ESXi 6.7P04(ビルド17167734)以降とのSSH非互換性

内容

概要

HXDP [3.5(x), 4.0(x)]とESXi 6.7P04(ビルド17167734)以降の間にソフトウェアの相互運用性の問題があります。 このソフトウェアの組み合わせは避けてください。

注：この問題は、6.7P04以降の6.7 ESXiバージョンに拡張されています

互換性の問題は**HXDP 4.0(2e)で解決されています。** この問題は、HXDP 4.5(1a)以降には影響しません。

要件

ESXi 6.7P04(ビルド17167734)以降

HXDPバージョン – 3.5(x)、4.0(x)

その他の情報

Defect

関連するバグIDは [CSCvv88204](#) - **HXDPとのESXi OpenSSH相互運用性の問題**

この問題は、VMwareがOpenSSHライブラリをOpenSSH_8.3p1にアップグレードしたためにESXi 6.7P04で発生します。この新しいバージョンのOpenSSHでは、SSHを介してESXiとの通信するときに内部で内部使用キー交換方式がをを使用サポートするをサポートするを削除します。次に、OpenSSHの変更ログからのスニペットを示します。このバージョンで行われた変更を説明しています。

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

proposal for both the client and server.

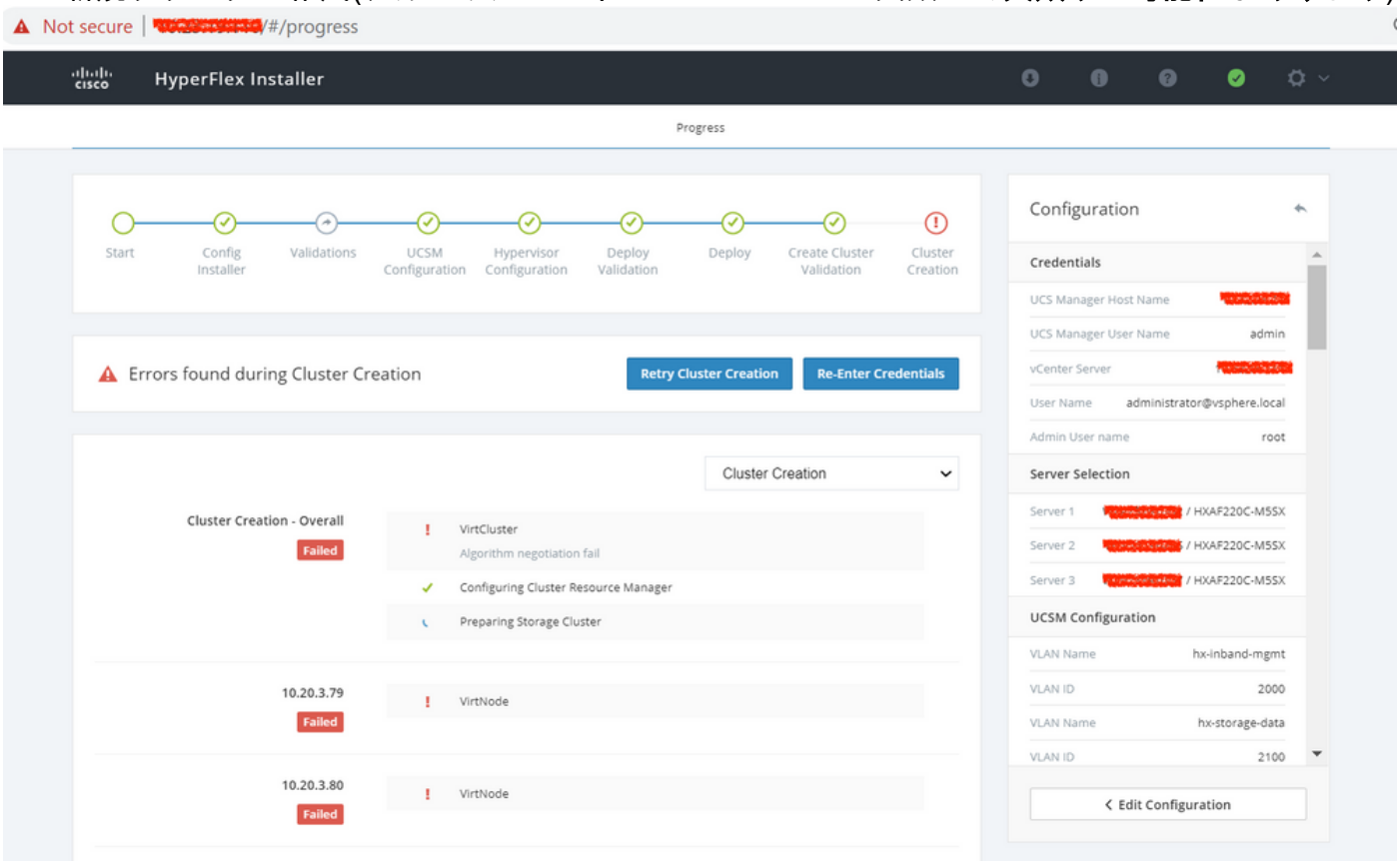
ソフトウェアアドバイザリ

詳細については、ソフトウェアアドバイザリを参照してください – ESXi 6.7 P04向けシスコソフトウェアアドバイザリ

