SSH与ESXi 6.7P04(内部版本17167734)及更高版本不兼容

目录

简介

HXDP [3.5(x), 4.0(x)]和ESXi 6.7P04(内部版本17167734)及更高版本之间存在软件互操作性问题。 客户应避免此软件组合。

NOTE:此问题扩展至6.7P04以上的任何6.7 ESXi版本

HXDP 4.0(2e)中**解决了兼容性问题。** 此问题不影响HXDP 4.5(1a)及更高版本。

要求

ESXi 6.7P04(内部版本17167734)及更高版本

HXDP版本 — 3.5(x)、4.0(x)

更多信息

缺陷

相关漏洞ID为 CSCv88204 - **ESXi OpenSSH与HXDP的互操作性问题**

ESXi 6.7P04中出现此问题，原因是VMware将openSSH库升级为：OpenSSH_8.3p1。此新版本的OpenSSH将取消对HXDP在通过SSH直接与ESXi通信时内部使用的密钥交换方法的支持。以下是OpenSSH更改日志中描述该版本中所做的中断更改的片段：

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

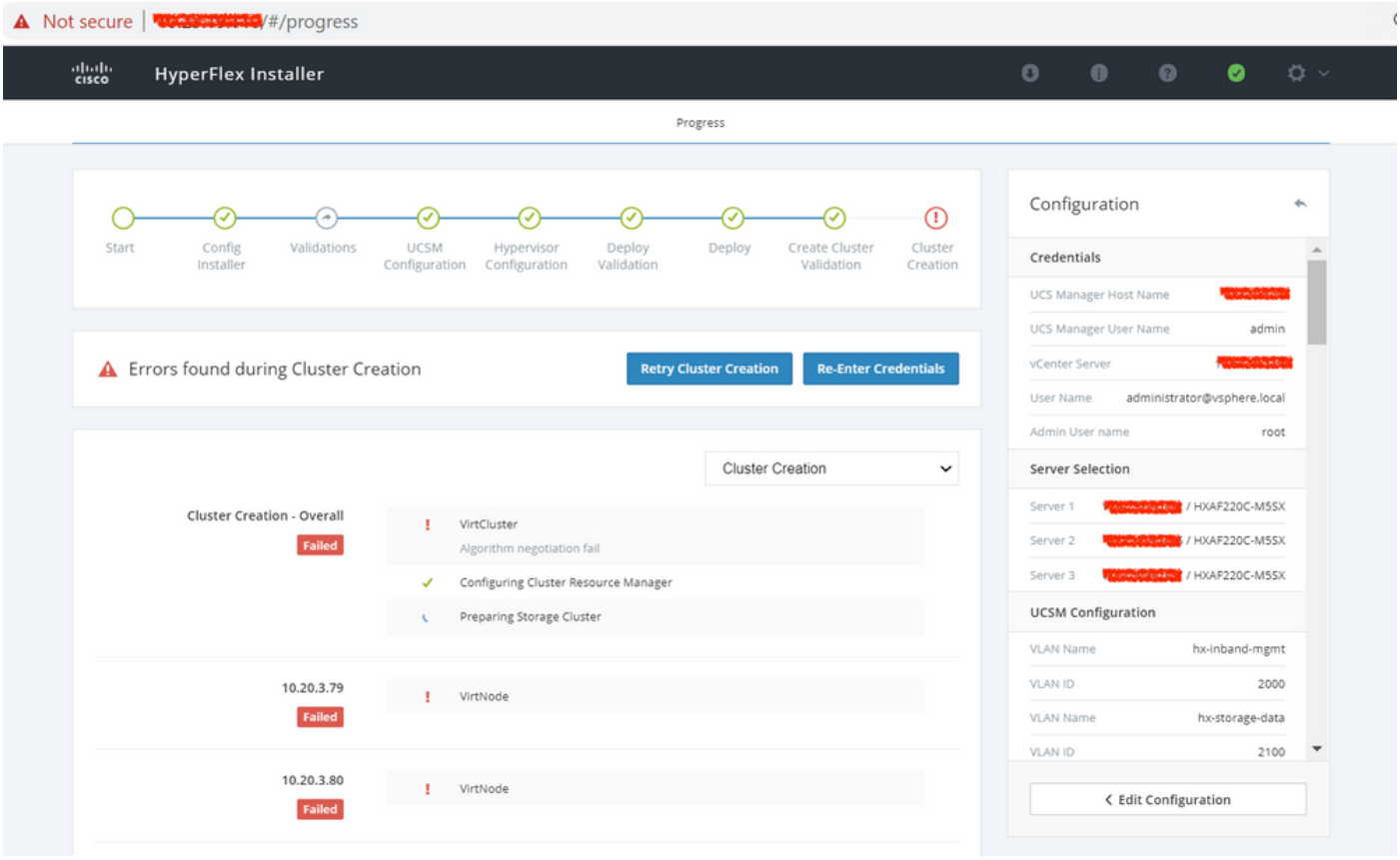
软件咨询

有关详细信息，请参阅软件[咨询 — 适用于ESXi 6.7 P04的思科软件咨询]

