Upgrade FMCv and Migrate from VMware ESXi 7.0 to ESXi 8.0: Staged Approach and Best Practices

Contents

Issue

An administrator running Firewall Management Center virtual (FMCv) version 7.3.1 on VMware ESXi 7.0 is planning to upgrade the FMC to a higher supported version and subsequently migrate the FMCv virtual machine to a new VMware ESXi 8.0 cluster. These concerns were raised during this planning effort:

- Whether it is safe to upgrade FMCv from 7.3.1 to 7.4.2 first, and then migrate the VM to the ESXi 8.0 cluster, before performing any further upgrades.
- Whether there are known compatibility issues or constraints when migrating an FMCv running version 7.3.1 or 7.4.2 to a VMware ESXi 8.0 environment.
- Whether VMware vMotion can be used to perform a seamless, same-IP migration of the FMCv virtual machine to the new cluster without creating a new VM instance.
- Whether VMware snapshots can be used as a backup and rollback mechanism in the event that the upgrade or migration fails.
- What the highest supportable FMC version is for the existing managed device landscape, which includes Firewall Threat Defense (FTD) devices ranging from version 7.2.8 to 7.4.2.
- How to avoid IP address conflicts when cutting over to the new FMCv instance on the new cluster while keeping the same management IP address and hostname.
- What the correct order of operations is for a phased upgrade and migration plan that minimizes risk and downtime.

Environment

- Product: FMCv
- Current FMC software version: 7.3.1
- Current hypervisor platform: VMware ESXi 7.0

- Target hypervisor platform: VMware ESXi 8.0.3 (new cluster)
- FMC deployment type: Standalone (not part of a High Availability pair)
- Managed devices: Multiple FTD devices ranging from version 7.2.8 to 7.4.2

Resolution

The recommended approach for this environment is a staged, phased upgrade and migration plan. This plan separates the FMC software upgrade, the hypervisor platform migration, and any subsequent FMC version upgrades into distinct maintenance events. This approach reduces risk at each phase and provides clear rollback points. The use of VMware vMotion, snapshots, cloning, or direct VM-level migration is explicitly **not** the supported method for migrating FMCv between clusters or versions.

Important: VMware Snapshots, vMotion, and Cloning Are Not Supported for FMCv Migration

Before proceeding with any phase of this plan, it is critical to understand these constraints regarding VMware-native migration methods:

- **VMware snapshots** are **not** a supported backup, restore, or rollback method for FMCv upgrades or migrations. Reverting an FMCv to a VMware snapshot can cause database corruption, version and content update mismatches, or an unsupported system state.
- **VMware vMotion**, **cloning**, and **direct virtual machine migration** between clusters are **not** the supported method for migrating FMCv to a new hypervisor platform. These methods bypass the FMC's internal data integrity mechanisms.
- The **only supported method** for migrating FMCv to a new cluster or host is the **FMC native backup and restore workflow**, combined with deploying a fresh FMCv instance on the target platform.

The correct rollback strategy, if validation fails after cutover, is to power off the new FMCv instance and return the original FMCv to service. Do not rely on snapshot reverts for this purpose.

Phase 1: Pre-Upgrade Compatibility Check

Before initiating any FMC software upgrade, confirm the exact software versions of all managed FTD devices in the environment.

- FMC 7.4.2 supports management of FTD devices running version 7.0 and later.
- FMC 7.6.6 supports management of FTD devices running version 7.1 and later.
- If any FTD device in the environment is running a version < 7.0, that device must be upgraded to at least version 7.0 while the FMC remains on version 7.3.1, before the FMC itself is upgraded.
- For the documented environment (FTD range: 7.2.8 to 7.4.2), all managed devices are within the compatibility range for both FMC 7.4.2 and FMC 7.6.6. No FTD pre-upgrade is required in this case.

