SSH Incompatibility with ESXi 6.7P04 (build 17167734) and later

Contents

Introduction

A software interoperability issue exists between HXDP [3.5(x), 4.0(x)] and ESXi 6.7P04 (build 17167734) and later. Customers should avoid this software combination.

NOTE: This Issue is extended to any 6.7 ESXi version above 6.7P04

The compatibility issue is resolved in **HXDP 4.0(2e)**. This issue does not impact HXDP 4.5(1a) and later.

Requirements

ESXi 6.7P04 (build 17167734) and later

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

More Information

Defect

The related bug ID is **CSCvv88204 - ESXi OpenSSH Interoperability Issue with HXDP**

The issue occurs in ESXi 6.7P04, due to VMware upgrading the openSSH library to: OpenSSH_8.3p1. This new version of OpenSSH removes support for the key exchange method used internally by HXDP when communicating to ESXi directly via SSH. Below is a snippet from the OpenSSH changelog describing the breaking change made in that version:

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

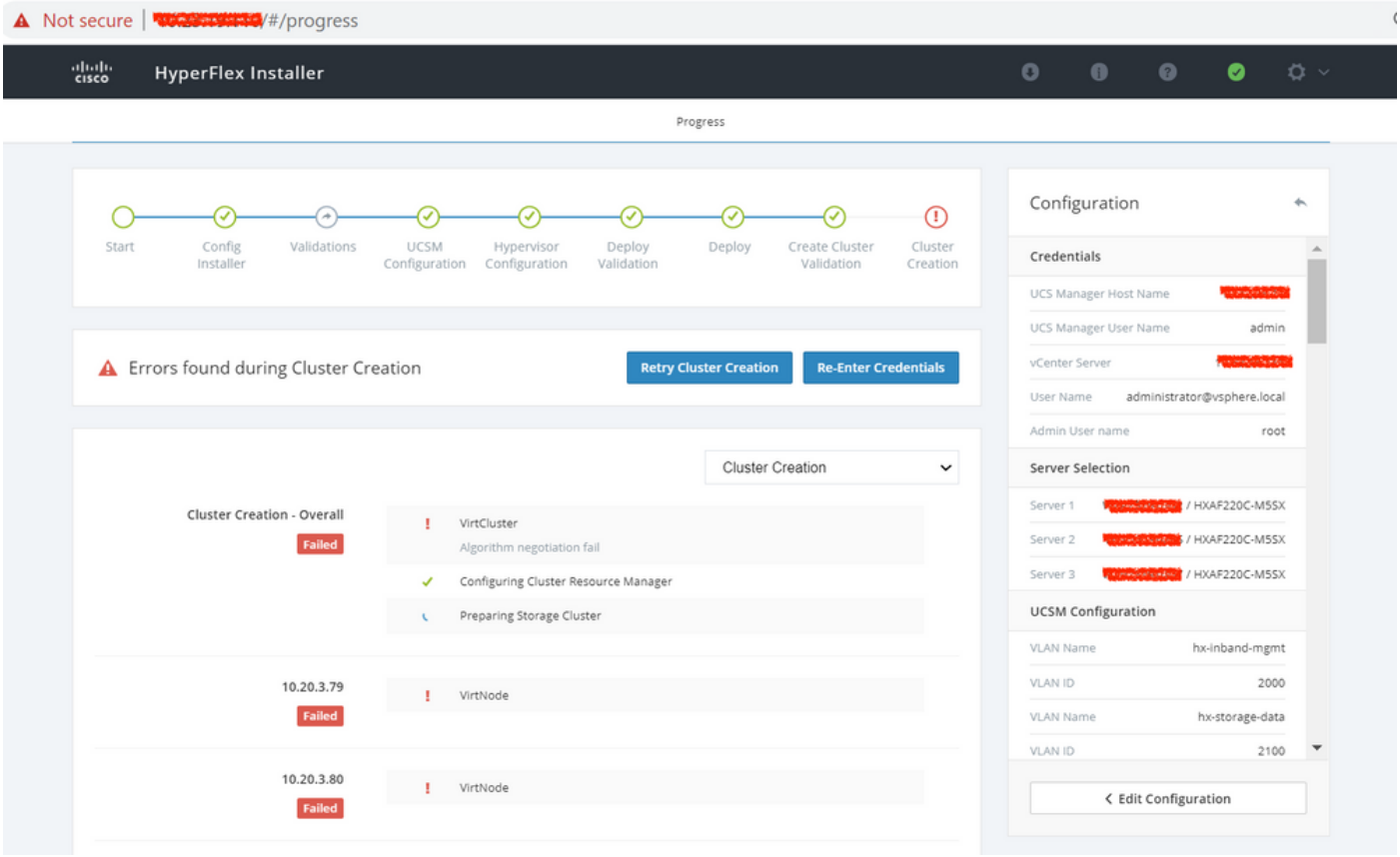
Software Advisory

Refer Software Advisory for more details - [Cisco Software Advisory for ESXi 6.7 P04]

