 3203172317343203629-5043383143428344954 mounted unavailable
```

Datenspeicher in vCenter/CLI überhaupt nicht verfügbar

Name	Status	Type	Datastore Cluster	Capacity	Free
SpringpathDS-FCH1953V09H	Normal	VMFS 5		111.75 GB	3.42

Anmerkung: Wenn Ihre Datenspeicher nicht in vCenter oder CLI vorhanden sind. Dies weist darauf hin, dass der Datenspeicher zuvor nie erfolgreich auf dem Host bereitgestellt wurde.

- Überprüfen Sie die Datenspeicher über die CLI.
SSH zum ESXi-Host und geben Sie den Befehl ein:

```
[root@node1:~] esxcfg-nas -l  
[root@node1:~]
```

Lösung

Die Gründe für das Bereitstellungsproblem können unterschiedlich sein. Überprüfen Sie die Liste der zu validierenden und ggf. zu korrigierenden Prüfungen.

Überprüfung der Netzwerkverfügbarkeit

Bei Datenspeicherproblemen muss zuerst geprüft werden, ob der Host die NFS-Server-IP erreichen kann.

Bei Hyperflex ist die NFS-Server-IP die IP, die der virtuellen Schnittstelle **eth1:0** zugewiesen ist, die auf einem der SCVMs vorhanden ist.

Wenn die ESXi-Hosts den NFS-Server-IP nicht pinggen können, ist der Zugriff auf die Datenspeicher nicht mehr möglich.

Suchen Sie die **eth1:0** IP mit dem Befehl "**ifconfig**" auf allen SCVMs.

Anmerkung: Die **Eth1:0** ist eine virtuelle Schnittstelle und nur auf einer der SCVMs vorhanden.

```
root@SpringpathControllerGDAKPUCJLE:~# ifconfig eth1:0  
eth1:0 Link encap:Ethernet HWaddr 00:50:56:8b:62:d5  
inet addr:10.197.252.106 Bcast:10.197.252.127 Mask:255.255.255.224  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Um den ESXi-Host mit Bereitstellungsproblemen im Datenspeicher zu erreichen und zu überprüfen, ob er die NFS-Server-IP erreichen kann.

```
[root@node1:~] ping 10.197.252.106
PING 10.197.252.106 (10.197.252.106): 56 data bytes
64 bytes from 10.197.252.106: icmp_seq=0 ttl=64 time=0.312 ms
64 bytes from 10.197.252.106: icmp_seq=1 ttl=64 time=0.166 m
```

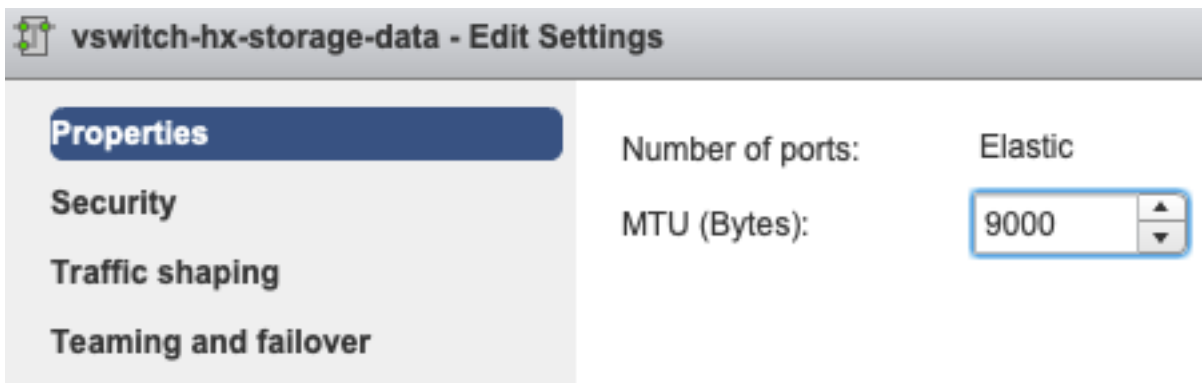
Wenn Sie einen Ping senden können, fahren Sie im nächsten Abschnitt mit den Schritten zur Fehlerbehebung fort.

Wenn Sie keine Ping-Verbindung herstellen können, müssen Sie Ihre Umgebung überprüfen, um die Erreichbarkeit zu beheben. Es gibt einige Zeiger, auf die Sie achten können:

- **hx-storage-data vSwitch-Einstellungen:**

Anmerkung: Standardmäßig wird die gesamte Konfiguration vom Installationsprogramm während der Cluster-Bereitstellung vorgenommen. Wenn Sie danach manuell geändert wurden, überprüfen Sie die Einstellungen.

