

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

## Contents

[Introduction](#)

[Requirements](#)

[More Information](#)

[Defect](#)

[Software Advisory](#)

[Impacted Areas](#)

[Workaround](#)

[Steps for Workarounds](#)

[Workaround 1](#)

[Workaround 2](#)

## 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**)

The screenshot shows the HyperFlex Installer progress screen. The progress bar indicates that the 'Cluster Creation' step has failed, while all previous steps (Start, Config Installer, Validations, UCSM Configuration, Hypervisor Configuration, Deploy Validation, Deploy, Create Cluster Validation) are successful. A red warning icon is present next to the 'Cluster Creation' step.

**Configuration**

**Credentials**

- UCS Manager Host Name: [Redacted]
- UCS Manager User Name: admin
- vCenter Server: [Redacted]
- User Name: administrator@vsphere.local
- Admin User name: root

**Server Selection**

- Server 1: [Redacted] / HXAF220C-M55X
- Server 2: [Redacted] / HXAF220C-M55X
- Server 3: [Redacted] / HXAF220C-M55X

**UCSM Configuration**

- VLAN Name: hx-inband-mgmt
- VLAN ID: 2000
- VLAN Name: hx-storage-data
- VLAN ID: 2100

**Cluster Creation - Overall**

**Failed**

- VirtCluster: Algorithm negotiation fail
- Configuring Cluster Resource Manager
- Preparing Storage Cluster

**10.20.3.79**

**Failed**

- VirtNode

**10.20.3.80**

**Failed**

- VirtNode

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

The screenshot shows the HyperFlex Installer progress screen during a cluster expansion. The progress bar indicates that the 'Cluster Expansion' step is in progress, while all previous steps (Start, Config Installer, Validations, UCSM Configuration, Hypervisor Configuration, Deploy Validation, Deploy, Expansion Validation) are successful. A red warning icon is present next to the 'Cluster Expansion' step.

**Cluster Expansion in Progress**

**Cluster Expansion - Overall**

**In Progress**

- 10.21.4.114
- Failed**
- Formatting disks: Some(Algorithm negotiation fail)
- VirtNode: Algorithm negotiation fail
- JoinCluster
- Mgmt Service
- StNode

**Configuration**

**Credentials**

- UCS Manager Host Name: [Redacted]
- UCS Manager User Name: admin
- vCenter Server: [Redacted]
- User Name: administrator@vsphere.local
- Admin User name: root

**Cluster Expand Configuration**

- Management Cluster: [Redacted]

**Server Selection**

- Server 4: [Redacted] / HX220C-M55X

**UCSM Configuration**

- VLAN Name: hx-inband-mgmt

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

```

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:~#

```

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

ESXi upgrade 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

The screenshot shows the 'Progress' tab of an upgrade operation. Under the 'Select Upgrade Type' section, there is a 'Validation failed' message. A table lists the validation steps:

Host	Status	Message
HX-02	Failed	Checking if ESXi upgrade is required Failed to establish SSH connection to host: Host is not reachable, or in lockdown mode
	Success	Checking cluster state
	Success	Checking if cluster rebalance is in progress
	Success	Checking if all nodes are online and connected to vCenter
	Success	Checking if all controller VMs have enough free space in root partition
	Success	Checking if all controller VMs have disks mounted correctly
	Success	Checking ESX Host Version on Cluster Nodes with NVMe Disks
	Success	Validating if all nodes have same HyperFlex version for ESXi only upgrade
	Success	Querying Hypervisor bundle details during upgrade

The screenshot shows the 'Progress' tab of an upgrade operation. Under the 'Select Upgrade Type' section, there is an 'Errors found during upgrade' message. A table lists the upgrade steps for three nodes:

Node	Status	Message
hx-02-esxi-1	In Progress	Copying Hypervisor Upgrade Package
hx-02-esxi-2	Failed	Copying Hypervisor Upgrade Package
	Success	Checking Cluster readiness
	Success	Entering Cluster Node into maintenance mode
	Success	Upgrading hypervisor
	Success	Rebooting Cluster Node
	Success	Waiting for vCenter to connect to cluster node
	Success	Exiting Cluster Node from maintenance mode
hx-02-esxi-3	In Progress	

- 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`

```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -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
# /etc/ssh/sshd_config [Modified] 54/54 100%
```

- 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.