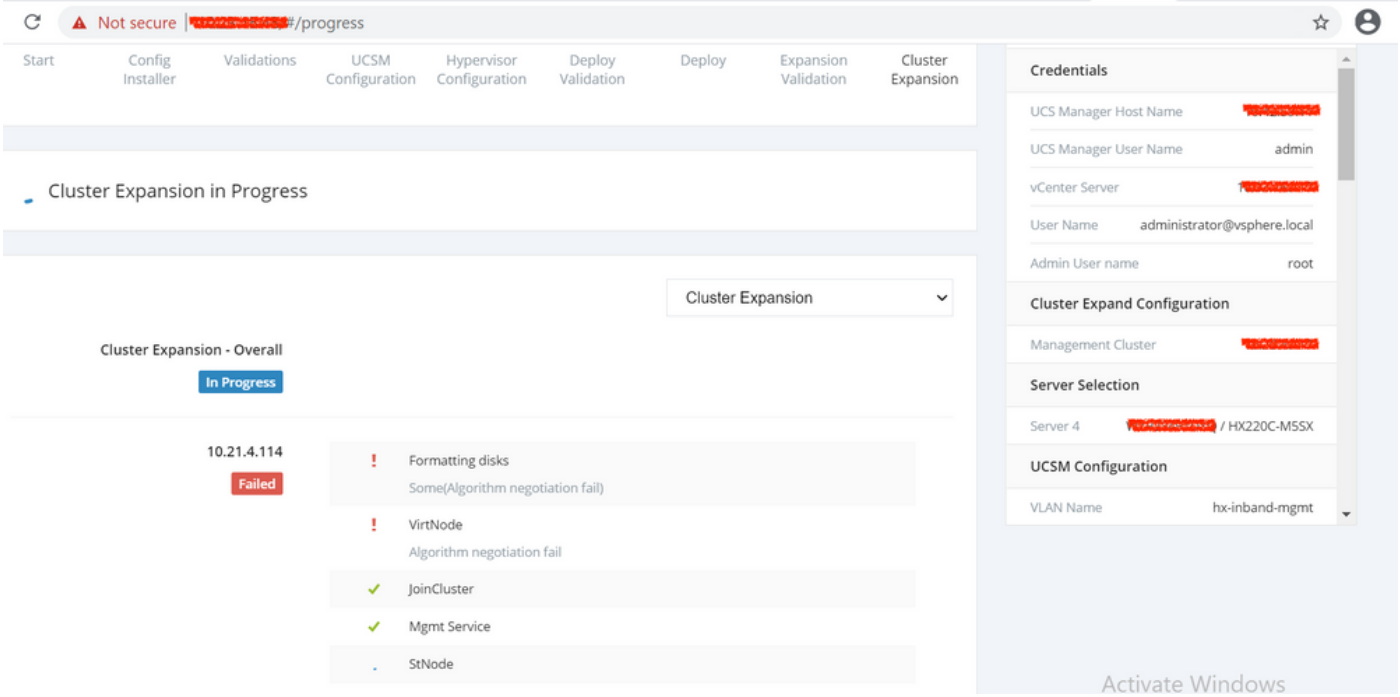
Impacted Areas

Some functional areas of HX will be impacted including:

- Fresh cluster creation (may fail with **Algorithm negotiation fail**)



- Cluster expansion (may fail with **Algorithm negotiation fail**)



- Cluster reregistaration (stcli cluster reregister may fail with **"Algorithm negotiation fail"**)