MTU-Einstellungen: Wenn Sie die Jumbo-MTU während der Cluster-Bereitstellung aktiviert haben, muss die MTU auf dem vSwitch ebenfalls 9000 betragen. Wenn Sie keine Jumbo-MTU verwenden, muss dies 1500 sein.



Teaming und Failover: Standardmäßig versucht das System sicherzustellen, dass der Speicherdatenverkehr lokal vom FI geschickt wird. Daher müssen die aktiven und Standby-Adapter auf allen Hosts identisch sein.

vswitch-hx-storage-data - Edit Settings

Properties
Security
Traffic shaping
Teaming and failover



Load balancing:

Network failure detection:

Notify switches:

Failback:

Failover order

Active adapters
 vmnic3
Standby adapters
 vmnic2
Unused adapters

Select a physical network ad

Portgruppen-VLAN-Einstellungen - Das Storage-Daten-VLAN muss sowohl auf den Port-Gruppen "Storage Controller Data Network" als auch "Storage Hypervisor Data Network" angegeben werden.

Storage Controller Data Network - Edit Settings

Properties
Security
Traffic shaping

Network label:

VLAN ID:

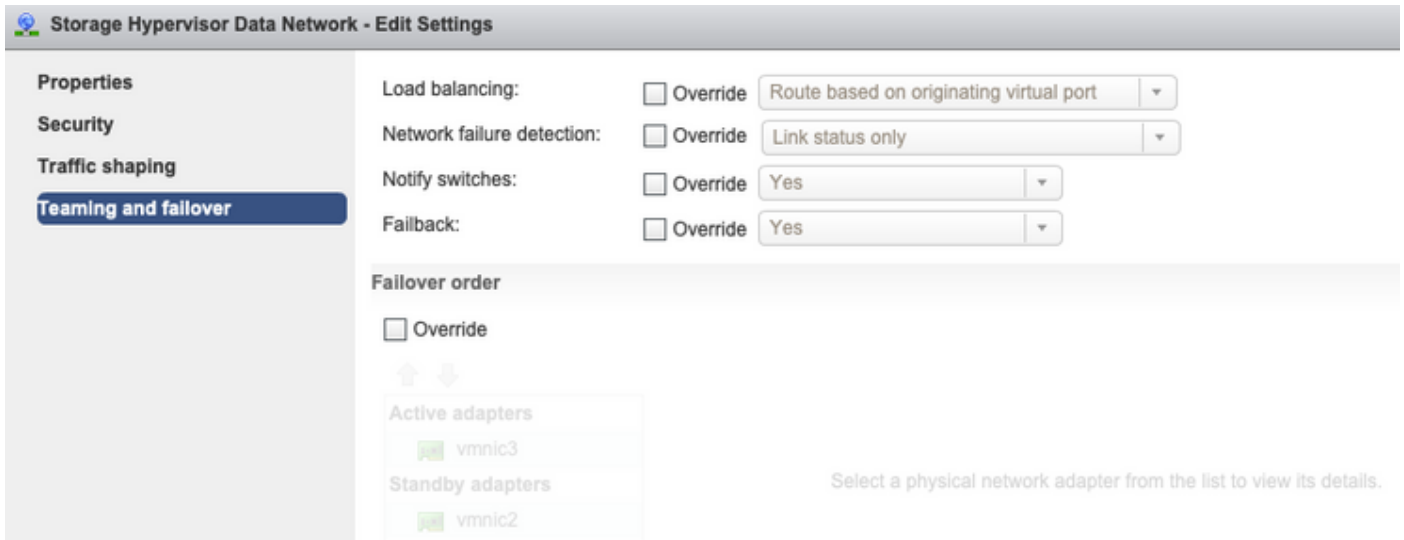
Storage Hypervisor Data Network - Edit Settings

Properties
Security
Traffic shaping

Network label:

VLAN ID:

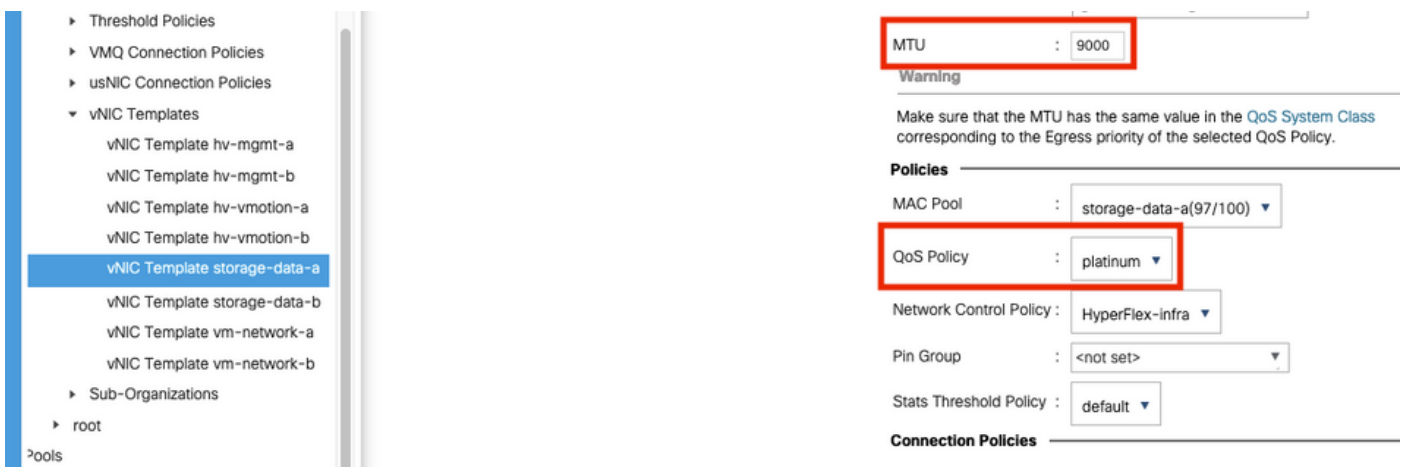
Keine Überschreibungen auf Port-Gruppenebene - Die auf vSwitch-Ebene vorgenommenen "Teaming & Failover"-Einstellungen werden standardmäßig auf die Portgruppen angewendet. Daher wird empfohlen, die Einstellungen auf Port-Gruppenebene nicht zu überschreiben.



• UCS vNIC-Einstellungen:

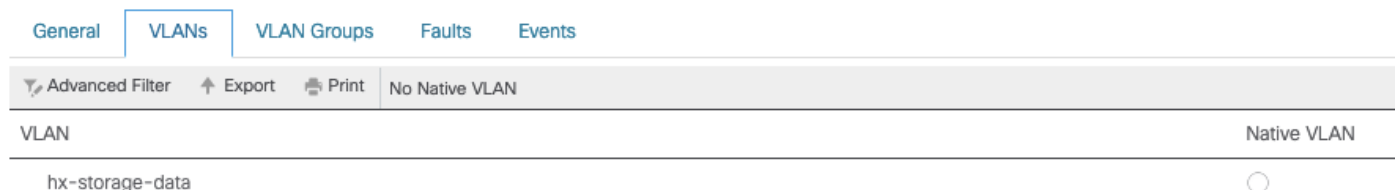
Anmerkung: Standardmäßig wird die gesamte Konfiguration vom Installationsprogramm während der Cluster-Bereitstellung vorgenommen. Wenn Sie danach manuell geändert wurden, überprüfen Sie die Einstellungen.

MTU-Einstellungen: Stellen Sie sicher, dass die MTU-Größe und die QoS-Richtlinie in der vNIC-Vorlage für die Speicherdaten korrekt konfiguriert sind. Die Storage-Daten-vNICs verwenden die Platinum-QoS-Richtlinie, und die MTU muss entsprechend Ihrer Umgebung konfiguriert werden.



VLAN-Einstellungen - Das während der Cluster-Bereitstellung erstellte hx-storage-data-VLAN muss in der vNIC-Vorlage zugelassen sein. Stellen Sie sicher, dass es nicht als nativ markiert ist.

LAN / Policies / root / Sub-Organizations / hxcluster1 / vNIC Templates / vNIC Template storage-da...



IOvisor/SCVMclient/NFS Proxy-Statusprüfung

Die SCVMclient-vib in der ESXI fungiert als NFS-Proxy. Er fängt die Virtual Machine IO ab, sendet

sie an das entsprechende SCVM und stellt ihnen die erforderlichen Informationen zur Verfügung.

