Upgrade von FMCv und Migration von VMware ESXi 7.0 auf ESXi 8.0: Stufenweiser Ansatz und Best Practices

Inhalt

Problem

Ein Administrator, der Firewall Management Center Virtual (FMCv) Version 7.3.1 auf VMware ESXi 7.0 ausführt, plant, das FMC auf eine höhere unterstützte Version zu aktualisieren und anschließend das virtuelle FMCv-System auf ein neues VMware ESXi 8.0-Cluster zu migrieren. Diese Bedenken wurden bei der Planung vorgebracht:

- Gibt an, ob ein Upgrade von FMCv von 7.3.1 auf 7.4.2 sicher ist, und migrieren Sie dann das virtuelle System zum ESXi 8.0-Cluster, bevor Sie weitere Upgrades durchführen.
- Gibt an, ob bei der Migration eines FMCv mit Version 7.3.1 oder 7.4.2 zu einer VMware ESXi 8.0-Umgebung bekannte Kompatibilitätsprobleme oder Einschränkungen auftreten.
- Hiermit wird festgelegt, ob VMware vMotion für eine nahtlose Migration der virtuellen FMCv-Maschine vom selben IP-Typ zum neuen Cluster ohne Erstellung einer neuen VM-Instanz verwendet werden kann.
- Legt fest, ob VMware-Snapshots als Backup- und Rollback-Mechanismus verwendet werden können, falls das Upgrade oder die Migration fehlschlägt.
- Wie sieht die höchste unterstützbare FMC-Version für die vorhandene verwaltete Gerätelandschaft aus, die Firewall Threat Defense (FTD)-Geräte von Version 7.2.8 bis 7.4.2 umfasst?
- Vermeidung von IP-Adresskonflikten beim Umschalten auf die neue FMCv-Instanz im neuen Cluster unter Beibehaltung der gleichen Management-IP-Adresse und des gleichen Hostnamens
- Die richtige Reihenfolge der Abläufe ist für einen schrittweisen Upgrade- und Migrationsplan, der Risiken und Ausfallzeiten minimiert.

Umwelt

- Produkt: FMC V
- Aktuelle FMC-Softwareversion: 7.3.1
- Aktuelle Hypervisor-Plattform: VMware ESXi 7.0
- Zielhypervisor-Plattform: VMware ESXi 8.0.3 (neuer Cluster)
- FMC-Bereitstellungstyp: Standalone (kein Teil eines Hochverfügbarkeitspaars)
- Verwaltete Geräte: Mehrere FTD-Geräte von Version 7.2.8 bis 7.4.2

Auflösung

Der empfohlene Ansatz für diese Umgebung ist ein stufenweiser Upgrade- und Migrationsplan. Bei diesem Plan werden das FMC-Software-Upgrade, die Hypervisor-Plattform-Migration und alle nachfolgenden FMC-Versionen in separate Wartungsereignisse aufgeteilt. Dieser Ansatz verringert das Risiko in jeder Phase und bietet klare Rollback-Punkte. Die Verwendung von VMware vMotion, Snapshots, Klonen oder die direkte Migration auf VM-Ebene ist explizit nicht die unterstützte Methode für die Migration von FMCv zwischen Clustern oder Versionen.

Wichtig: VMware-Snapshots, vMotion und Klonen werden für die FMCv-Migration nicht unterstützt

Bevor Sie mit einer Phase dieses Plans fortfahren, müssen Sie die folgenden Einschränkungen hinsichtlich der nativen VMware-Migrationsmethoden kennen:

- VMware-Snapshots sind keine unterstützte Backup-, Wiederherstellungs- oder Rollback-Methode für FMCv-Upgrades oder -Migrationen. Das Zurücksetzen eines FMCv auf einen VMware-Snapshot kann zu Datenbankfehlern, falschen Zuordnungen von Versionen und Inhaltsaktualisierungen oder einem nicht unterstützten Systemstatus führen.
- VMware vMotion, Klonen und die direkte Migration virtueller Systeme zwischen Clustern werden nicht für die Migration von FMCv auf eine neue Hypervisor-Plattform unterstützt. Diese Methoden umgehen die internen Datenintegritätsmechanismen des FMC.