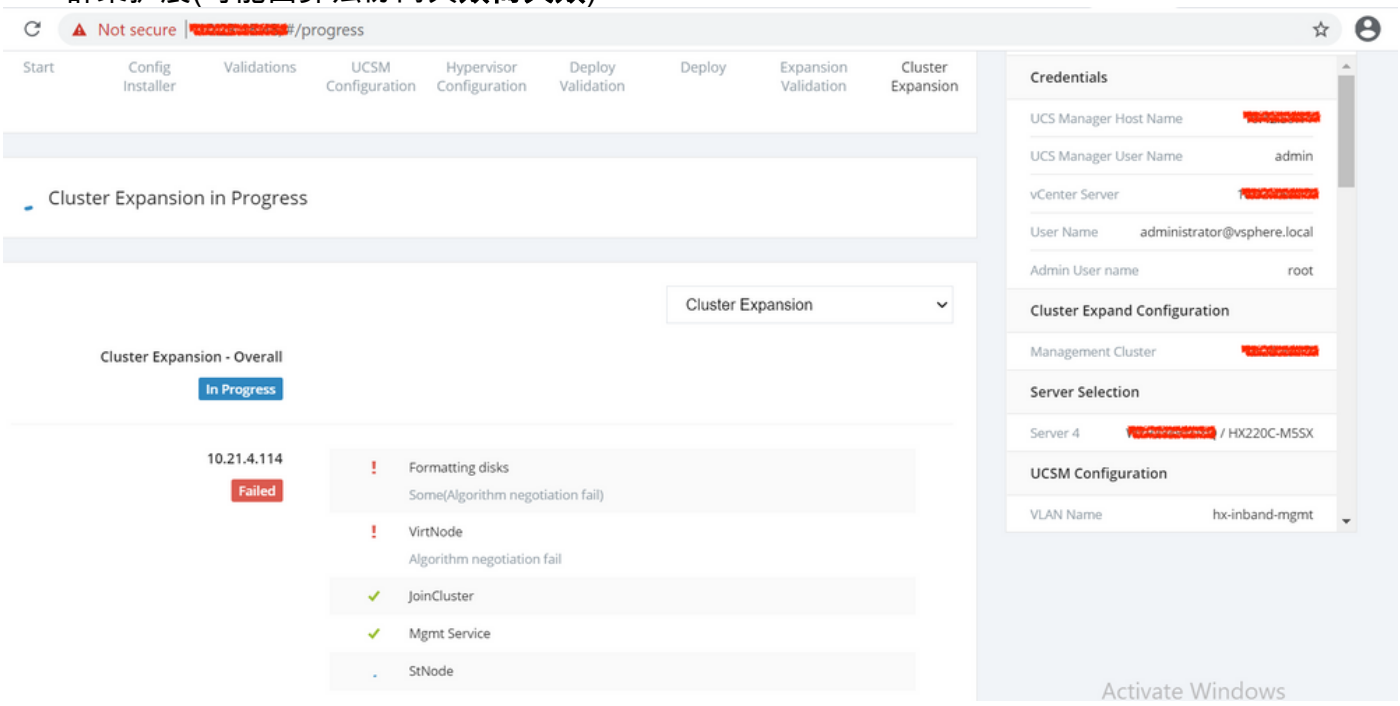
受影响区域

HX的一些功能领域将受到影响，包括：

- 新群集创建(可能因算法协商失**败而失败**)



- 群集扩展(可能因算法协商失**败而失败**)



- 集群重注册(stcli集群重注册可能因“算**法协商失败”而失败**)

