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

Inhalt

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.
```

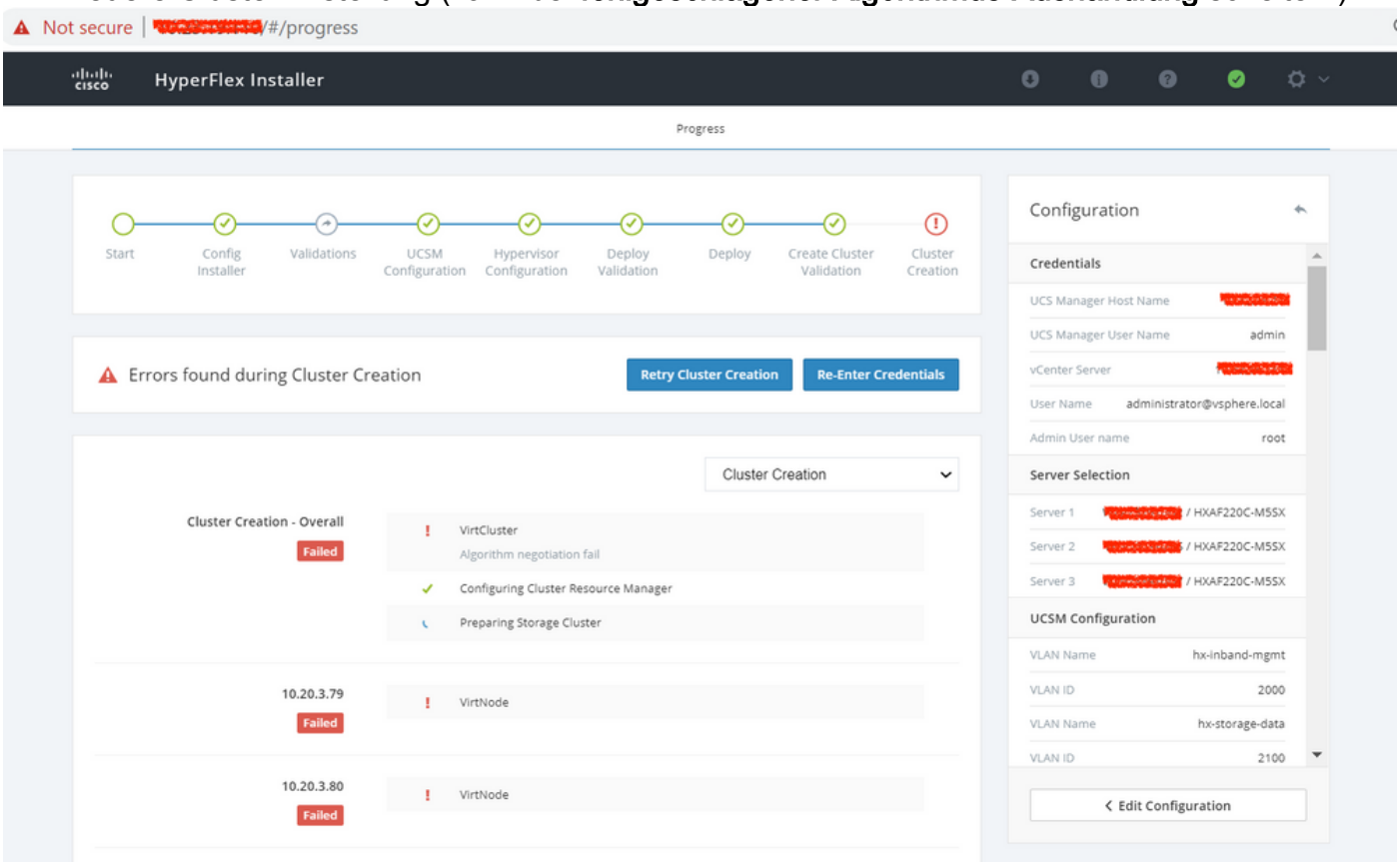
Software-Beratung

Weitere Einzelheiten finden Sie in der Software Advisory - Cisco Software Advisory for ESXi 6.7 P04

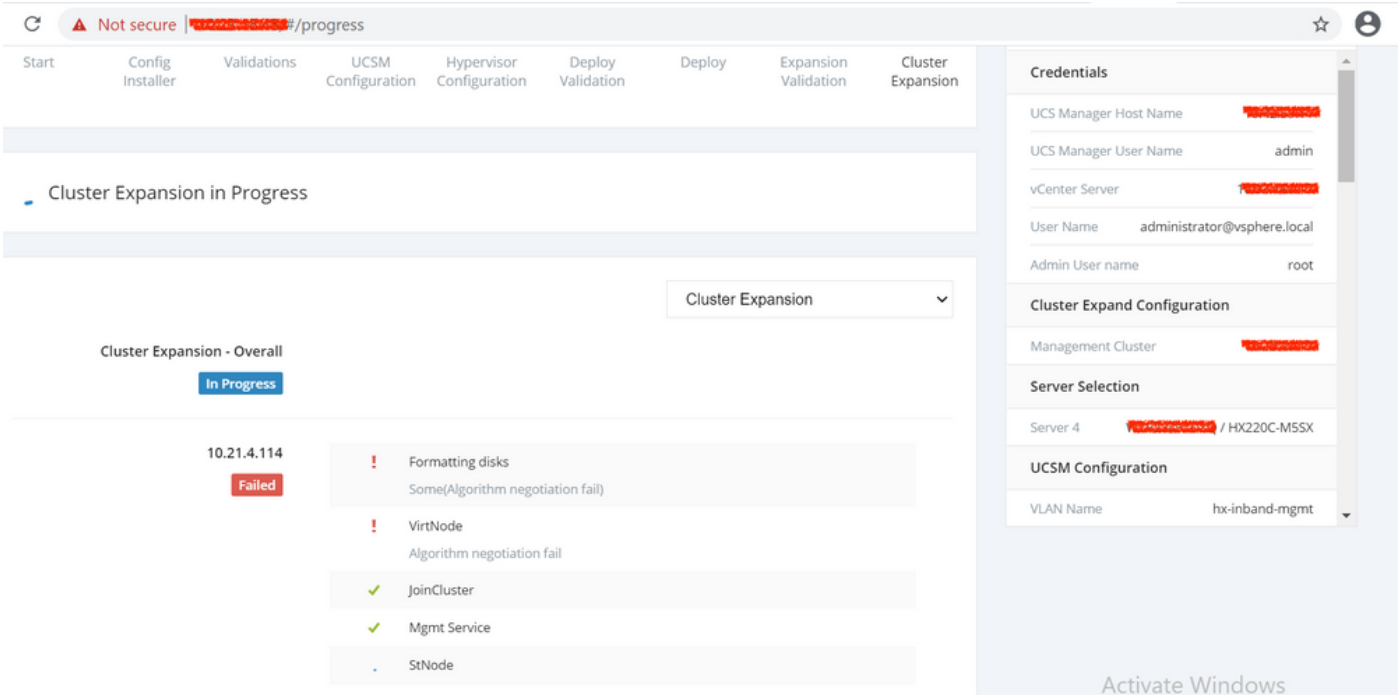
Betroffene Bereiche

Einige Funktionsbereiche von HX sind betroffen, darunter:

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



- Cluster-Erweiterung (kann bei **fehlgeschlagener Algorithmusverhandlung** fehlschlagen)



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

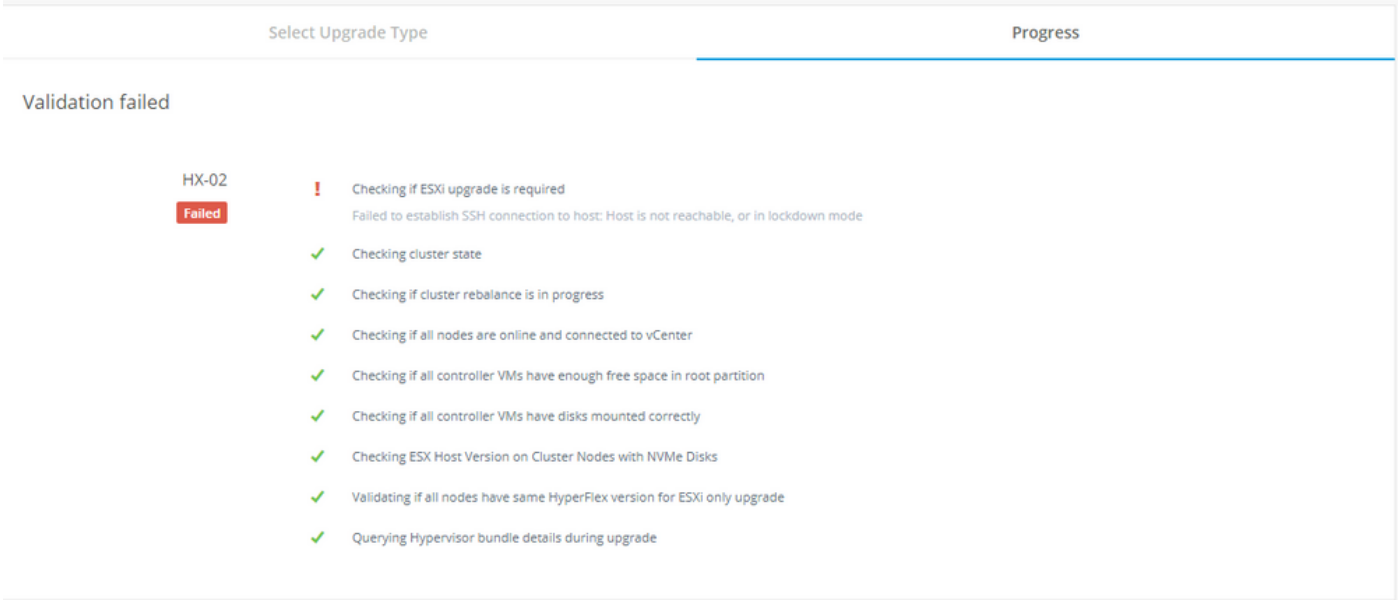
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration with a new vCenter failed
Algorithm negotiation fail
root@ucsblr1152-svcm:~#
```

