

SSH-Inkompatibilität mit ESXi 6.7P04 (Build 17167734) und höher

Inhalt

[Einführung](#)

[Anforderungen](#)

[Weitere Informationen](#)

[Defekt](#)

[Software-Beratung](#)

[Betroffene Bereiche](#)

[Probleumgehung](#)

[Schritte für Workarounds](#)

[Probleumgehung 1](#)

[Probleumgehung 2](#)

Einführung

Zwischen HXDP [3.5(x), 4.0(x)] und ESXi 6.7P04 (Build 17167734) und höheren Versionen besteht ein Softwareinteroperabilitätsproblem. Kunden sollten diese Softwarekombination vermeiden.

HINWEIS: Dieses Problem wird auf alle 6.7 ESXi-Versionen über 6.7P04 ausgeweitet.

Das Kompatibilitätsproblem wurde in HXDP 4.0(2e) behoben. Dieses Problem betrifft HXDP 4.5(1a) und höher nicht.

Anforderungen

ESXi 6.7P04 (Build 17167734) und höher

HXDP-Version - 3.5(x), 4.0(x)

Weitere Informationen

Defekt

Die zugehörige Bug-ID lautet [CSCv88204](#) - ESXi OpenSSH-Interoperabilitätsproblem mit HXDP

Das Problem tritt in ESXi 6.7P04 auf, da VMware die OpenSSH-Bibliothek auf OpenSSH_8.3p1 aktualisiert hat. Diese neue Version von OpenSSH entfernt die Unterstützung für die Schlüsselaustauschmethode, die HXDP bei der direkten Kommunikation mit ESXi über SSH intern verwendet. Im Folgenden finden Sie einen Ausschnitt aus dem OpenSSH-Changelog, der die grundlegenden Änderungen in dieser Version beschreibt:

ssh(1), sshd(8): this release removes diffie-hellman-group14-sha1 from the default key exchange proposal for both the client and server.

Software-Beratung

Weitere Einzelheiten finden Sie in der Software Advisory - [Cisco Software Advisory for ESXi 6.7 P04](#)

Betroffene Bereiche

Einige Funktionsbereiche von HX sind betroffen, darunter:

- Neuere Cluster-Erstellung (kann bei fehlgeschlagener Algorithmus-Aushandlung scheitern)

The screenshot shows the Cisco HyperFlex Installer interface. At the top, a progress bar indicates the status of various steps: Start, Config Installer, Validations, UCSM Configuration, Hypervisor Configuration, Deploy Validation, Deploy, Create Cluster Validation, and Cluster Creation. The Cluster Creation step is marked with a red exclamation mark, indicating a failure. Below the progress bar, a message reads "Errors found during Cluster Creation" with buttons for "Retry Cluster Creation" and "Re-Enter Credentials". The main area displays a detailed error log for "Cluster Creation - Overall", which is marked as "Failed". The error log shows the following steps and their status:

Step	Status	Details
Cluster Creation - Overall	Failed	
VirtCluster	Failed	Algorithm negotiation fail
Configuring Cluster Resource Manager	Success	
Preparing Storage Cluster	In Progress	
10.20.3.79	Failed	VirtNode
10.20.3.80	Failed	VirtNode

On the right side, the "Configuration" panel is visible, showing fields for Credentials (UCS Manager Host Name, UCS Manager User Name, vCenter Server, User Name, Admin User name), Server Selection (Server 1, Server 2, Server 3), and UCSM Configuration (VLAN Name, VLAN ID).

- Cluster-Erweiterung (kann bei fehlgeschlagener Algorithmusverhandlung fehlschlagen)

The screenshot shows the UCS Manager web interface during a cluster expansion. The main content area displays the progress of the expansion for IP 10.21.4.114, which is marked as 'Failed'. The summary table shows the following steps:

Step	Status	Details
Formatting disks	Failed	Some(Algorithm negotiation fail)
VirtNode	Failed	Algorithm negotiation fail
JoinCluster	Success	
Mgmt Service	Success	
StNode	In Progress	

The right-hand sidebar contains configuration details:

- Credentials:** UCS Manager Host Name, UCS Manager User Name (admin), vCenter Server, User Name (administrator@vsphere.local), Admin User name (root).
- Cluster Expand Configuration:** Management Cluster.
- Server Selection:** Server 4 (HX220C-M5SX).
- UCSM Configuration:** VLAN Name (hx-inband-mgmt).

- Cluster-Neuregistrierung (stcli Cluster-Registrierung kann fehlschlagen, wenn "Algorithm-Aushandlung fehlgeschlagen")

```

root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrator@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster ucsblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration with a new vCenter failed
Algorithm negotiation fail
root@ucsblr1152-svcm:~#

```

- Systeminformationen auf der HX Connect-Seite
- Upgrades können fehlschlagen mit "Es konnte keine SSH-Verbindung zum Host hergestellt werden" oder mit "Fehler, die während des Upgrades gefunden wurden".