- Die einzige unterstützte Methode für die Migration von FMCv zu einem neuen Cluster oder Host ist der native FMC-Sicherungs- und Wiederherstellungs-Workflow in Verbindung mit der Bereitstellung einer neuen FMCv-Instanz auf der Zielplattform.

Wenn die Validierung nach der Umstellung fehlschlägt, sollten Sie die neue FMCv-Instanz ausschalten und das ursprüngliche FMCv wieder in Betrieb nehmen. Verlassen Sie sich zu diesem Zweck nicht auf Snapshot-Reverts.

Phase 1: Kompatibilitätsprüfung vor dem Upgrade

Bevor Sie ein FMC-Software-Upgrade einleiten, bestätigen Sie die genaue Softwareversion aller verwalteten FTD-Geräte in der Umgebung.

- FMC 7.4.2 unterstützt die Verwaltung von FTD-Geräten mit Version 7.0 und höher.
- FMC 7.6.6 unterstützt die Verwaltung von FTD-Geräten ab Version 7.1.
- Wenn auf einem FTD-Gerät in der Umgebung eine Version < 7.0 ausgeführt wird, muss dieses Gerät auf mindestens Version 7.0 aktualisiert werden, während das FMC auf Version 7.3.1 bleibt, bevor das FMC selbst aktualisiert wird.
- Für die dokumentierte Umgebung (FTD-Bereich: 7.2.8 bis 7.4.2) befinden sich alle verwalteten Geräte im Kompatibilitätsbereich für FMC 7.4.2 und FMC 7.6.6. In diesem Fall ist kein FTD-Pre-Upgrade erforderlich.

Bestätigen Sie vor dem Fortfahren die folgenden Punkte:

- Das FMC ist eigenständig und nicht Teil eines Hochverfügbarkeitspaars.
- Die genaue Version von VMware ESXi 8.0 baut auf dem neuen Cluster auf (in dieser Umgebung als ESXi 8.0.3 bestätigt).
- Das FMCv-Ressourcenprofil (vCPUs, Arbeitsspeicher, Festplatte) erfüllt die Anforderungen für die FMC-Zielversion. Die aktuelle Spezifikation von 4 vCPUs, 32 GB RAM und 250 GB Festplatte muss vor dem Upgrade auf FMC 7.6.6 mit den aktuellen Bereitstellungsrichtlinien abgeglichen werden.
- Legt fest, ob die IP-Adresse und der Hostname des FMC nach der Migration unverändert bleiben (dringend empfohlen, um zu vermeiden, dass Updates der Manager-Adressen auf allen verwalteten FTD-Geräten erforderlich sind).

Phase 2: Upgrade von vorhandenem FMCv von 7.3.1 auf 7.4.2 im aktuellen ESXi 7.0-Cluster

In dieser Phase wird die FMCv-Software auf Version 7.4.2 aktualisiert, während sie in der bestehenden ESXi 7.0-Infrastruktur verbleibt. FMCv 7.4.2 bietet eine explizite Unterstützung für VMware ESXi 8.0, die vor der Plattform-Migration in Phase 3 erforderlich ist.

Schritt 1: Vergewissern Sie sich, dass auf dem FMC derzeit keine ausstehenden Richtlinienbereitstellungen, aktiven Sicherungsaufträge oder Hintergrundaufgaben ausgeführt werden, bevor Sie mit dem Upgrade beginnen.

Phase 2: Führen Sie eine vollständige native FMC-Sicherung mithilfe des integrierten FMC-Sicherungsprogramms durch. Speichern Sie die Sicherung an einem sicheren Remote-Standort außerhalb des virtuellen FMCv-Systems. Überprüfen Sie, ob die Sicherung erfolgreich abgeschlossen wurde, bevor Sie fortfahren.

Schritt 3: Führen Sie alle Prüfungen der Upgrade-Fähigkeit gemäß den Angaben im FMC 7.4-Upgrade-Planungsleitfaden durch. Beheben Sie alle gekennzeichneten Probleme, bevor Sie das Upgrade starten.