Also confirm these before proceeding:

- The FMC is standalone and not part of a high availability (HA) pair.
- The exact VMware ESXi 8.0 build on the new cluster (confirmed as ESXi 8.0.3 in this environment).
- The FMCv resource profile (vCPUs, memory, disk) meets the requirements for the target FMC release. The current specification of 4 vCPUs, 32 GB RAM, and 250 GB disk must be reviewed against current deployment guidelines, particularly before upgrading to FMC 7.6.6.
- Whether the FMC management IP address and hostname remain the same after migration (strongly recommended to avoid requiring manager-address updates on all managed FTD devices).

Phase 2: Upgrade Existing FMCv from 7.3.1 to 7.4.2 on the Current ESXi 7.0 Cluster

This phase upgrades the FMCv software to version 7.4.2 while it remains on the existing ESXi 7.0 infrastructure. FMCv 7.4.2 adds explicit support for VMware ESXi 8.0, which is required before the platform migration in Phase 3.

Step 1: Confirm that no pending policy deployments, active backup jobs, or background tasks are currently running on the FMC before beginning the upgrade.

Step 2: Perform a full native FMC backup using the FMC built-in backup utility. Store the backup in a secure, remote location outside of the FMCv virtual machine. Verify the backup completes successfully before proceeding.

Step 3: Complete all upgrade readiness checks as documented in the FMC 7.4 upgrade planning guide. Resolve any flagged issues before initiating the upgrade.

Step 4: Upgrade the existing FMCv from version 7.3.1 to version 7.4.2. This uses the supported upgrade transition path: **7.3 → 7.4**.

Step 5: After the upgrade completes, perform post-upgrade validation:

- Verify that all managed FTD devices have reconnected to the FMC.
- Confirm that event ingestion is active and events are appearing in the FMC.
- Confirm that licensing status is correct.
- Execute a test policy deployment to a managed device and confirm it succeeds.

Do not proceed to Phase 3 until all post-upgrade validation steps pass successfully on the upgraded FMCv 7.4.2.

Phase 3: Migrate FMCv to the VMware ESXi 8.0.3 Cluster Using Native Backup and Restore

This phase migrates the FMCv from the existing ESXi 7.0 cluster to the new ESXi 8.0.3 cluster. This is accomplished by deploying a new FMCv instance on the target cluster and restoring a native FMC backup onto it. The same management IP address and hostname are retained to avoid requiring manager-address changes on all managed FTD devices.

Step 1: Once the FMCv is confirmed stable on version 7.4.2, generate a fresh native FMC backup. Store it in a secure, remote location. Verify the backup is complete and valid before proceeding.

Step 2: Deploy a new FMCv instance on the ESXi 8.0.3 cluster. The software version and build of this new instance must **exactly match** the version of the FMCv (including patches and hotfixes) from which the backup was taken (FMCv 7.4.2). Ensure the new instance is configured with equivalent or greater resources (vCPUs, memory, disk) and that network configuration is staged but the production management IP address is **not yet assigned** to the new instance at this point.

Step 3: Restore the native FMC backup onto the new FMCv instance on ESXi 8.0.3.

Step 4: Before bringing the new FMCv online with the production management IP address and hostname, **fully power off or disconnect the original FMCv** from the network. This is a mandatory step to prevent a duplicate IP condition and to avoid two FMC instances attempting to communicate with the same managed FTD devices simultaneously.

During the period when the original FMCv is powered off and before the new FMCv is online, this is expected behavior for the managed FTD devices:

- **Traffic Forwarding:** FTD devices operate data planes independently of the FMC and continue to seamlessly forward traffic and enforce the last successfully deployed access control policy, except the cases mentioned here.
- **Management & Visibility Changes:** Policy deployments, configuration adjustments, FMC health

alerts, and device-management visibility are completely unavailable.

