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

Table des matières

- Introduction
  - Exigences
  - Plus d'informations
    - Défaillance
    - Conseil logiciel
- Zones impactées
- 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 logicielle.

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'affecte pas HXDP 4.5(1a) et versions ultérieures.

Exigences

ESXi 6.7P04 (build 17167734) et versions ultérieures

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

Plus d'informations

Défaillance

L'ID de bogue associé est CSCv88204 - Problème d'interopérabilité ESXi OpenSSH avec HXDP

Le problème se produit dans ESXi 6.7P04, en raison de la mise à niveau 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 avec ESXi directement via SSH. Voici un extrait du changelog d'OpenSSH décrivant la modification de rupture effectuée dans cette version :

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

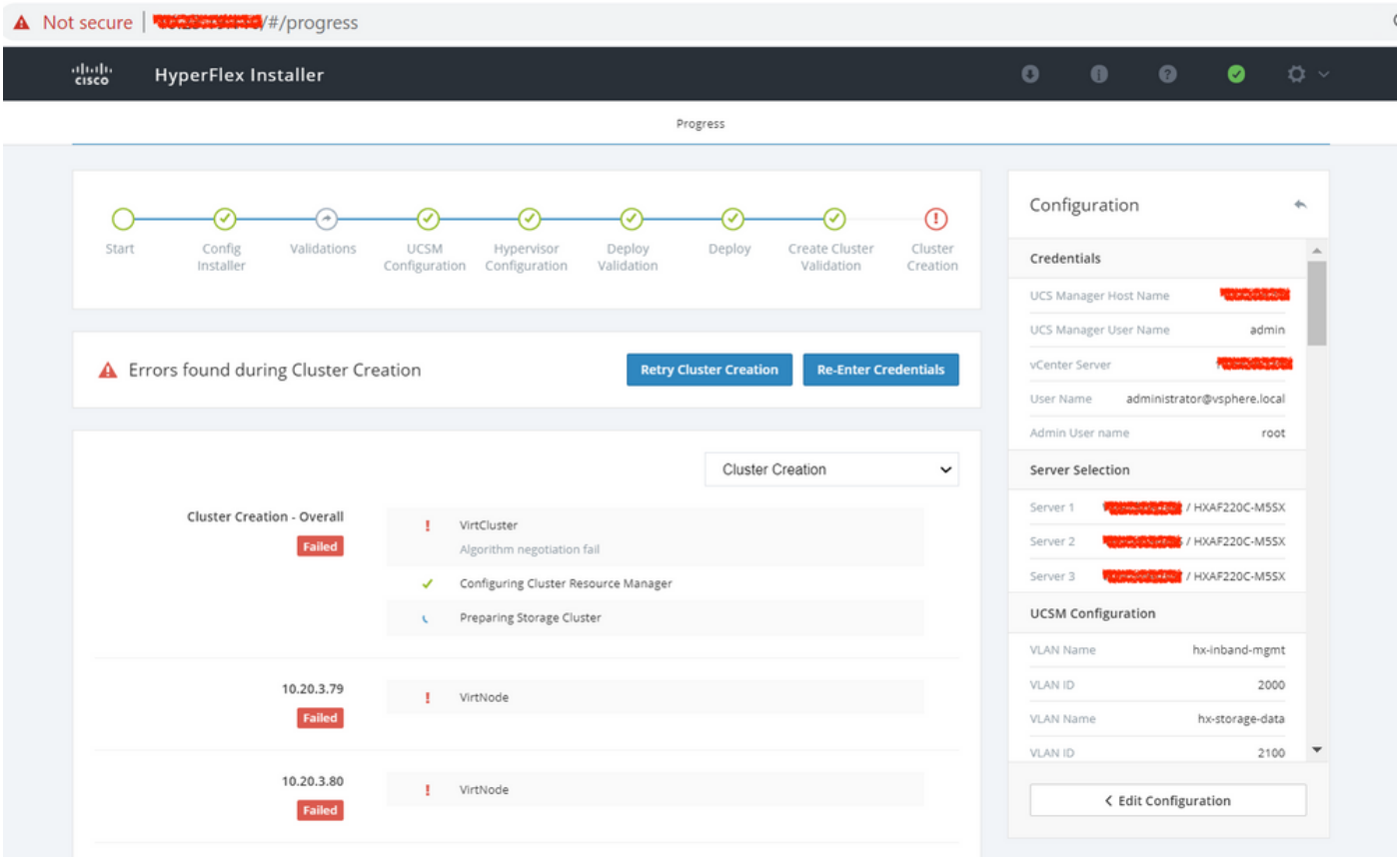
Conseil logiciel

Consultez Software Advisory pour plus de détails - [Cisco Software Advisory for ESXi 6.7 P04]

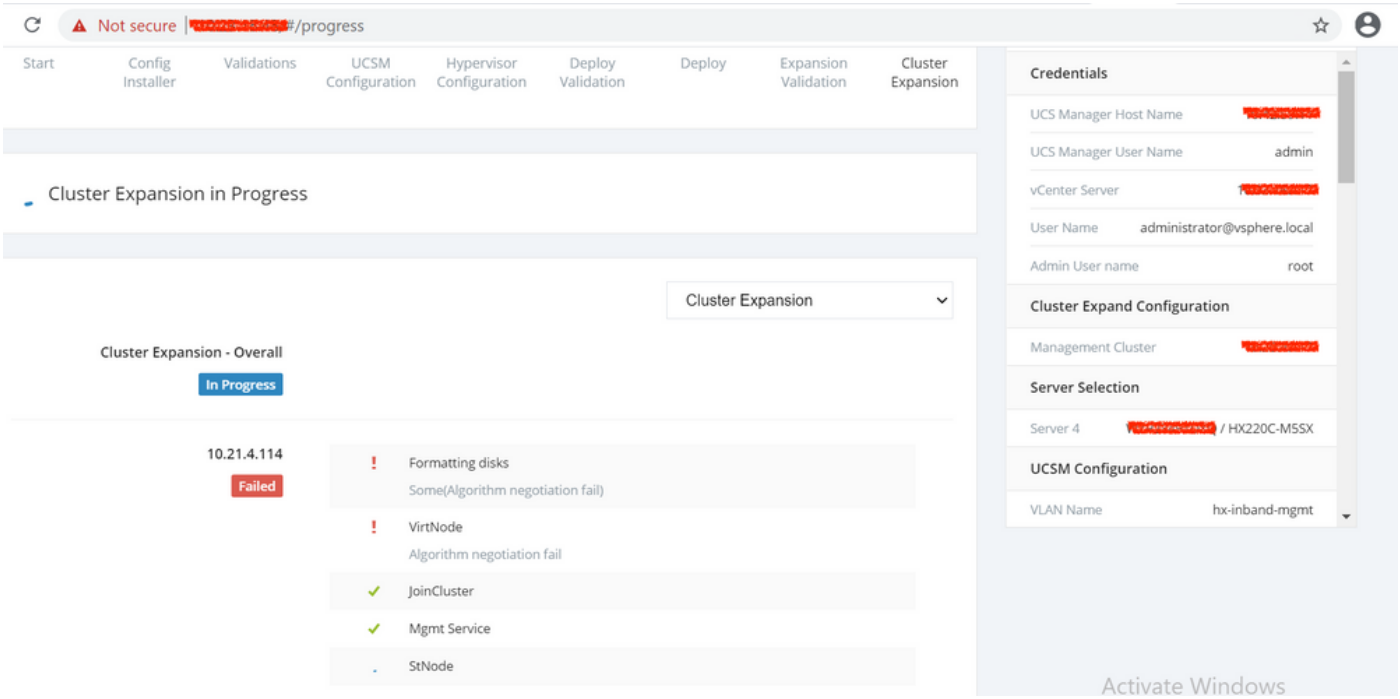
Zones impactées

Certains domaines fonctionnels de HX seront touchés, notamment :

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



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



- Réenregistrement de cluster (le réenregistrement de cluster stcli peut échouer avec "Échec de la négociation d'algorithme")