Schritt 4: Aktualisieren Sie die vorhandene FMCv-Version von Version 7.3.1 auf Version 7.4.2. Hierbei wird der unterstützte Upgrade-Übergangspfad verwendet: 7,3 → 7,4.

Schritt 5: Führen Sie nach Abschluss des Upgrades eine Validierung nach dem Upgrade durch:

- Überprüfen Sie, ob alle verwalteten FTD-Geräte wieder mit dem FMC verbunden sind.
- Bestätigen Sie, dass die Ereignisaufnahme aktiv ist und Ereignisse im FMC angezeigt werden.
- Bestätigen Sie, dass der Lizenzierungsstatus korrekt ist.
- Führen Sie eine Testrichtlinienbereitstellung auf einem verwalteten Gerät aus, und bestätigen Sie, dass sie erfolgreich ist.

Fahren Sie erst mit Phase 3 fort, wenn alle Validierungsschritte nach dem Upgrade für das aktualisierte FMCv 7.4.2 erfolgreich bestanden haben.

Phase 3: Migration von FMCv auf den VMware ESXi 8.0.3-Cluster mit nativem

Backup und nativer Wiederherstellung

In dieser Phase wird FMCv vom vorhandenen ESXi 7.0-Cluster zum neuen ESXi 8.0.3-Cluster migriert. Hierzu wird eine neue FMCv-Instanz auf dem Zielcluster bereitgestellt und ein natives FMC-Backup darauf wiederhergestellt. Es werden dieselbe IP-Adresse und derselbe Hostname beibehalten, um zu vermeiden, dass Änderungen an der Manager-Adresse auf allen verwalteten FTD-Geräten erforderlich sind.

Schritt 1: Nachdem FMCv in Version 7.4.2 als stabil bestätigt wurde, erstellen Sie ein neues natives FMC-Backup. Bewahren Sie die Lösung an einem sicheren, entfernten Ort auf. Überprüfen Sie, ob die Sicherung abgeschlossen und gültig ist, bevor Sie fortfahren.

Phase 2: Stellen Sie eine neue FMCv-Instanz auf dem ESXi 8.0.3-Cluster bereit. Die Softwareversion und der Build dieser neuen Instanz müssen genau der Version des FMCv (einschließlich Patches und Hotfixes) entsprechen, von der die Sicherung stammt (FMCv 7.4.2). Stellen Sie sicher, dass die neue Instanz mit gleichwertigen oder höheren Ressourcen (vCPUs, Arbeitsspeicher, Festplatte) konfiguriert ist und dass die Netzwerkkonfiguration bereitgestellt wird, die IP-Adresse für das Produktionsmanagement jedoch der neuen Instanz noch nicht zugewiesen ist.

Schritt 3: Stellen Sie die native FMC-Sicherung auf der neuen FMCv-Instanz von ESXi 8.0.3 wieder her.

Schritt 4: Bevor Sie das neue FMCv mit der IP-Adresse und dem Hostnamen für die Produktionsverwaltung online stellen, schalten Sie das ursprüngliche FMCv vollständig aus, oder trennen Sie es vom Netzwerk. Dies ist ein zwingender Schritt, um eine doppelte IP-Adresse zu vermeiden und zu verhindern, dass zwei FMC-Instanzen gleichzeitig mit den gleichen verwalteten FTD-Geräten kommunizieren.

Während des Zeitraums, in dem das ursprüngliche FMCv ausgeschaltet ist, und bevor das neue FMCv online ist, wird dieses Verhalten für die verwalteten FTD-Geräte erwartet:

