Best Practices for Patching VMware vSphere

VMware Security

Table of contents

Best Practices for Patching VMware vSphere

Introduction

This document provides actions to take that help ensure successful patching and updates in a VMware vSphere environment.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

Preparation

Ensure Access to VCSA Root and SSO Administrator Accounts

Ensure that the VCSA root and administrator@vsphere.local accounts work. By default, the VCSA root account locks after 90 days of inactivity, which may pose issues in emergencies. Note that password recovery may need a vCenter Server restart. Update passwords after maintenance.

Ensure Access to ESXi

Ensure direct access to ESXi for taking powered-off snapshots of vCenter Server and Platform Services Controllers (on vSphere 6.7 and earlier), as well as possible diagnostics. Ensure that you have working access to the hosts, with administrator rights.

Double-Check DNS

Ensure A (forward) and PTR (reverse) DNS records for vCenter Server, ESXi, and other appliances resolve correctly. The A record should match the right IP address, which should have a PTR record pointing back to the original A record. This simple check takes seconds and can detect unexpected changes that can cause problems during patches and upgrades.

Double-Check NTP

Ensure correct NTP settings for all virtual environment components, including ESXi, vCenter Server, SDDC Manager, appliances, storage, and switches. Many hard-to-diagnose system problems arise from poor time synchronization.

Check and Resolve Alarms

Examine and resolve alarms that are present on vCenter Server and ESXi. Examine and resolve vSAN health check warnings that may interfere with automated patching via Lifecycle Manager.

Double-Check Firewall Rules for Reduced Downtime Upgrade Temporary IP Address

Double-check that firewall rules are in place for the Reduced Downtime Upgrade temporary IP address, if using that update feature found in vCenter Server 8.0.2 and newer.

DRS Rules for Key Components

Use a DRS group and rules to keep vCenter Server and key VMs (like KMS, DNS, and AD) on a designated ESXi host. Prefer a 'should' rule for flexibility. This setup lets you quickly find and repair the VCSA using the Host Client if issues arise. Ensure a management workstation can access and log into the Host Client on that ESXi host.

'Should' DRS affinity rules are recommended because they allow automatic VM relocation during host patching and return them without manual action, reducing the potential for human error.

Ensure File-Based Backups of vCenter Server Have Been Taken

Ensure the vCenter Server's file-based backup and restore feature has produced a valid backup archive for all vCenter Servers. Manage this configuration through the Virtual Appliance Management Interface (VAMI). If File-Based Backups are not configured use the “Backup Now” feature to generate a one-time backup.

Export the Configuration of Distributed Switches

Export the configuration of Distributed Switches to ensure that you have a recent copy of the switch configuration. Store this backup in a place that is accessible.

Stage Update Payloads

Stage vCenter and ESXi updates in advance of execution. Staging allows the payloads to be downloaded to the local systems and mitigates against update operations failing due to network interruptions.

Deactivate vCenter HA

If in use, **vCenter HA must be deactivated** before you can update vCenter Server.

Execute Pre-Update Checks

Prior to staging and/or installing updates, expand the available versions in the VAMI "Available Updates" and click the "Run Pre-Update Checks" link to help ensure no known issues are present on your systems.

Execution

Proactive Reboot

Restart vCenter Server and related components if they've been running for an extended period. This assesses operational health before major updates, helping to identify if issues existed prior or resulted from recent changes. While it leads to additional brief downtime, it will speed up service recovery if problems occur.

Take Powered-Off Snapshots

Before performing an update, take a powered-off snapshot of the VCSA and all related Platform Service Controllers. You must use the ESXi host client after the VCSA has been gracefully and cleanly shut down. This offers a recovery point if issues arise during the update.

Environments that use Enhanced Linked Mode must power off all linked vCenter Server and Platform Service Controller instances and snapshot them simultaneously. Failure to do so will introduce replication errors and conflicts. Similarly, if reverting one snapshot, all must be reverted.

An example is an environment that has ten vCenter Servers and ten corresponding Platform Service Controllers, all linked using Enhanced Linked Mode. To upgrade successfully all twenty nodes must succeed in their updates. If eight vCenter Servers upgrade successfully, and the ninth fails, all twenty snapshots must be reverted. Failure to do this may result in invalid data replicating between the nodes.

Complex Environments Should Take Multiple Snapshots Throughout Patching. Environments with many linked vCenter Servers and/or Platform Service Controllers should take additional powered-off snapshots at intervals during the upgrade, to avoid having to revert everything if a failure occurs.

In the example above, if a new set of snapshots was taken after the seventh vCenter Server was patched, the failure on the ninth vCenter Server would only result in having to redo two updates (the eight and ninth vCenter Servers), not nine.

DRS to Partially Automated Mode

To avoid errors and issues resulting from updates to the ESXi host management agents **consider placing vSphere DRS in "Partially Automated" mode** so that migrations do not occur for the duration of the vCenter Server update. Remember to re-enable it afterwards.

Do not deactivate DRS! Doing so will cause the deletion of all resource pools.

Deactivate vSphere HA

To avoid errors and delays due to ESXi host management agent updates causing High Availability cluster elections **consider deactivating vSphere HA prior to the update**, then re-enabling it afterwards.