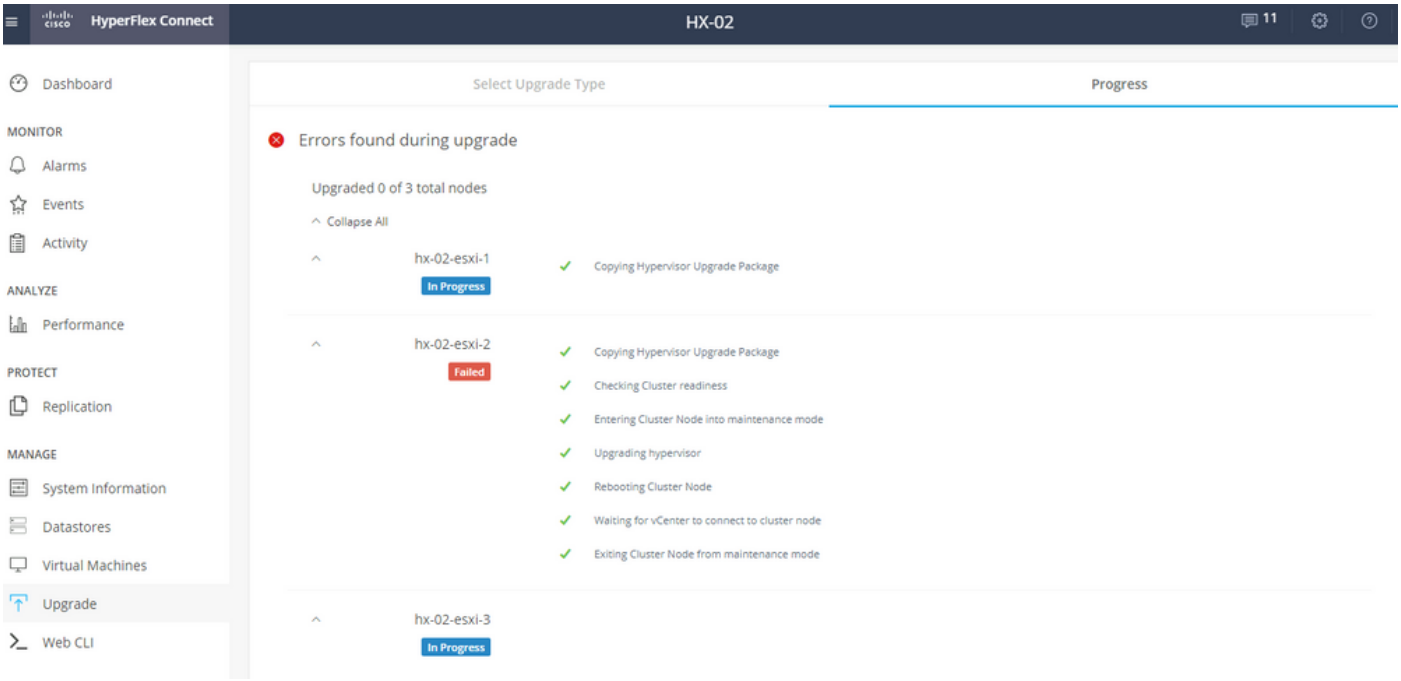
- Systeminformationen auf der HX Connect-Seite
- Upgrades können fehlschlagen mit **"Es konnte keine SSH-Verbindung zum Host hergestellt werden"** oder **mit "Fehler, die während des Upgrades gefunden wurden".**