Stellen Sie sicher, dass die VIB auf unseren Hosts für diese SSH zu einer der ESXI installiert ist, und führen Sie die folgenden Befehle aus:

```
[root@node1:~] esxcli software vib list | grep -i spring
scvmclient 3.5.2b-31674 Springpath VMwareAccepted 2019-04-17
stHypervisorSvc 3.5.2b-31674 Springpath VMwareAccepted 2019-05-20
vmware-esx-STFSNasPlugin 1.0.1-21 Springpath VMwareAccepted 2018-11-23
```

Überprüfen Sie jetzt den Status des scvmclient auf esxi und stellen Sie sicher, dass er **ausgeführt wird**. Wenn er angehalten wird, starten Sie ihn bitte mit dem Befehl **/etc/init.d/scvmclient start**

```
[root@node1:~] /etc/init.d/scvmclient status
+ LOGFILE=/var/run/springpath/scvmclient_status
+ mkdir -p /var/run/springpath
+ trap mv /var/run/springpath/scvmclient_status /var/run/springpath/scvmclient_status.old && cat /var/run/springpath/scvmclient_status.old |logger -s EXIT
+ exec
+ exec
Scvmclient is running
```

Cluster-UID auflösbar mit ESXI-Loopback-IP

Hyperflex ordnet die UUID des Clusters der Loopback-Schnittstelle des ESXi zu, sodass die ESXi die NFS-Anfragen an seinen eigenen scvmclient weiterleitet. Wenn dies nicht der Fall ist, können Probleme mit der Bereitstellung der Datenspeicher auf dem Host auftreten. Um dies zu überprüfen, leiten Sie ssh an den Host weiter, auf dem die Datenspeicher gemountet sind, und ssh an den Host mit Problemen, und katzen Sie die Datei **/etc/hosts**.

Wenn der nicht funktionierende Host den Eintrag in **/etc/hosts** nicht hat, können Sie ihn von einem funktionierenden Host in den **/etc/hosts** des nicht funktionierenden Hosts kopieren.

Nicht funktionierender Host

```
[root@node1:~] cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
10.197.252.75 node1
```

Arbeitsgeber

```
[root@node2:~] cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
10.197.252.76 node2
127.0.0.1 3203172317343203629-5043383143428344954.springpath 3203172317343203629-5043383143428344954
```

Einträge in veralteten Datenspeichern unter **/etc/vmware/esx.conf**

Wenn der HX-Cluster ohne Neuinstallation von ESXi neu erstellt wurde, können in der Datei

esx.conf alte Einträge für den Datenspeicher enthalten sein.

Dadurch können Sie die neuen Datenspeicher nicht mit demselben Namen bereitstellen. Sie können alle HX-Datenspeicher in **esx.conf** aus der Datei überprüfen:

```
[root@node1:~] cat /etc/vmware/esx.conf | grep -I nas
/nas/RepSec/share = "10.197.252.106:RepSec"
/nas/RepSec/enabled = "true"
/nas/RepSec/host = "5983172317343203629-5043383143428344954"
/nas/RepSec/readOnly = "false"
/nas/DS/share = "10.197.252.106:DS"
/nas/DS/enabled = "true"
/nas/DS/host = "3203172317343203629-5043383143428344954"
/nas/DS/readOnly = "false"
```

Wenn Sie in der Ausgabe sehen, dass der alte zugeordnete Datenspeicher und die alte Cluster-UUID verwenden, sodass ESXi Ihnen nicht ermöglicht, den gleichen Namen für den Datenspeicher mit der neuen UUID bereitzustellen.

Um dies zu beheben, ist erforderlich, um den alten Datenspeicheroreintrag mit dem Befehl **- esxcfg-nas -d RepSec** zu entfernen.

Versuchen Sie nach dem Entfernen erneut, die Bereitstellung des Datenspeichers vom HX-Connect-Server aus durchzuführen.

Firewall-Regeln im ESXi überprüfen

Nach Firewall-Aktivierungseinstellungen suchen

Es ist auf **False** gesetzt, es verursacht Probleme.

```
[root@node1:~] esxcli network firewall get
Default Action: DROP
Enabled: false
Loaded: true
```

Aktivieren Sie es mit den folgenden Befehlen:

```
[root@node1:~] esxcli network firewall set -e true
```

```
[root@node1:~] esxcli network firewall get
Default Action: DROP
Enabled: true
Loaded: true
```

Auf Verbindungsregleinstellungen überprüfen:

Es ist auf **False** gesetzt, es verursacht Probleme.

```
[root@node1:~] esxcli network firewall ruleset list | grep -i scvm
ScvmClientConnectionRule      false
```


Aktivieren Sie es mit den folgenden Befehlen:

```
[root@node1:~] esxcli network firewall ruleset set -e true -r ScvmClientConnectionRule
```

```
[root@node1:~] esxcli network firewall ruleset list | grep -i scvm
```

```
ScvmClientConnectionRule true
```

Überprüfen Sie iptable Regeln auf dem SCVM.

Überprüfen und abgleichen Sie die Anzahl der Regeln auf allen SCVMs. Wenn sie nicht übereinstimmen, öffnen Sie ein TAC-Ticket, um es zu korrigieren.

```
root@SpringpathControllerI51U7U6QZX:~# iptables -L | wc -l
```

```
48
```

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)