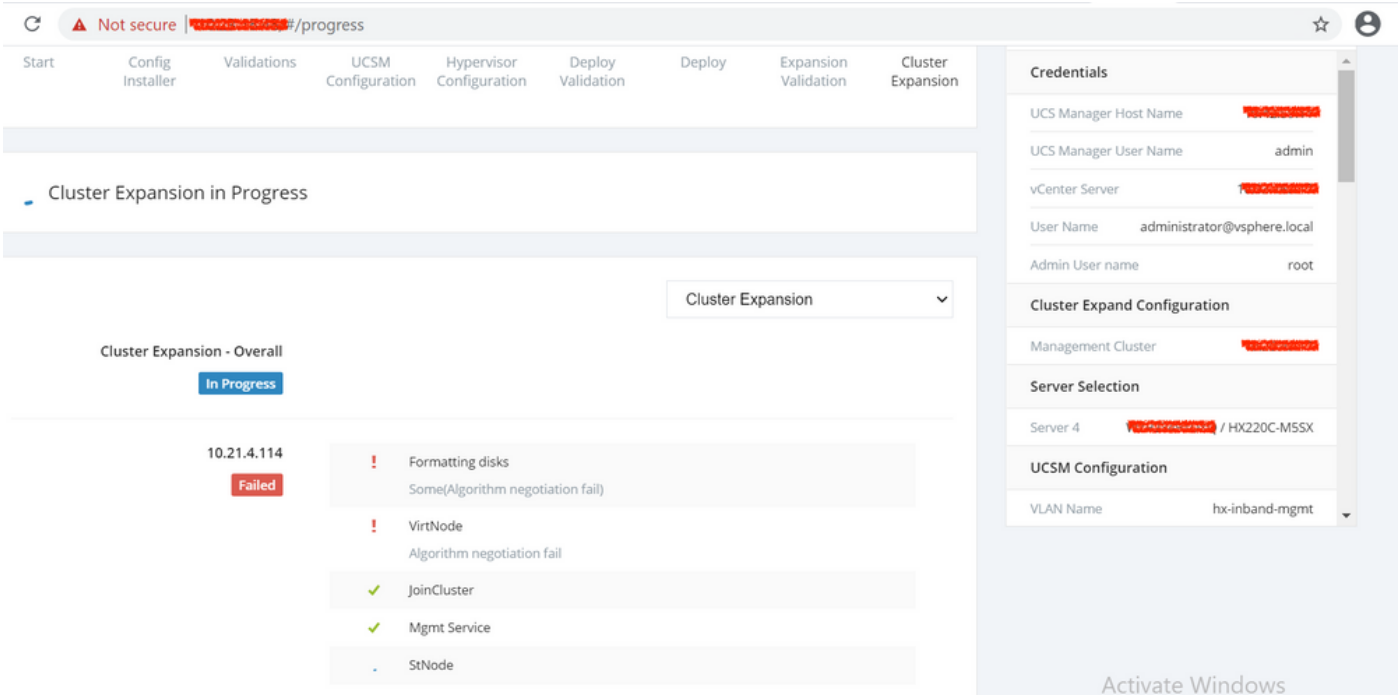
影響を受けるエリア

HXの一部の機能領域には、次のような影響があります。

- 新規クラスタの作成(アルゴリズムのネゴシエーションが失敗して**失敗する可能性があります**)



- クラスタの拡張(アルゴリズムのネゴシエーションが**失敗した場合があります**)



- クラスタの再登録(stcliクラスタの再登録が「アルゴリズムネゴシエーションが失敗する」で失敗する場合がある)

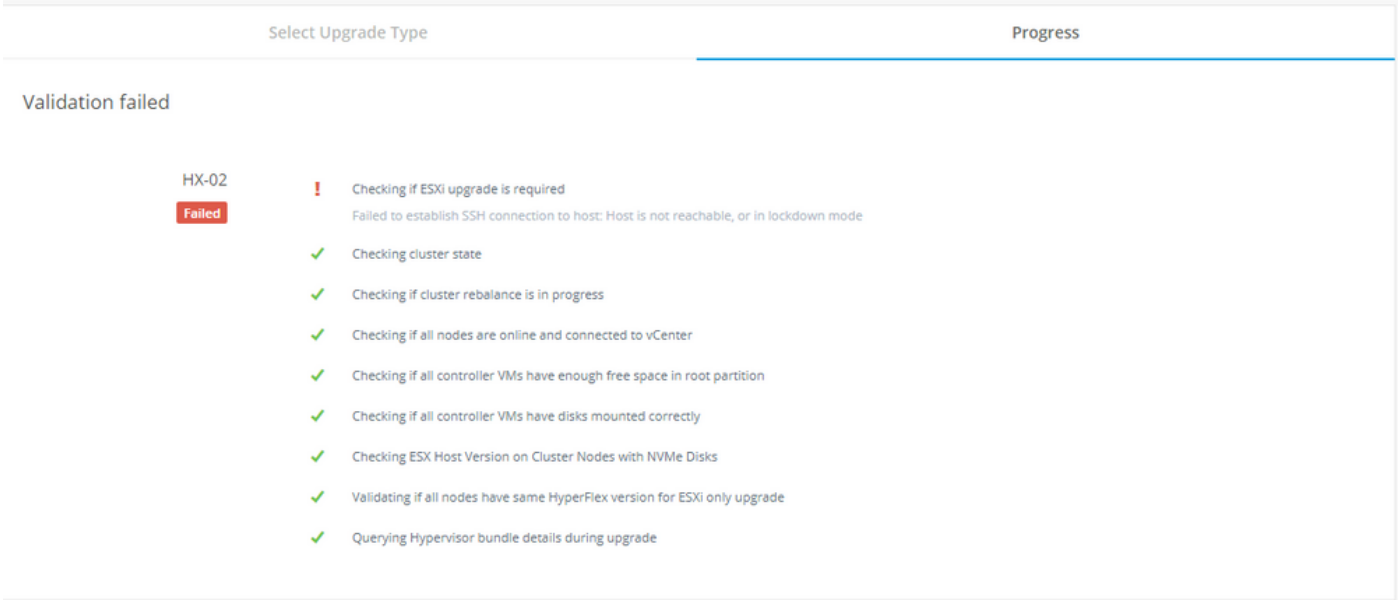
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration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