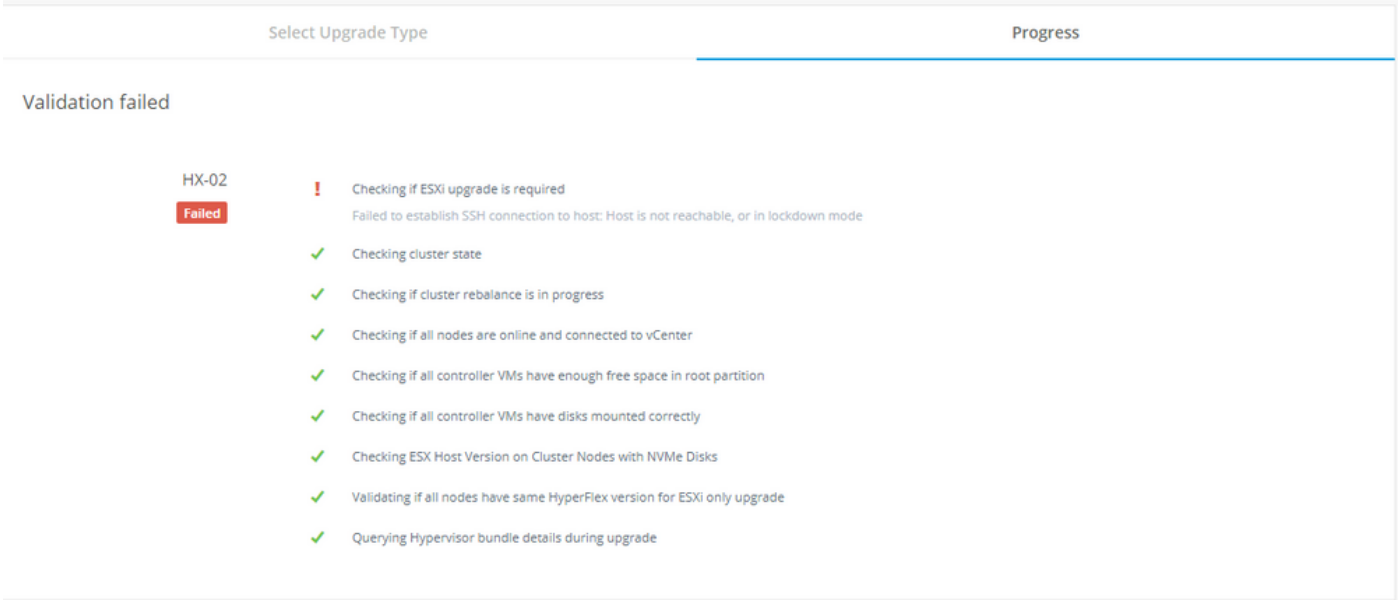
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration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