Do Not Rush

Do not upgrade multiple vCenter Servers and/or Platform Service Controllers simultaneously. Doing so will introduce replication errors between components and will result in the failure of the upgrade.

vCenter Server First, Then ESXi

Always update vCenter Server before ESXi to ensure compatibility and system stability. If only ESXi updates are available, proceed without waiting for a vCenter Server update. Environments that use Enhanced Linked Mode must update all vCenter Server and Platform Service Controller instances to the same version before applying ESXi updates.

Post-Upgrade

Re-Enable DRS & HA

If you deactivated vSphere HA and/or placed DRS in “Partially Automated” mode restore the original settings.

Re-Enable vCenter HA

If you deactivated vCenter HA and wish to continue using it, re-enable it.

Delete Snapshots

Over time, snapshots can reduce storage performance and become hard to delete. Once updates are confirmed, remove the snapshots.

Clear Your Browser’s Cache

If there is unexpected behavior in the vSphere Client during or after the update clear your browser’s cache. This often resolves anomalies in the vSphere and ESXi Host Clients.

Reset and Store New Passwords

Change the root passwords on ESXi and VCSA, and the administrator@vsphere.local password, storing the new passwords in your password manager or vault.

Create Fresh Backups

Trigger your normal backup process to create a new backup of vCenter Server, either through the File-Based Backup method or a third-party solution.

People & Process

Communicate the Implications of Patching to Non-Technical Stakeholders

vSphere Administrators know that patching vCenter Server doesn't affect workloads, and vMotion allows easy migration during ESXi patching. However, other organization members may not grasp these details. Informing change managers, risk assessors, and senior management can help get approval for essential patches and updates.

Establish Maintenance Windows for Predictability

Establish and communicate regular maintenance windows for your virtualization infrastructure. This allows administrators of downstream applications and other stakeholders anticipate and plan for these periods.

Reduce Resistance to vMotion

Resistance to vMotion, typically from workload and app administrators and vendors, creates challenges in patching vSphere. VMware vSphere 7 and 8 enhanced vMotion and DRS to decrease VM stun time, boost vMotion throughput, lessen guest OS impact, and eliminate excessive vMotion actions during patching with vSphere Lifecycle Manager. Moreover, vSphere 8's vMotion Notification aids applications in preparing for and rebounding from a vMotion, facilitating automatic infrastructure patching.

Leverage ITIL Change Categories for Effective Communication

Adopt the ITIL framework's definitions for changes: 'standard' changes are routine and non-disruptive, like deploying a new VM. 'Emergency' changes need immediate action, such as critical security patches. 'Normal' changes don't fit the other categories and occur during maintenance windows. Using these ITIL terms clarifies task significance and aids in prioritizing, ensuring alignment within the organization. Always label critical updates as 'emergency' for clarity and effective risk assessment.

System Design

Configure vCenter Server File-Based Backup and Restore

Ensure the vCenter Server's file-based backup and restore feature is properly configured and produces scheduled output. Manage this configuration through the Virtual Appliance Management Interface (VAMI) on port 5480/tcp of the VCSA. Regularly check the backup and restore functions to ensure data security and operational continuity.

Configure vSphere HA Isolation Addresses Properly

Ensure that vSphere High Availability (HA) doesn't use the vCenter Server as its custom isolation address (das.isolationaddress). Instead, use multiple addresses (das.isolationaddress0 to das.isolationaddress9) to prevent unnecessary HA failovers due to a single address's unavailability.

Minimize vCenter Server Plugins

Limit the number of plugins on vCenter Server where possible. Following the zero-trust architecture reduces system interconnections, decreasing potential attack avenues. Fewer plugins also simplify compatibility and ease upgrades, making the system more manageable and secure.

Reduce Additional VIBs on ESXi

Limit the number of VIBs on ESXi. Prefer 'stock' VMware ESXi over OEM versions to avoid VIB conflicts from vendor packages (good exceptions tend to be inclusion of newer NIC and HBA drivers). For security, only install essential software, and remove all non-VMware software that is not absolutely necessary for the operation of your environment.

Minimize the Use of Enhanced Linked Mode

Enhanced Linked Mode (ELM) offers a consolidated view of an organization’s vSphere environments, but also introduces security and availability considerations, and complicates updates and upgrades. Where possible, simplify your deployments by discontinuing the use of ELM.

PowerCLI is a very straightforward way to do management of virtual environments at scale, with a thriving community and thousands of code examples (including good ones in the vSphere Security Configuration & Hardening Guide).

Ensure N+1 Cluster Resources

vMotion and DRS work best when there are enough free cluster resources to migrate workloads to. Ensure that the vSphere cluster contains an appropriate amount of resources to absorb workloads stemming from the loss of a host (from patching or otherwise), without causing memory overcommitment or excessive CPU contention.

More Resources

For more VMware Security Resources please visit https://core.vmware.com/security.

For information about upgrading to new major versions of vSphere visit:

vSphere 8: https://core.vmware.com/vsphere-8-upgrade-activity-path
vSphere 7: https://core.vmware.com/vsphere-7-upgrade-activity-path