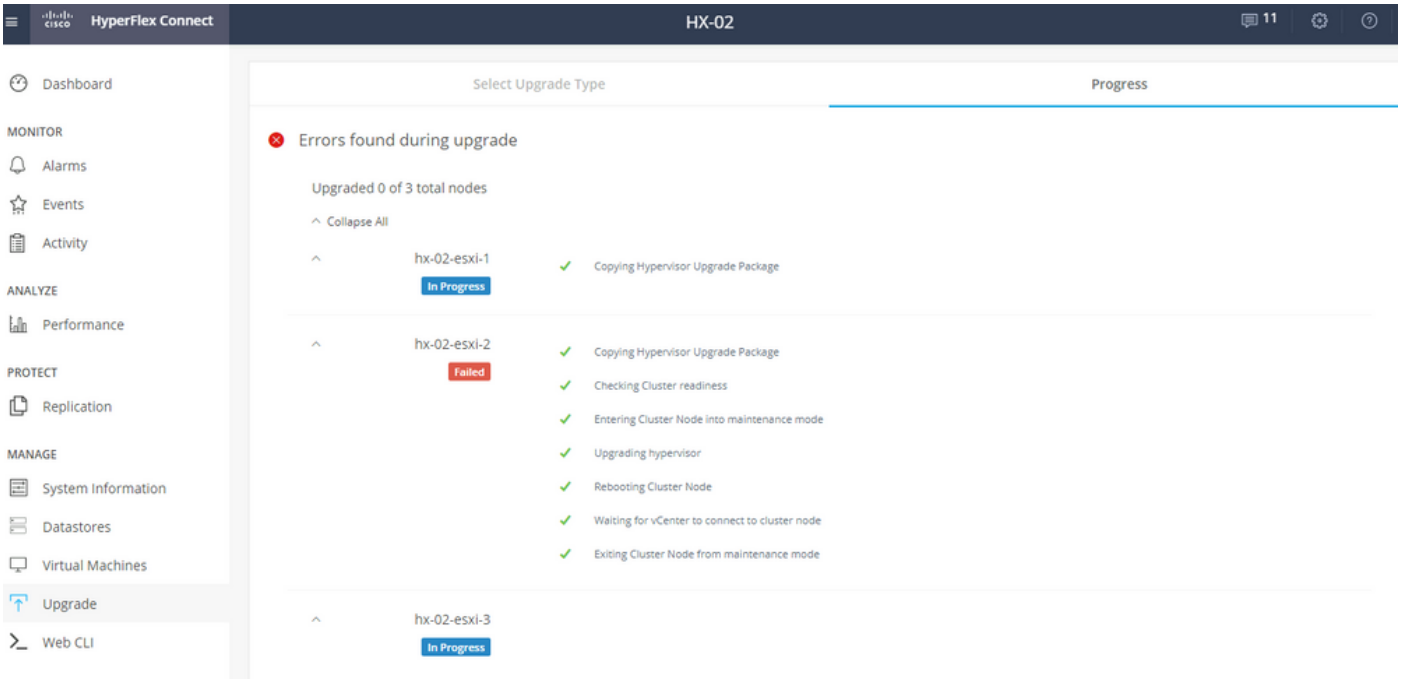
- HX Connectのシステム情報ページ
- 「Failed to **Establish SSH Connection to host**」または「**Errors found during upgrade**」でアップグレードが失敗する場合があります

ESXiアップグレードがssh例外で失敗する

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9] ERROR c.s.sysmgmt.stMgr.SshScpUtilImpl - Failed to establish SSH connection to host:ホストに到達できないか、ロックダウンモードです

com.jcraft.jsch.JSchException:アルゴリズムのネゴシエーションが失敗する





- 潜在的に他の領域

回避策

HXDPリリースノートは、3.5(x)および4.0(x)リリースではサポートされていない6.7のこのバージョンを具体的に説明するように更新されています。この問題は、HXDP 4.0パッチ – 4.0(2e)および4.5(1a)以降のすべてのリリースで修正されています。