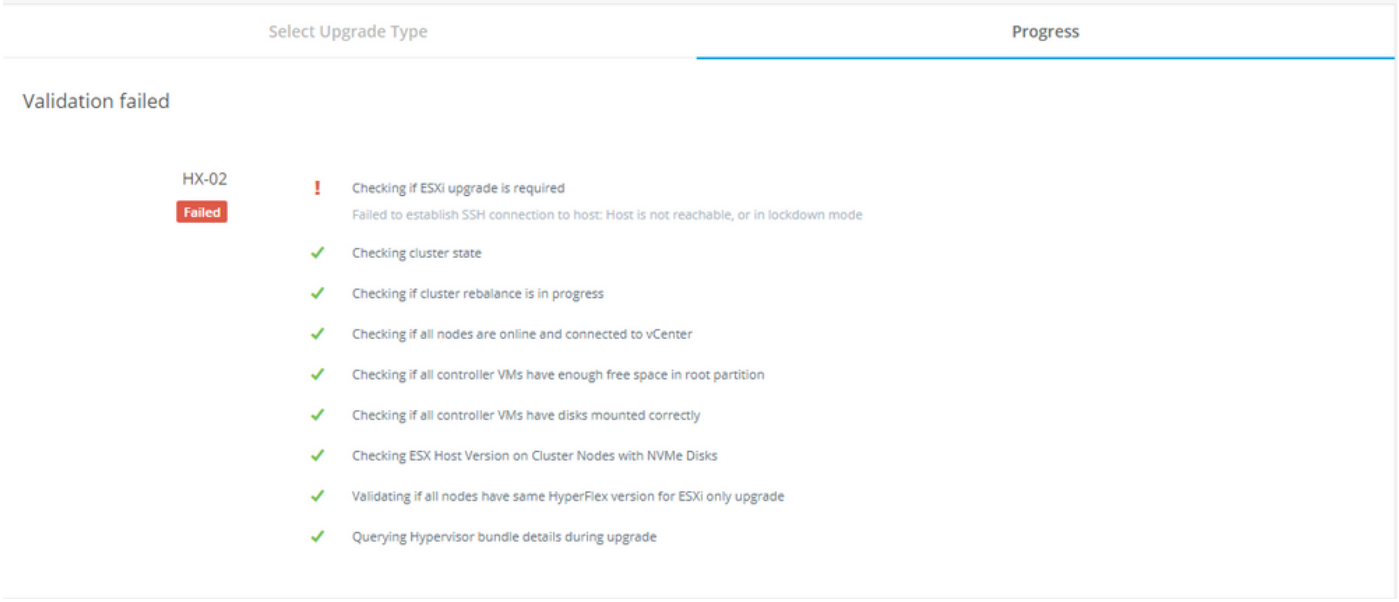
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration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

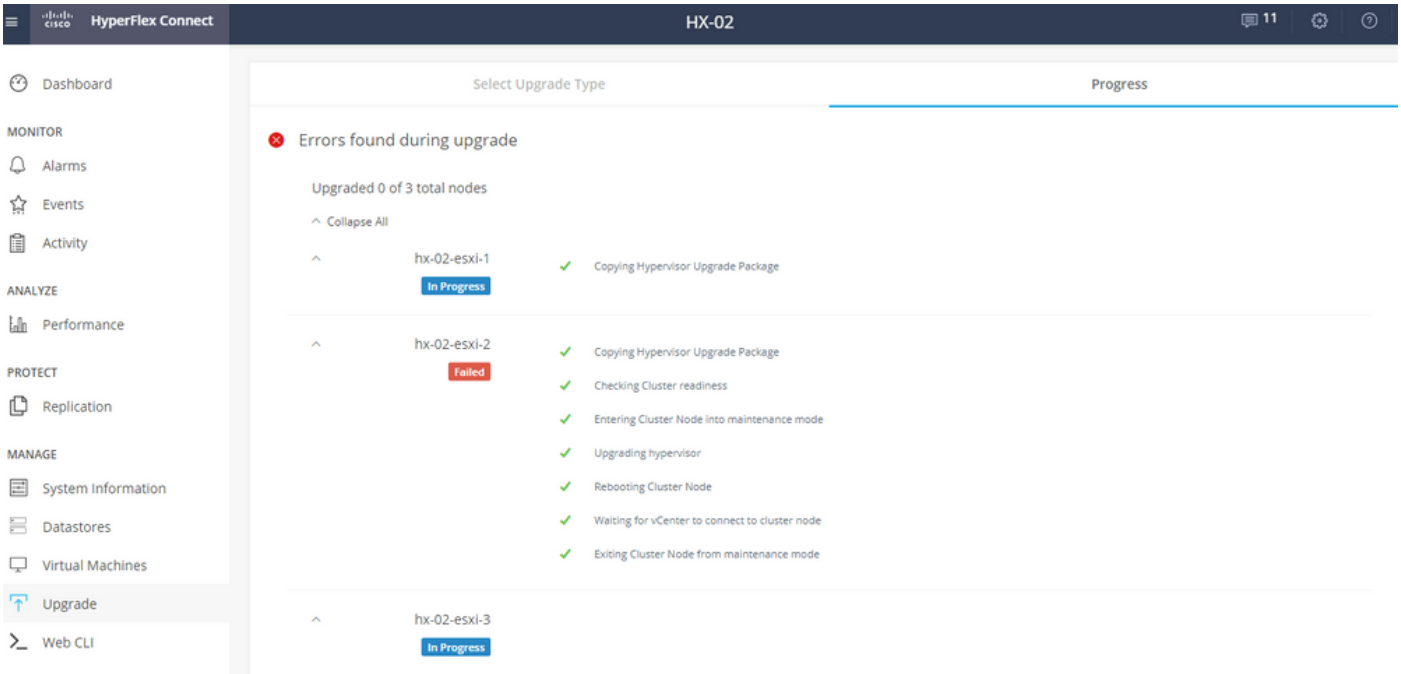
- HX连接中的系统信息页面
- 升级可能失败，**原因是"未能建立与主机的SSH连接"**或"升**级期间发现错误"**