- **Event Buffering & Potential Loss:** Real-time event visibility at the FMC are paused. While the FTD attempts to log security and connection events locally in its temporary unified files, these files have strict storage limits and operate on a circular overwrite basis. High-volume connection logs can be overwritten or lost during an extended migration window. Events remaining in the local buffer are streamed to the new FMC once it is online.
- **Malware (AMP) Rules:** Real-time cloud lookup requests for uncached files are temporarily unavailable because the FMC proxies these reputation queries to the AMP Cloud. The FTD continues to enforce blocking or allowing rules *only* for files already stored in its local on-box disposition cache. Uncached files bypass cloud analysis and use your policy's fail-safe settings (typically failing open to prevent traffic disruption). Sandboxing submissions to Threat Grid and retrospective alerts are paused until the new FMC is operational.
- **Identity-Based Rules:** Users who are already logged in and mapped to an IP address experience no interruption, as the FTD retains active mappings in its local memory. However, because the FMC acts as the broker for identity sources (for example., Cisco ISE or Active Directory Agents), **new user logins or IP changes during this window cannot be learned by the FTD.** These unknown sessions fall back to your policy's default or guest rules.
- **URL Filtering:** Live cloud lookups for completely unknown websites are temporarily unavailable because the FMC proxies unknown URL requests to the Cisco Talos cloud. The FTD continues to fully filter and enforce policy *only* for websites already found within its pushed local dataset or its active local memory cache. Web traffic hitting an uncached, unknown URL bypasses cloud classification and match your policy's fallback settings for uncategorized traffic (typically allowed). URL database package updates are paused until the new FMC is online.

Step 5: Assign the production management IP address and hostname to the restored FMCv on ESXi 8.0.3 and bring it online. Because the same IP address and hostname are used, the managed FTD devices canreconnect to the FMC automatically without requiring manager-address changes on individual FTD devices.

Step 6: Perform post-migration validation:

- Verify that all managed FTD devices have reconnected to the new FMCv instance.
- Check licensing status and confirm all licenses are correctly applied.
- Confirm that event flow and any external integrations are functioning correctly.
- Execute a controlled policy deployment to a managed device and confirm it succeeds.

If validation fails at any point during this phase, power off the new FMCv instance, restore the original FMCv on ESXi 7.0 to service, and troubleshoot before reattempting the migration. Do not use a VMware snapshot revert as a rollback mechanism.

Phase 4: Upgrade FMCv from 7.4.2 to 7.6.6 (After Migration Is Confirmed Stable)

Once the FMCv migration to ESXi 8.0.3 is fully validated and confirmed stable, a further upgrade to FMC 7.6.6 can be considered. It is strongly recommended to **not** combine the hypervisor platform migration (Phase 3) and this additional FMC version upgrade into a single maintenance event. Completing the migration first provides a clean, low-risk checkpoint before proceeding.

Before initiating the upgrade to 7.6.6, confirm these prerequisites:

- Every managed FTD device in the environment is running version 7.1 or later. FMC 7.6.6 does not support management of FTD devices < version 7.1. In the documented environment (FTD range: 7.2.8 to 7.4.2), all devices meet this requirement.
- The FMCv resource profile (4 vCPUs, 32 GB RAM, 250 GB disk) has been validated against the FMC 7.6.6 deployment guidelines for the total managed device count and event-retention requirements in this environment.
- The supported upgrade transition path is confirmed: **7.4 → 7.6**.
- The FMC is confirmed as standalone (not part of a High Availability pair).

Step 1: Create and verify a fresh native FMC backup from the stable FMCv 7.4.2 instance on ESXi 8.0.3. Store it in a secure, remote location.

Step 2: Upgrade the FMCv from version 7.4.2 to version 7.6.6.

Step 3: Perform final post-upgrade validation:

- Verify that all managed FTD devices have reconnected to the FMC.
- Confirm event handling and event ingestion are functioning correctly.
- Confirm licensing status is correct.
- Execute a controlled policy deployment to confirm policy application is successful.