- Weiterleitung von Datenverkehr: FTD-Geräte betreiben Datenebenen unabhängig vom FMC und leiten den Datenverkehr nahtlos weiter und setzen die letzte erfolgreich bereitgestellte Zugriffskontrollrichtlinie durch, mit Ausnahme der hier genannten Fälle.
- Änderungen bei Management und Transparenz: Richtlinienbereitstellungen, Konfigurationsanpassungen, FMC-Integritätswarnungen und Transparenz beim Gerätemanagement sind nicht verfügbar.
- Ereignispufferung und potenzieller Verlust: Die Echtzeit-Ereignistransparenz am FMC wird

angehalten. Während die FTD versucht, Sicherheits- und Verbindungsereignisse lokal in ihren temporären Unified-Dateien zu protokollieren, haben diese Dateien strenge Speichergrenzen und arbeiten auf einer zirkulären Überschreibungsbasis. Verbindungsprotokolle mit hohem Volumen können während eines erweiterten Migrationsfensters überschrieben werden oder verloren gehen. Ereignisse, die im lokalen Puffer verbleiben, werden an das neue FMC übertragen, sobald es online ist.

- Malware-Regeln (AMP): Cloud-Suchanfragen in Echtzeit für nicht zwischengespeicherte Dateien sind vorübergehend nicht verfügbar, da das FMC diese Reputationsabfragen an die AMP-Cloud proxyiert. Die FTD setzt weiterhin die Blockierung oder das Zulassen von Regeln nur für Dateien durch, die bereits im internen Dispositionscache gespeichert sind. Nicht zwischengespeicherte Dateien umgehen die Cloud-Analyse und verwenden die ausfallsicheren Einstellungen Ihrer Richtlinie (normalerweise können sie nicht geöffnet werden, um Unterbrechungen des Datenverkehrs zu verhindern). Sandboxing-Meldungen bei Threat Grid und retrospektive Warnmeldungen werden angehalten, bis das neue FMC einsatzbereit ist.

- Identitätsbasierte Regeln: Benutzer, die bereits angemeldet und einer IP-Adresse zugeordnet sind, erhalten keine Unterbrechung, da die FTD aktive Zuordnungen im lokalen Speicher speichert. Da das FMC jedoch als Broker für Identitätsquellen fungiert (z. B. Cisco ISE oder Active Directory Agents), können neue Benutzeranmeldungen oder IP-Änderungen während dieses Fensters vom FTD nicht abgerufen werden. Diese unbekannten Sitzungen greifen auf die Standard- oder Gastregeln Ihrer Richtlinie zurück.

- URL-Filterung: Live-Cloud-Suchen nach völlig unbekannten Websites sind vorübergehend nicht verfügbar, da das FMC unbekannte URL-Anfragen an die Cisco Talos Cloud weiterleitet. Die FTD filtert und setzt Richtlinien nur für Websites durch, die bereits in ihrem lokalen Push-Datensatz oder im aktiven lokalen Speicher-Cache gefunden wurden. Webdatenverkehr, der auf eine nicht zwischengespeicherte, unbekannte URL trifft, umgeht die Cloud-Klassifizierung und entspricht den Fallback-Einstellungen Ihrer Richtlinie für nicht kategorisierten Datenverkehr (in der Regel zulässig). Aktualisierungen des URL-Datenbankpakets werden angehalten, bis das neue FMC online ist.

Schritt 5: Weisen Sie dem wiederhergestellten FMCv auf ESXi 8.0.3 die IP-Adresse und den Hostnamen für das Produktionsmanagement zu, und stellen Sie sie online. Da dieselbe IP-Adresse und derselbe Hostname verwendet werden, können die verwalteten FTD-Geräte automatisch eine Verbindung zum FMC herstellen, ohne dass Änderungen an der Manager-Adresse einzelner FTD-Geräte erforderlich sind.

Schritt 6: Validierung nach der Migration:

- Überprüfen Sie, ob alle verwalteten FTD-Geräte wieder mit der neuen FMCv-Instanz verbunden wurden.

- Überprüfen Sie den Lizenzstatus, und bestätigen Sie, dass alle Lizenzen korrekt

angewendet wurden.

- Bestätigen Sie, dass der Ereignisfluss und alle externen Integrationen ordnungsgemäß funktionieren.
- Führen Sie eine kontrollierte Richtlinienbereitstellung auf einem verwalteten Gerät aus, und bestätigen Sie, dass sie erfolgreich ist.