ESXi升级失败，出现ssh异常 —

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9]错误c.s.sysmgmt.stMgr.SshScpUtilImpl — 无法建立与主机的SSH连接：主机不可达或处于锁定模式

com.jcraft.jsch.JSchException:算法协商失败





- 可能是其他领域

解决方法

HXDP版本说明已更新，以明确指出3.5(x)和4.0(x)版本不支持此版本的6.7。此问题已在HXDP 4.0补丁4.0(2e)和所有4.5(1a)及更高版本中解决。

- 使用ESXi内置的回滚机制回滚到兼容的ESXi版本。
- 另一个可能的解决方法是在每台ESXi主机上更新sshd_config并重新启动SSH服务，以重新启用删除的密钥交换方法。建议仅临时实施此解决方法。

注意：目标应是将集群移至固定HXDP版本，并尽快删除此解决方法。集群不应长期处于此状态，此额外的密钥算法设置会添加到sshd_config。

解决方法步骤

如果无法将HXDP升级到固定版本，请使用以下解决方法 —

解决方法1

- 使用ESXi内置的回滚机制回滚到兼容的ESXi版本。请参阅vmware KB - https://kb.vmware.com/s/article/1033604

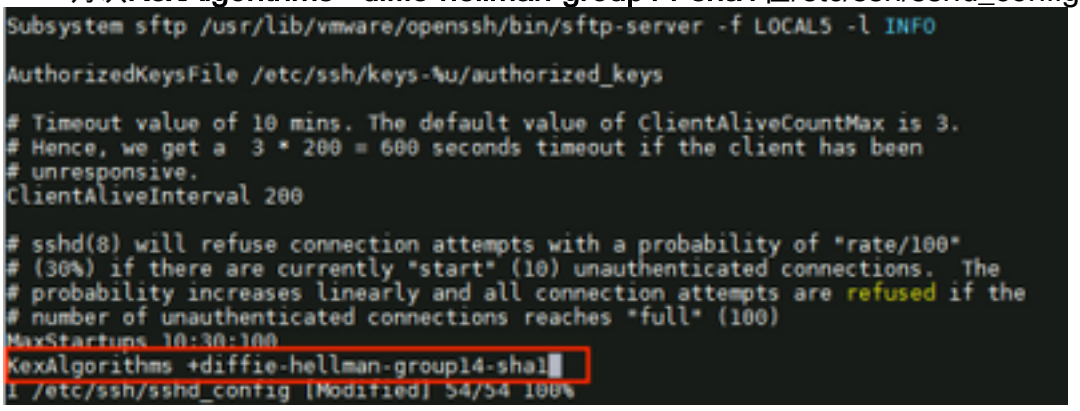
解决方法2

在每台ESXi主机上更新sshd_config并重新启动SSH服务，以重新启用删除的密钥交换方法。

- 在每台ESXi主机上的/etc/ssh/sshd_config下，将+diffie-hellman-group14-sha1添加到KexAlgorithms中

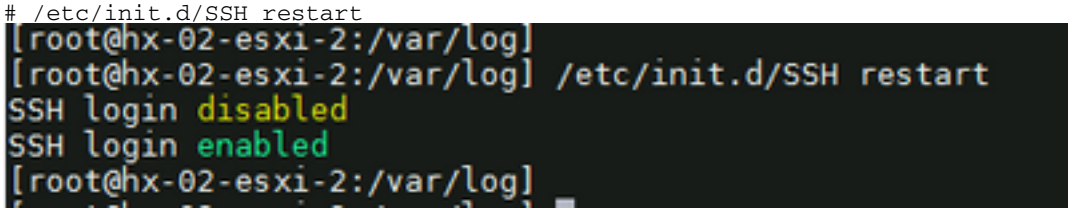
```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

- 确认**KexAlgorithms +diffie-hellman-group14-sha1**在/etc/ssh/sshd_config中显示



- 重新启动ESXi SSH进程

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



- 重新启动或恢复以前失败的工作流程。