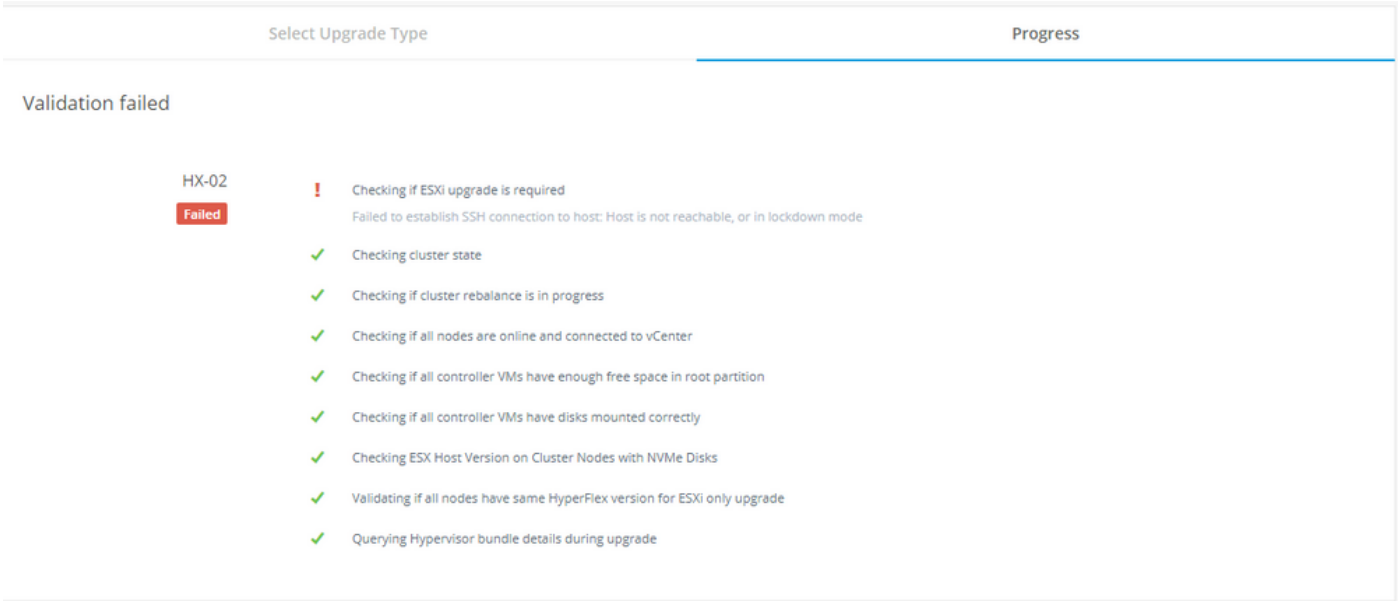
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration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

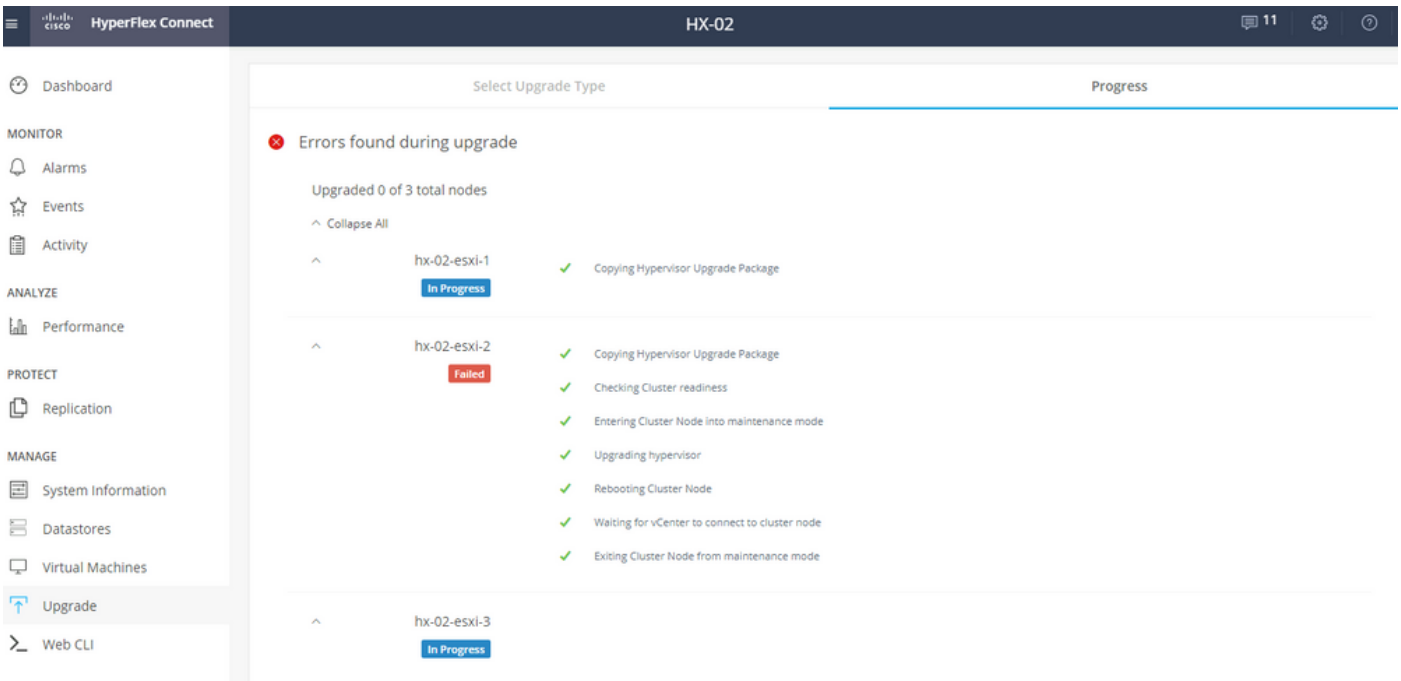
- System information page in HX Connect
- Upgrades may fail with **"Failed to Establish SSH Connection to host"** or **"Errors found during upgrade"**

