

Incompatibilità SSH con ESXi 6.7P04 (build 17167734) e versioni successive

Sommario

[Introduzione](#)

[Requisiti](#)

[Ulteriori informazioni](#)

[Difetto](#)

[Consulenza software](#)

[Aree interessate](#)

[Soluzione alternativa](#)

[Passi per le soluzioni](#)

[Soluzione 1](#)

[Soluzione 2](#)

Introduzione

Esiste un problema di interoperabilità software tra HXDP [3.5(x), 4.0(x)] ed ESXi 6.7P04 (build 17167734) e versioni successive. I clienti devono evitare questa combinazione software.

NOTA: Questo problema è esteso a qualsiasi versione 6.7 ESXi superiore alla 6.7P04

Il problema di compatibilità è stato risolto in **HXDP 4.0(2e)**. Questo problema non influisce su HXDP 4.5(1a) e versioni successive.

Requisiti

ESXi 6.7P04 (build 17167734) e versioni successive

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

Ulteriori informazioni

Difetto

L'ID bug correlato è [CSCv8204](#) - Problema di interoperabilità ESXi OpenSSH con HXDP

Il problema si verifica in ESXi 6.7P04, a causa dell'aggiornamento della libreria openSSH da parte di VMware a: OpenSSH_8.3p1. Questa nuova versione di OpenSSH rimuove il supporto per il metodo di scambio delle chiavi utilizzato internamente da HXDP durante la comunicazione con ESXi direttamente tramite SSH. Di seguito è riportato un frammento del log delle modifiche OpenSSH che descrive la modifica sostanziale apportata in quella versione:

```
ssh(1), sshd(8): this release removes diffie-hellman-group14-sha1 from the default key exchange
```

proposal for both the client and server.

Consulenza software

Per ulteriori informazioni, fare riferimento a Software Advisory - [Cisco Software Advisory per ESXi 6.7 P04](#)

Aree interessate

Alcune aree funzionali di HX saranno interessate, tra cui:

- Creazione di un nuovo cluster (potrebbe avere esito negativo con **negoziamento dell'algoritmo non riuscita**)

The screenshot shows the Cisco HyperFlex Installer interface. At the top, there is a progress bar with 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 failure. Below the progress bar, there is a section titled 'Errors found during Cluster Creation' with buttons for 'Retry Cluster Creation' and 'Re-Enter Credentials'. The main area displays the 'Cluster Creation - Overall' status as 'Failed'. It lists three failed components: 'VirtCluster' (Algorithm negotiation fail), 'VirtNode' (IP 10.20.3.79), and another 'VirtNode' (IP 10.20.3.80). On the right side, there is a 'Configuration' panel with sections for 'Credentials', 'Server Selection', and 'UCSM Configuration'. The 'Credentials' section shows fields for UCS Manager Host Name, UCS Manager User Name (admin), vCenter Server, User Name (administrator@vsphere.local), and Admin User name (root). The 'Server Selection' section lists three servers (Server 1, 2, 3) with their respective IP addresses and hostnames. The 'UCSM Configuration' section shows fields for VLAN Name (hx-inband-mgmt), VLAN ID (2000), and another VLAN Name (hx-storage-data) with VLAN ID (2100). An 'Edit Configuration' button is visible at the bottom of the configuration panel.

- Espansione del cluster (possibile errore con **negoziamento algoritmo non riuscita**)

The screenshot shows the UCS Manager web interface during a cluster expansion. The main content area is titled 'Cluster Expansion in Progress' and shows a summary for IP 10.21.4.114 with a 'Failed' status. A list of tasks is displayed with their respective statuses: 'Formatting disks' (Failed), 'VirtNode' (Failed), 'JoinCluster' (Success), 'Mgmt Service' (Success), and 'StNode' (In Progress). A sidebar on the right contains configuration details for 'Credentials', 'Cluster Expand Configuration', 'Server Selection', and 'UCSM Configuration'. The 'Credentials' section includes fields for UCS Manager Host Name, UCS Manager User Name (admin), vCenter Server, User Name (administrator@vsphere.local), and Admin User name (root). The 'Cluster Expand Configuration' section includes Management Cluster. The 'Server Selection' section includes Server 4 (HX220C-M5SX). The 'UCSM Configuration' section includes VLAN Name (hx-inband-mgmt).

- Nuova registrazione cluster (la registrazione del cluster stcli potrebbe non riuscire con "Negoziazione algoritmi non riuscita")

```
root@ucsblr1152-svc:~# 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-svc:~#
```

- Pagina delle informazioni di sistema in HX Connect
- Gli aggiornamenti potrebbero non riuscire con i messaggi "Failed to Establish SSH Connection to host" (Impossibile stabilire la connessione SSH all'host) " o "Errori trovati durante l'aggiornamento" (Errori trovati durante l'aggiornamento)

L'upgrade di ESXi non riesce con l'eccezione SSH:

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9] ERRORE
 c.s.sysmgmt.stMgr.SshScpUtilImpl - Impossibile stabilire la connessione SSH all'host: Host non raggiungibile o in modalità di blocco

com.jcraft.jsch.JSchEccezione: Negoziazione algoritmo non riuscita

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	Steps
hx-02-esxi-1	In Progress	Copying Hypervisor Upgrade Package
hx-02-esxi-2	Failed	<ul style="list-style-type: none"> Copying Hypervisor Upgrade Package Checking Cluster readiness Entering Cluster Node into maintenance mode Upgrading hypervisor Rebooting Cluster Node Waiting for vCenter to connect to cluster node Exiting Cluster Node from maintenance mode
hx-02-esxi-3	In Progress	

- Potenzialmente altre aree

Soluzione alternativa

Le note di rilascio di HXDP sono state aggiornate per evidenziare questa versione della versione 6.7 che non è supportata nelle versioni 3.5(x) e 4.0(x). Questo problema è risolto nella patch di HXDP 4.0 - 4.0(2e) e in tutte le versioni 4.5(1a) e successive.

- Utilizzare il meccanismo di rollback incorporato in ESXi per ripristinare una versione ESXi compatibile.
- Un'altra soluzione possibile è riabilitare il metodo di scambio delle chiavi rimosso aggiornando sshd_config su ciascun host ESXi e riavviando il servizio SSH. Si consiglia di implementare questa soluzione solo temporaneamente.

NOTA: l'obiettivo dovrebbe essere quello di spostare il cluster in una versione HXDP fissa e rimuovere questa soluzione non appena possibile. I cluster non devono rimanere in questo stato a lungo termine con questa impostazione di algoritmo a chiave aggiuntiva aggiunta a sshd_config.

Passi per le soluzioni

Se non è possibile aggiornare HXDP a una versione fissa, utilizzare le seguenti soluzioni alternative:

Soluzione 1

- Utilizzare il meccanismo di rollback incorporato in ESXi per ripristinare una versione ESXi compatibile. Consultare la Knowledge Base di vmware - <https://kb.vmware.com/s/article/1033604>

Soluzione 2

Riabilitare il metodo di scambio delle chiavi rimosso aggiornando sshd_config su ciascun host ESXi e riavviando il servizio SSH.

- Aggiungere +diffie-hellman-group14-sha1 agli algoritmi Kex sotto /etc/ssh/sshd_config su ciascun host ESXi

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

- Confermare che **KexAlgorithms +diffie-hellman-group14-sha1** sia visualizzato in /etc/ssh/sshd_config

```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCALS -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
1 /etc/ssh/sshd_config [Modified] 54/54 100%
```

- Riavviare il processo ESXi SSH

```
# /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]
```

- Riavviare o riprendere il flusso di lavoro precedentemente non riuscito.