

Incompatibilidade SSH com ESXi 6.7P04 (build 17167734) e posterior

Contents

[Introduction](#)

[Requirements](#)

[Mais informações](#)

[Defeito](#)

[Consultoria de software](#)

[Áreas afetadas](#)

[Solução](#)

[Etapas para soluções alternativas](#)

[Solução 1](#)

[Solução 2](#)

Introduction

Existe um problema de interoperabilidade de software entre HXDP [3.5(x), 4.0(x)] e ESXi 6.7P04 (build 17167734) e posterior. Os clientes devem evitar essa combinação de software.

NOTE: Este problema é estendido para qualquer versão 6.7 do ESXi acima de 6.7P04

O problema de compatibilidade foi resolvido no **HXDP 4.0(2e)**. Esse problema não afeta o HXDP 4.5(1a) e posterior.

Requirements

ESXi 6.7P04 (build 17167734) e posterior

Versão HXDP - 3.5(x), 4.0(x)

Mais informações

Defeito

O ID do bug relacionado é [CSCvv88204](#) - Problema de interoperabilidade do ESXi OpenSSH com HXDP

O problema ocorre no ESXi 6.7P04, devido à atualização da VMware da biblioteca openSSH para: OpenSSH_8.3p1. Essa nova versão do OpenSSH remove o suporte para o método de troca de chaves usado internamente pelo HXDP ao se comunicar diretamente com o ESXi via SSH. Abaixo está um trecho do registro de alterações do OpenSSH que descreve a alteração de quebra feita nessa versão:

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

Consultoria de software

Consulte o Software Advisory para obter mais detalhes - [Cisco Software Advisory for ESXi 6.7 P04](#)

Áreas afetadas

Algumas áreas funcionais do HX serão afetadas, incluindo:

- Nova criação de cluster (pode falhar com **falha na negociação de algoritmo**)

The screenshot displays the Cisco HyperFlex Installer web interface. At the top, a progress bar shows the installation 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 states 'Errors found during Cluster Creation' with buttons for 'Retry Cluster Creation' and 'Re-Enter Credentials'. The main content area shows a detailed view of the 'Cluster Creation - Overall' status, which is 'Failed'. The error details are as follows:

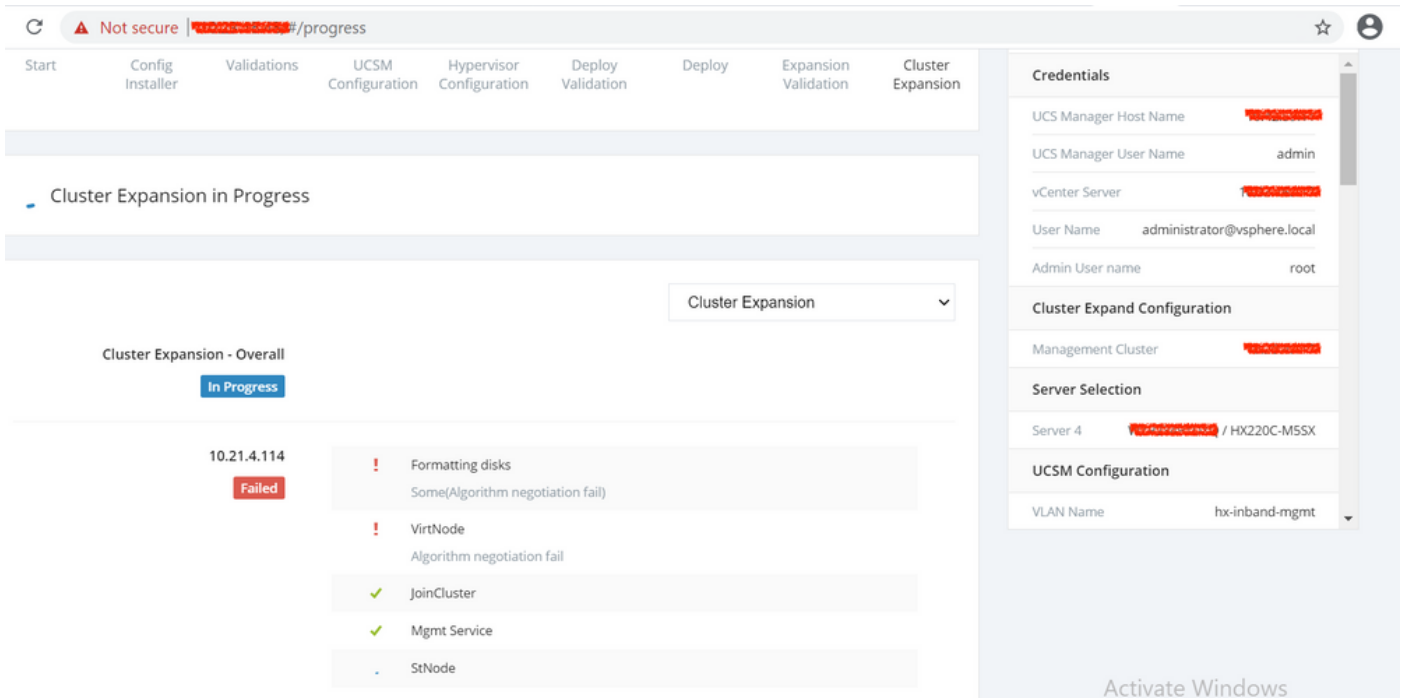
Component	Status	Message
VirtCluster	Failed	Algorithm negotiation fail
Configuring Cluster Resource Manager	Success	
Preparing Storage Cluster	In Progress	