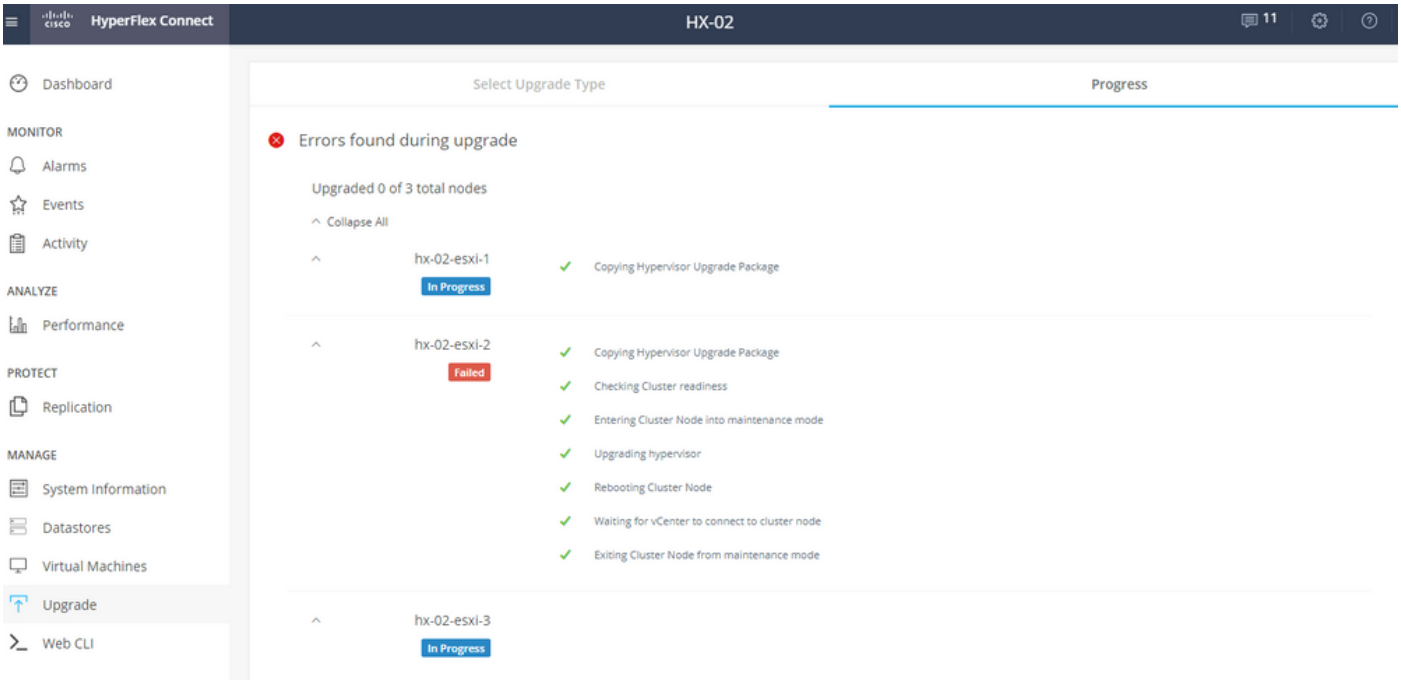
- Page d'informations système dans HX Connect
- Les mises à niveau peuvent échouer avec "Failed to Establishment SSH Connection to host" ou "Errors found during upgrade"

La mise à niveau ESXi échoue avec une exception ssh-

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

com.jcraft.jsch.JSchException : Échec de la négociation algorithmique





- Potentiellement d'autres domaines

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 correctif 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 ESXi compatible.
- Une autre solution de contournement 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 de contournement ne soit implémentée que temporairement.

REMARQUE : l'objectif doit être de déplacer le cluster vers une version HXDP fixe et de supprimer cette solution de contournement 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, utilisez les solutions de contournement suivantes :

Solution 1

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

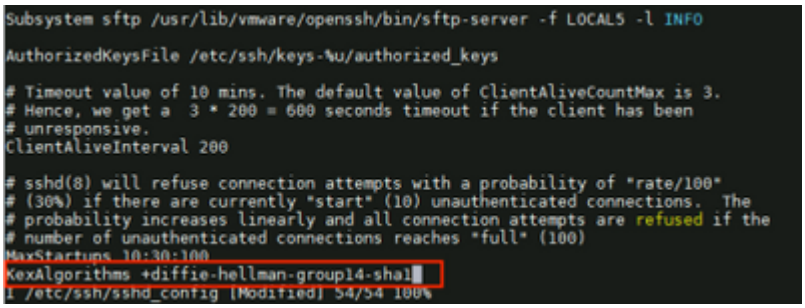
Solution 2

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 KexAlgorithms sous /etc/ssh/sshd_config sur chaque hôte ESXi

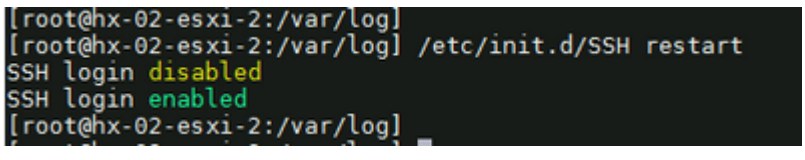
```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

- Vérifiez que KexAlgorithms +diffie-hellman-group14-sha1 s'affiche dans /etc/ssh/sshd_config



- Redémarrer le processus ESXi SSH

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



- Redémarrez ou reprenez le workflow précédemment en échec.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.