ESXi upgradae fails with ssh exception-

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9] ERROR c.s.sysmgmt.stMgr.SshScpUtilImpl - Failed to establish SSH connection to host: Host is not reachable, or in lockdown mode

com.jcraft.jsch.JSchException: Algorithm negotiation fail





- Potentially other areas

Workaround

The HXDP release notes have been updated to specifically call out this version of 6.7 not being supported on 3.5(x) and 4.0(x) releases. This issue is fixed in the HXDP 4.0 patch - 4.0(2e) and in all releases 4.5(1a) and later.

- Use the rollback mechanism built into ESXi to roll back to a compatible ESXi version.
- Another possible workaround is to re-enable the removed key exchange method by updating sshd_config on each ESXi host and restarting the SSH service.It is recommended that this workaround only be implemented temporarily only.

NOTE: The goal should be to move the cluster to a fixed HXDP release and remove this workaround as soon as possible. Clusters should not remain in this state long term with this extra key algorithm setting added to sshd_config.

Steps for Workarounds

If you are unable to upgrade HXDP to a fixed release, use the following workarounds -

Workaround 1

- Use the rollback mechanism built into ESXi to roll back to a compatible ESXi version. Refer vmware KB - https://kb.vmware.com/s/article/1033604

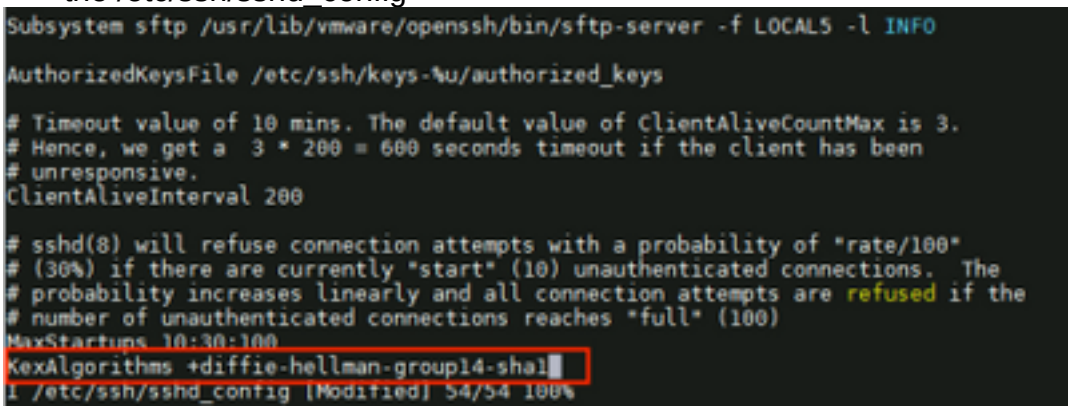
Workaround 2

Re-enable the removed key exchange method by updating sshd_config on each ESXi host and restarting the SSH service.

- Add +diffie-hellman-group14-sha1 to the KexAlgorithms under /etc/ssh/sshd_config on each ESXi host

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

- Confirm that **KexAlgorithms +diffie-hellman-group14-sha1** shows in the /etc/ssh/sshd_config



- Restart ESXi SSH process

```
# /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]
```

- Re-start or resume the previously failed workflow.