Summary of Upgrade Path and Transition Sequence

The table summarizes the complete staged plan, the supported upgrade transitions, and the key action at each phase:

Phase	Action	FMC Version	Hypervisor	Supported Transition
Phase 1	Pre-upgrade compatibility check; confirm FTD versions, FMC HA status, and resource profile	7.3.1 (current)	ESXi 7.0	N/A — preparation only

Phase 2	Upgrade FMCv software; perform native backup; validate managed devices and policy deployment	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4 (supported)
Phase 3	Deploy new FMCv on ESXi 8.0.3; restore native backup; cut over using same IP/hostname; validate	7.4.2 (no version change)	ESXi 7.0 → ESXi 8.0.3	Native backup/restore — supported method
Phase 4	After migration is stable: upgrade FMCv; validate device connectivity, licensing, events, policy	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6 (supported)

Key Considerations

- **Upgrade Path Compliance:** The complete upgrade sequence — 7.3.1 → 7.4.2 → 7.6.6 — uses the supported FMC upgrade transition paths (7.3 → 7.4 and 7.4 → 7.6). Skipping intermediate versions or combining phases into a single event is not recommended.
- **FMC-FTD Compatibility:** FMC 7.6.6 maintains full management compatibility with FTD devices running versions 7.2.8 through 7.4.2. FMC 7.6 requires all managed FTD devices to be at version 7.1 or later.
- **Same IP Address Cutover:** The original FMCv must be fully powered off or disconnected from the network before the replacement FMCv is brought online with the production management IP address. This prevents a duplicate-IP condition and avoids two management centers simultaneously attempting to communicate with the same FTD devices. When the restored FMCv returns with the same IP address and hostname, managed FTD devices can reconnect without requiring manager-address changes.
- **Resource Validation Before 7.6.6:** The FMCv resource profile (4 vCPUs, 32 GB RAM, 250 GB disk) must be reviewed against current deployment guidelines before upgrading to FMC 7.6.6, taking into account the total managed device count and event-retention requirements for the environment.
- **Native Backup Verification:** At each phase where a native FMC backup is taken, the backup must be verified as complete and valid before proceeding. Backups must be stored in a secure, remote location outside of the FMCv virtual machine.
- **Do Not Combine Migration and Upgrade:** The platform migration (Phase 3) and the subsequent FMC version upgrade to 7.6.6 (Phase 4) must be performed as separate maintenance events. This ensures a clean checkpoint exists at FMCv 7.4.2 on ESXi 8.0.3 before any further changes are made.

Cause

This is not a break-fix issue resulting from a software defect or misconfiguration. The underlying cause

requiring this guidance is a combination of version compatibility requirements and platform migration constraints specific to the Cisco FMCv on VMware:

- **FMC version compatibility with FTD 7.4.2:** The presence of a managed FTD device running version 7.4.2 in the environment requires the FMC to be upgraded to a minimum of version 7.4.2, as earlier FMC versions cannot manage FTD devices at a higher version than the FMC itself.
- **FMCv support for VMware ESXi 8.0:** FMCv 7.3.1 does not support VMware ESXi 8.0 as a hypervisor platform. The FMCv must be upgraded to version 7.4.2 (or later) before it can be deployed or operated on ESXi 8.0.x. Attempting to migrate the FMCv 7.3.1 VM directly to ESXi 8.0 without first upgrading the FMC software introduces compatibility risk.
- **Unsupported VM migration methods:** VMware vMotion, snapshots, cloning, and direct VM migration are not supported methods for migrating FMCv between clusters or hypervisor versions. These methods can result in database corruption, version mismatches, or an unsupported system state. The only supported migration path is the FMC native backup and restore workflow combined with a fresh FMCv deployment on the target platform.

Related Content

- Cisco Secure Firewall Management Center Upgrade Guide, Version 7.4 — Upgrade Planning and Supported Paths
- Cisco Secure Firewall Management Center Upgrade Guide, Version 7.6 — Upgrade Planning and Supported Paths
- Cisco Secure Firewall Management Center Compatibility Guide (FMC and FTD Compatibility Matrix)
- Cisco Secure Firewall Management Center New Features by Release — Version 7.4.2
- Cisco Firepower Management Center Upgrade Guide — Upgrade Planning
- Cisco Technical Support & Downloads