Wenn die Validierung in dieser Phase zu einem beliebigen Zeitpunkt fehlschlägt, schalten Sie die neue FMCv-Instanz aus, stellen Sie die ursprüngliche FMCv auf ESXi 7.0 wieder her, und beheben Sie die Fehler, bevor Sie die Migration erneut versuchen. Verwenden Sie keine VMware-Snapshot-Wiederherstellung als Rollback-Mechanismus.

Phase 4: Upgrade von FMCv von 7.4.2 auf 7.6.6 (nach Bestätigung der Migration als stabil)

Sobald die FMCv-Migration auf ESXi 8.0.3 vollständig validiert und als stabil bestätigt wurde, kann ein weiteres Upgrade auf FMC 7.6.6 in Betracht gezogen werden. Es wird dringend empfohlen, die Migration der Hypervisor-Plattform (Phase 3) und dieses zusätzliche FMC-Versionsupgrade nicht in einem einzigen Wartungsfall zu kombinieren. Wenn Sie die Migration abschließen, erhalten Sie zunächst einen sauberen Prüfpunkt mit geringem Risiko, bevor Sie fortfahren.

Bevor Sie das Upgrade auf 7.6.6 starten, müssen Sie folgende Voraussetzungen erfüllen:

- Auf jedem verwalteten FTD-Gerät in der Umgebung wird Version 7.1 oder höher ausgeführt. FMC 7.6.6 unterstützt kein Management von FTD Devices < Version 7.1. In der dokumentierten Umgebung (FTD-Bereich: 7.2.8 bis 7.4.2) erfüllen alle Geräte diese Anforderung.
- Das FMCv-Ressourcenprofil (4 vCPUs, 32 GB RAM, 250 GB Festplatte) wurde anhand der FMC 7.6.6-Bereitstellungsrichtlinien hinsichtlich der Gesamtzahl der verwalteten Geräte und der Anforderungen an die Beibehaltung von Ereignissen in dieser Umgebung validiert.
- Der unterstützte Upgrade-Übergangspfad wird bestätigt: 7,4 → 7,6.
- Das FMC ist als eigenständig (nicht Teil eines Hochverfügbarkeitspaars) bestätigt.

Schritt 1: Erstellen und überprüfen Sie eine neue native FMC-Sicherung von der stabilen FMCv 7.4.2-Instanz auf ESXi 8.0.3. Speichern Sie sie an einem sicheren Remote-Speicherort.

Phase 2: Aktualisieren Sie FMCv von Version 7.4.2 auf Version 7.6.6.

Schritt 3: Führen Sie nach dem Upgrade eine abschließende Validierung durch:

- Überprüfen Sie, ob alle verwalteten FTD-Geräte wieder mit dem FMC verbunden sind.
- Bestätigen Sie, dass die Ereignisbehandlung und die Ereigniseingabe ordnungsgemäß funktionieren.
- Bestätigen Sie, dass der Lizenzierungsstatus korrekt ist.
- Führen Sie eine kontrollierte Richtlinienbereitstellung aus, um zu bestätigen, dass die Richtlinienanwendung erfolgreich ist.

Zusammenfassung von Upgrade-Pfad und Übergangssequenz

In der Tabelle sind der vollständige Stufenplan, die unterstützten Upgrade-Übergänge und die wichtigsten Maßnahmen in jeder Phase zusammengefasst:

Phase	Aktion	FMC-Version	Hypervisor	Unterstützter Übergang
Phase 1	Kompatibilitätsprüfung vor dem Upgrade; FTD-Versionen, FMC HA-Status und Ressourcenprofil bestätigen	7.3.1 (aktuell)	ESXi 7.0	N/A — nur Zubereitung
Phase 2	FMCv-Software aktualisieren natives Backup durchführen; Validierung verwalteter Geräte und der Richtlinienbereitstellung	7,3,1 → 7,4,2	ESXi 7.0	7.3 → 7.4 (unterstützt)
Phase 3	Bereitstellung eines neuen FMCv auf ESXi 8.0.3 natives Backup wiederherstellen; Cut-over mit derselben IP/Hostname; validieren	7.4.2 (keine Versionsänderung)	ESXi 7.0 → ESXi 8.0.3	Natives Backup/Wiederherstellung — unterstützte Methode