- 互換性のあるESXiバージョンにロールバックするには、ESXiに組み込まれたロールバックメカニズムを使用します。
- 別の回避策として、削除したキー交換方式を再度有効にし、各ESXiホストのsshd_configを更新してSSHサービスを再起動する方法があります。この回避策は一時的にのみ実装することを推奨します。

注：目的は、クラスタを固定HXDPリリースに移動し、できるだけ早くこの回避策を削除することです。sshd_configに追加されたこの追加キーアルゴリズム設定では、クラスタは長期間この状態を維持しないでください。

回避策の手順

HXDPを修正済みリリースにアップグレードできない場合は、次の回避策を使用します。

回避策 1

- 互換性のあるESXiバージョンにロールバックするには、ESXiに組み込まれたロールバックメカニズムを使用します。VMware KBを参照：https://kb.vmware.com/s/article/1033604

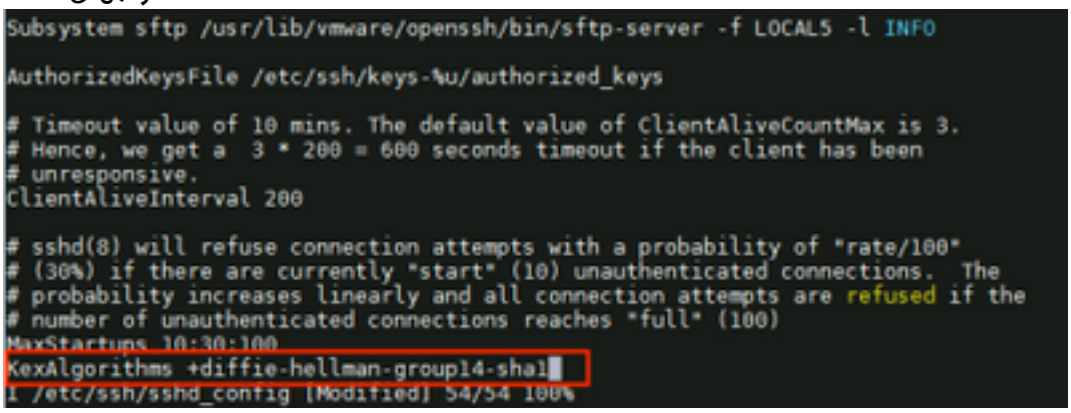
回避策 2

各ESXiホストのsshd_configを更新し、SSHサービスを再起動して、削除したキー交換方式を再度有効にします。

- 各ESXiホストの/etc/ssh/sshd_configの下のKexAlgorithmsに+diffie-hellman-group14-sha1を追加します

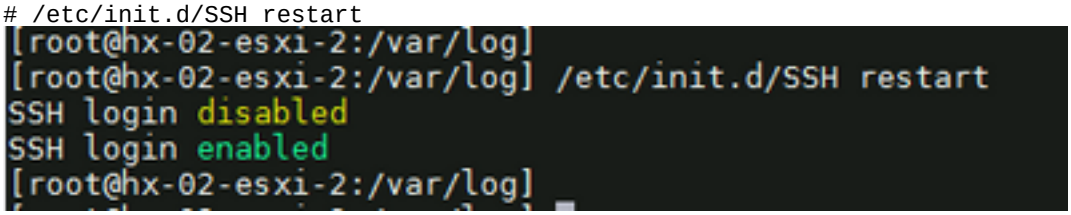
```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

- **KexAlgorithms +diffie-hellman-group14-sha1**が/etc/ssh/sshd_configに表示されることを確認します



- ESXi SSHプロセスの再起動

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



- 以前に失敗したワークフローを再起動または再開します。