ESXi and HXDP Compatibility Guidelines

First Published: 2017-04-28

Last Modified: 2023-02-14

Introduction

The HyperFlex Data Platform works in tandem with the ESXi hypervisor and UCS hardware components to provide a seamless customer experience. From a great out of box experience to easy ongoing maintenance, HyperFlex is designed to run optimally throughout its lifecycle. To ensure the best experience with your HyperFlex deployment, we recommend following these guidelines to ensure proper interoperability between HX Data Platform and ESXi software layers.

Important Using VMware Update Manager (VUM) or VMware Lifecycle Manager (vLCM) for upgrading the ESXi on HyperFlex node is not supported. Using these upgrade methods may delete Cisco custom drivers and cause cluster outages. We recommend using Cisco Intersight or HyperFlex Connect for ESXi upgrades including the security patches from VMware or manually installing patches using the offline zip bundle with ESXCLI commands.

ESXi Hypervisor

ESXi serves as a core foundational element for the HyperFlex data platform. Customers should therefore ensure that they are running an approved build that has been tested and known to work well with all HX platform features. For the latest list of tested ESXi versions, reference the section *Supported VMware vSphere Versions and Editions* in the Cisco HX Data Platform Release Notes.

It is common for VMware to release major, minor, bugfix, and security patches as part of the normal vSphere/ESXi product lifecycle. Customers are encouraged to use the specific version of ESXi called out in the release notes to ensure full compatibility. The rules for deviating to any other ESXi version is as follows:

- Major Releases (e.g. 5.5, 6.0, 6.5) – No deviation is allowed outside of the versions listed in the release notes.
- Update Releases (e.g. 6.0 U1, U2, U3) – No deviation is allowed outside of the versions listed in the release notes. Cisco will attempt to qualify these releases within a 90-day time window on a best effort basis.
- Bugfixes (Patch releases and Express Patches) – May be installed so long as you stay within the current update release. Cisco cannot guarantee full HX operation on untested ESXi builds. Customers are encouraged to try builds first in a lab or pre-production environment to ensure full operating capability. In the event the patch yields undesired results, customers may be asked to revert the patch. Cisco will attempt to qualify these releases within a 90-day time window on a best effort basis.
- Security Only Patches – May be installed so long as you stay within the current update release. Patch reversal may be necessary if incompatibility is determined.

Example

VMware Security Advisory VMSA-2017-0006 – this may be applied so long as you select the patch corresponding to a supported update release.

Important In all cases, it is strongly encouraged to remain on one of the specific versions listed in the release notes for long-term stability.

Notable Exceptions

ESXi 6.5 and later must be coupled with HX Data Platform 2.5(1a) as a minimum version. Earlier versions of HXDP will not function with ESXi 6.5 installed. Please upgrade HXDP to 2.5(1a) or later before upgrading to ESXi 6.5.

Patch Removal

The modular ESXi architecture provides dual boot banks to allow safe and easy reversal from patch installation. Customers should install patches manually using the offline zip bundle with ESXCLI commands. Alternatively, VUM can be used but only for single host remediation after the host has entered HX maintenance mode by the administrator.

Note Cluster level VUM remediation is not permitted at any time.

In the event a patch removal is required, please reference VMware KB: 1033604. Customers should avoid applying multiple patches sequentially until full stability has been determined. This ensures the alternate boot bank can be used to revert to a known working state with HyperFlex.