Below this, the status for individual nodes is shown:

IP Address	Component	Status
10.20.3.79	VirtNode	Failed
10.20.3.80	VirtNode	Failed

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

- Expansão do cluster (pode falhar com **falha na negociação do algoritmo**)



- Registro de cluster reregistrado (o registro de cluster stcli pode falhar com "Falha na negociação de algoritmo")

```
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:~#
```

- Página de informações do sistema no HX Connect
- As atualizações podem falhar com "Falha ao estabelecer conexão SSH com o host" ou "Erros encontrados durante a atualização"

Falha na atualização do ESXi com exceção de SSH-

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9] ERRO c.s.sysmgmt.stMgr.SshScpUtilImpl - Falha ao estabelecer conexão SSH com o host: O host não pode ser alcançado ou está no modo de bloqueio

com.jcraft.jsch.JSchException: Falha na negociação do algoritmo

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	

- Potencialmente outras áreas

Solução

As notas de versão do HXDP foram atualizadas para chamar especificamente esta versão do 6.7 que não é suportada nas versões 3.5(x) e 4.0(x). Esse problema é corrigido no patch HXDP 4.0 - 4.0(2e) e em todas as versões 4.5(1a) e posteriores.

- Use o mecanismo de reversão integrado ao ESXi para reverter para uma versão compatível do ESXi.
- Outra solução possível é reativar o método de troca de chaves removido atualizando sshd_config em cada host ESXi e reiniciando o serviço SSH. Recomenda-se que essa solução seja implementada apenas temporariamente.

NOTA: o objetivo deve ser mover o cluster para uma versão HXDP fixa e remover essa solução o mais rápido possível. Os clusters não devem permanecer nesse estado a longo prazo com essa configuração extra de algoritmo de chave adicionada a sshd_config.

Etapas para soluções alternativas

Se você não puder atualizar o HXDP para uma versão fixa, use as seguintes soluções alternativas -

Solução 1

- Use o mecanismo de reversão integrado ao ESXi para reverter para uma versão compatível do ESXi. Consulte o KB do vmware - <https://kb.vmware.com/s/article/1033604>

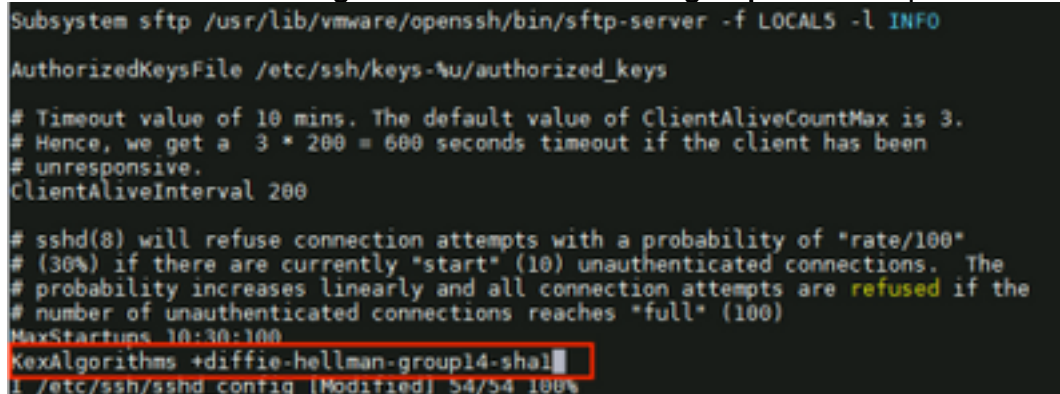
Solução 2

Reative o método de troca de chaves removido atualizando sshd_config em cada host ESXi e reiniciando o serviço SSH.

- Adicione +diffie-hellman-group14-sha1 aos KexAlgorithms em /etc/ssh/sshd_config em cada host ESXi

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

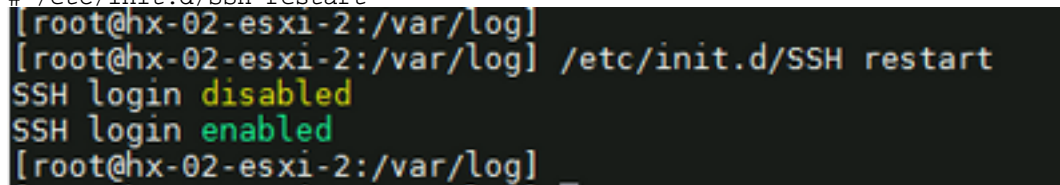
- Confirme se **KexAlgorithms +diffie-hellman-group14-sha1** aparece no /etc/ssh/sshd_config



```
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
1 /etc/ssh/sshd_config [Modified] 54/54 100%
```

- Reiniciar o processo SSH ESXi

```
# /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]
```

- Reinicie ou reinicie o fluxo de trabalho com falha anterior.