ESXi-Upgrades fehlschlagen mit ssh exception-

2020-12-16-10:31:04.675 [] [vmware-upgrade-pool-9] ERROR c.s.sysmgmt.stMgr.SshScpUtilImpl - Es konnte keine SSH-Verbindung zum Host hergestellt werden: Host ist nicht erreichbar oder befindet sich im Sperrmodus

com.jcraft.jsch.JSchException: Algorithmusverhandlung fehlgeschlagen

Select Upgrade Type Progress

Validation failed

HX-02
Failed

- ❗ Checking if ESXi upgrade is required
Failed to establish SSH connection to host: Host is not reachable, or in lockdown mode
- ✅ Checking cluster state
- ✅ Checking if cluster rebalance is in progress
- ✅ Checking if all nodes are online and connected to vCenter
- ✅ Checking if all controller VMs have enough free space in root partition
- ✅ Checking if all controller VMs have disks mounted correctly
- ✅ Checking ESX Host Version on Cluster Nodes with NVMe Disks
- ✅ Validating if all nodes have same HyperFlex version for ESXi only upgrade
- ✅ Querying Hypervisor bundle details during upgrade

HyperFlex Connect HX-02 11

Select Upgrade Type Progress

❗ Errors found during upgrade

Upgraded 0 of 3 total nodes

^ Collapse All

Node	Status	Step
hx-02-esxi-1	In Progress	Copying Hypervisor Upgrade Package
hx-02-esxi-2	Failed	Copying Hypervisor Upgrade Package
hx-02-esxi-2	Failed	Checking Cluster readiness
hx-02-esxi-2	Failed	Entering Cluster Node into maintenance mode
hx-02-esxi-2	Failed	Upgrading hypervisor
hx-02-esxi-2	Failed	Rebooting Cluster Node
hx-02-esxi-2	Failed	Waiting for vCenter to connect to cluster node
hx-02-esxi-2	Failed	Exiting Cluster Node from maintenance mode
hx-02-esxi-3	In Progress	

- Potenziell andere Bereiche

Problemumgehung

Die HXDP-Versionshinweise wurden aktualisiert, um speziell darauf hinzuweisen, dass diese Version von 6.7 auf 3.5(x)- und 4.0(x)-Versionen nicht unterstützt wird. Dieses Problem wurde im HXDP 4.0-Patch - 4.0(2e) und in allen Versionen 4.5(1a) und höher behoben.

- Verwenden Sie den in ESXi integrierten Rollback-Mechanismus, um auf eine kompatible ESXi-Version zurückzusetzen.
- Eine weitere mögliche Problemumgehung besteht darin, die entfernte Schlüsselaustauschmethode durch Aktualisieren von `sshd_config` auf jedem ESXi-Host erneut zu aktivieren und den SSH-Dienst neu zu starten. Es wird empfohlen, diese Problemumgehung nur vorübergehend zu implementieren.

HINWEIS: Ziel sollte es sein, den Cluster zu einer festen HXDP-Version zu verschieben und diese Problemumgehung so schnell wie möglich zu entfernen. Cluster sollten in diesem Zustand nicht

langfristig verbleiben, wenn diese zusätzliche Schlüsselalgorithmuseinstellung zu sshd_config hinzugefügt wird.

Schritte für Workarounds

Wenn Sie HXDP nicht auf eine feste Version aktualisieren können, verwenden Sie die folgenden Problemumgehungen:

Problemumgehung 1

- Verwenden Sie den in ESXi integrierten Rollback-Mechanismus, um auf eine kompatible ESXi-Version zurückzusetzen. Siehe vmware KB - <https://kb.vmware.com/s/article/1033604>

Problemumgehung 2

Aktivieren Sie die entfernte Schlüsselaustauschmethode erneut, indem Sie sshd_config auf jedem ESXi-Host aktualisieren und den SSH-Dienst neu starten.

- Fügen Sie +diffie-hellman-group14-sha1 zu den KexAlgorithms unter /etc/ssh/sshd_config auf jedem ESXi-Host hinzu.

```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

- Vergewissern Sie sich, dass **KexAlgorithms +diffie-hellman-group14-sha1** in /etc/ssh/sshd_config angezeigt wird.

```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO
AuthorizedKeysFile /etc/ssh/keys-%u/authorized_keys
# Timeout value of 10 mins. The default value of ClientAliveCountMax is 3.
# Hence, we get a 3 * 200 = 600 seconds timeout if the client has been
# unresponsive.
ClientAliveInterval 200
# sshd(8) will refuse connection attempts with a probability of "rate/100"
# (30%) if there are currently "start" (10) unauthenticated connections. The
# probability increases linearly and all connection attempts are refused if the
# number of unauthenticated connections reaches "full" (100)
MaxStartups 10:30:100
KexAlgorithms +diffie-hellman-group14-sha1
l /etc/ssh/sshd_config [Modified] 54/54 100%
```

- ESXi SSH-Prozess neu starten

```
# /etc/init.d/SSH restart
```

```
[root@hx-02-esxi-2:/var/log]
[root@hx-02-esxi-2:/var/log] /etc/init.d/SSH restart
SSH login disabled
SSH login enabled
[root@hx-02-esxi-2:/var/log]
```

- Starten Sie den zuvor fehlgeschlagenen Workflow erneut, oder setzen Sie ihn fort.