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





- 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

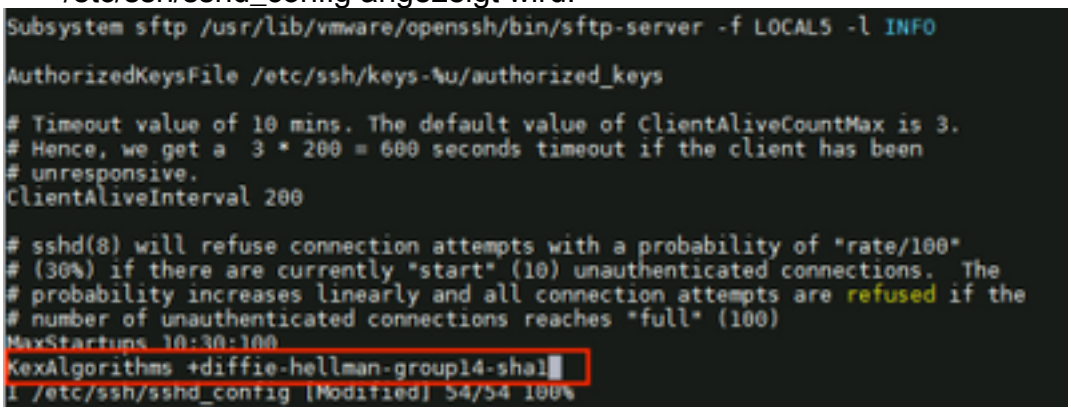
Problemumgehung 2

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.

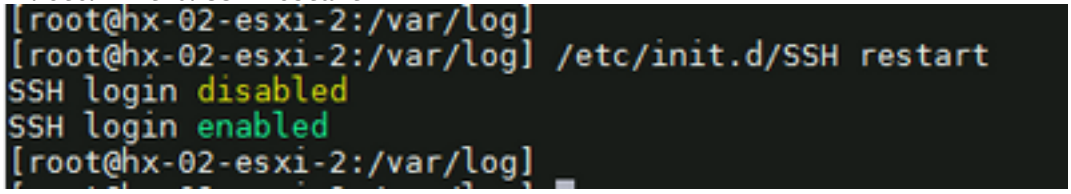
```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

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



- ESXi SSH-Prozess neu starten

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



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