

Incompatibilité SSH avec ESXi 6.7P04 (build 17167734) et versions ultérieures

Contenu

[Introduction](#)

[Conditions requises](#)

[Plus d'informations](#)

[Défaillance](#)

[Conseils logiciels](#)

[Zones touchées](#)

[Solution de contournement](#)

[Étapes de contournement](#)

[Solution 1](#)

[Solution 2](#)

Introduction

Un problème d'interopérabilité logicielle existe entre HXDP [3.5(x), 4.0(x)] et ESXi 6.7P04 (build 17167734) et versions ultérieures. Les clients doivent éviter cette combinaison de logiciels.

NOTE: Ce problème est étendu à toute version 6.7 ESXi supérieure à 6.7P04

Le problème de compatibilité est résolu dans **HXDP 4.0(2e)**. Ce problème n'a pas d'impact sur HXDP 4.5(1a) et versions ultérieures.

Conditions requises

ESXi 6.7P04 (build 17167734) et ultérieur

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

Plus d'informations

Défaillance

L'ID de bogue associé est [CSCvv88204](#) - Problème d'interopérabilité ESXi OpenSSH avec HXDP

Le problème se produit dans ESXi 6.7P04, en raison de la mise à niveau de VMware de la bibliothèque openSSH vers : OpenSSH_8.3p1. Cette nouvelle version d'OpenSSH supprime la prise en charge de la méthode d'échange de clés utilisée en interne par HXDP lors de la communication à ESXi directement via SSH. Ci-dessous, un extrait du fichier de modifications OpenSSH décrivant les changements de rupture effectués dans cette version :

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

proposal for both the client and server.

Conseils logiciels

Référez-vous à Software Advisory pour plus de détails - [Cisco Software Advisory pour ESXi 6.7 P04](#)

Zones touchées

Certains aspects fonctionnels de HX seront touchés, notamment :

- Nouvelle création de cluster (peut échouer avec **échec de négociation d'algorithme**)

The screenshot shows the HyperFlex Installer interface. At the top, a progress bar indicates the following 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 summary of the failed cluster creation process. It shows 'Cluster Creation - Overall' as 'Failed'. The error details are as follows:

IP Address	Component	Status	Message
	VirtCluster	Failed	Algorithm negotiation fail
	Configuring Cluster Resource Manager	Success	
	Preparing Storage Cluster	In Progress	
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, 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).

- Extension de cluster (peut échouer avec **échec de négociation d'algorithme**)

Cluster Expansion in Progress

Cluster Expansion - Overall

In Progress

IP Address	Task Name	Status	Message
10.21.4.114	Formatting disks	Failed	Some(Algorithm negotiation fail)
	VirtNode	Failed	Algorithm negotiation fail
	JoinCluster	In Progress	
	Mgmt Service	In Progress	
	StNode	In Progress	

Cluster Expand Configuration

Management Cluster

Server Selection

Server 4 / HX220C-M5SX

UCSM Configuration

VLAN Name: hx-inband-mgmt

- Réinscription de cluster (échec de la **négociation d'algorithme** dans le Registre de cluster stcli)

```
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:~#
```

- Page Informations système de HX Connect
- Les mises à niveau peuvent échouer avec « **Échec de l'établissement de la connexion SSH à l'hôte** » ou « **Erreurs détectées lors de la mise à niveau** »

Échec de la mise à niveau ESXi avec ssh exception-

2020-12-16-10:31:04.675 [vmware-upgrade-pool-9] ERROR
 c.s.systemgmt.stMgr.SshScpUtilImpl - Échec de l'établissement de la connexion SSH à l'hôte :
 L'hôte n'est pas accessible ou en mode de verrouillage

com.jcraft.jsch.JSchException : Echec de la négociation d'algorithme

- Autres zones potentiellement

Solution de contournement

Les notes de version HXDP ont été mises à jour pour indiquer spécifiquement que cette version de 6.7 n'est pas prise en charge sur les versions 3.5(x) et 4.0(x). Ce problème est corrigé dans le patch HXDP 4.0 - 4.0(2e) et dans toutes les versions 4.5(1a) et ultérieures.

- Utilisez le mécanisme de restauration intégré à ESXi pour revenir à une version compatible ESXi.
- Une autre solution possible consiste à réactiver la méthode d'échange de clés supprimée en mettant à jour `sshd_config` sur chaque hôte ESXi et en redémarrant le service SSH. Il est recommandé que cette solution ne soit mise en oeuvre que temporairement.

REMARQUE : l'objectif doit être de déplacer le cluster vers une version HXDP fixe et de supprimer cette solution dès que possible. Les clusters ne doivent pas rester dans cet état à long terme avec ce paramètre d'algorithme de clé supplémentaire ajouté à `sshd_config`.

Étapes de contournement

Si vous ne parvenez pas à mettre à niveau HXDP vers une version fixe, procédez comme suit :

Solution 1

- Utilisez le mécanisme de restauration intégré à ESXi pour revenir à une version compatible ESXi. Référez-vous à la Ko vmware - <https://kb.vmware.com/s/article/1033604>

Solution 2

Réactivez la méthode d'échange de clés supprimée en mettant à jour sshd_config sur chaque hôte ESXi et en redémarrant le service SSH.

- Ajoutez +diffie-hellman-group14-sha1 aux algorithmes KexAlgorithms sous /etc/ssh/sshd_config sur chaque hôte ESXi

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

- Confirmez que **KexAlgorithms +diffie-hellman-group14-sha1** apparaît dans le fichier /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%
```

- Redémarrer le processus 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]
```

- Redémarrer ou reprendre le workflow précédemment échoué.