Phase 4	Nach stabiler Migration: Upgrade FMCv; Validierung von Geräteverbindungen, Lizenzen, Ereignissen und Richtlinien	7,4,2 → 7,6,6	ESXi 8.0.3	7.4 → 7.6 (unterstützt)

Wichtige Überlegungen

- Upgrade-Pfad-Compliance: Die vollständige Upgrade-Sequenz - 7.3.1 → 7.4.2 → 7.6.6 - verwendet die unterstützten FMC-Upgrade-Übergangsoptionen (7.3 → 7.4 und 7.4 → 7.6). Das Überspringen von Zwischenversionen oder das Kombinieren von Phasen zu einem einzelnen Ereignis wird nicht empfohlen.
- FMC-FTD-Kompatibilität: FMC 7.6.6 gewährleistet die volle Verwaltungskompatibilität mit FTD-Geräten der Versionen 7.2.8 bis 7.4.2. FMC 7.6 setzt voraus, dass alle verwalteten FTD-Geräte Version 7.1 oder höher aufweisen.
- Gleiche IP-Adressumstellung: Das ursprüngliche FMCv muss vollständig ausgeschaltet oder vom Netzwerk getrennt werden, bevor das Ersatz-FMCv mit der IP-Adresse für das Produktionsmanagement online geschaltet wird. Dadurch wird eine doppelte IP-Adresse verhindert, und es wird vermieden, dass zwei Verwaltungszentren gleichzeitig versuchen, mit denselben FTD-Geräten zu kommunizieren. Wenn das wiederhergestellte FMCv mit derselben IP-Adresse und demselben Hostnamen zurückkehrt, können verwaltete FTD-Geräte die Verbindung wiederherstellen, ohne dass Änderungen an der Manager-Adresse erforderlich sind.
- Ressourcenvalidierung vor 7.6.6: Das FMCv-Ressourcenprofil (4 vCPUs, 32 GB RAM, 250 GB Festplatte) muss vor dem Upgrade auf FMC 7.6.6 anhand der aktuellen Bereitstellungsrichtlinien überprüft werden. Dabei sind die Gesamtzahl der verwalteten Geräte und die Anforderungen an die Beibehaltung von Ereignissen für die Umgebung zu berücksichtigen.
- Überprüfung der nativen Sicherung: In jeder Phase, in der ein natives FMC-Backup durchgeführt wird, muss das Backup als vollständig und gültig verifiziert werden, bevor fortgefahren werden kann. Sicherungen müssen an einem sicheren Remote-Speicherort außerhalb des virtuellen FMCv-Systems gespeichert werden.
- Migration und Upgrade nicht kombinieren: Die Plattformmigration (Phase 3) und das anschließende FMC-Versionsupgrade auf 7.6.6 (Phase 4) müssen als separate Wartungsereignisse durchgeführt werden. Dadurch wird sichergestellt, dass bei FMCv 7.4.2 auf ESXi 8.0.3 ein sauberer Prüfpunkt vorhanden ist, bevor weitere Änderungen vorgenommen werden.

Ursache

Dies ist kein Problem mit der Behebung von Softwarefehlern, das auf einen Softwarefehler oder eine Fehlkonfiguration zurückzuführen ist. Der zugrunde liegende Grund, der diese Anleitung erfordert, ist eine Kombination aus Versionskompatibilitätsanforderungen und Einschränkungen der Plattformmigration speziell für Cisco FMCv auf VMware:

- FMC-Versionskompatibilität mit FTD 7.4.2: Wenn ein verwaltetes FTD-Gerät mit Version 7.4.2 in der Umgebung vorhanden ist, muss das FMC auf mindestens Version 7.4.2 aktualisiert werden, da ältere FMC-Versionen FTD-Geräte mit einer höheren Version als das FMC selbst nicht verwalten können.
- FMCv-Unterstützung für VMware ESXi 8.0: FMCv 7.3.1 unterstützt VMware ESXi 8.0 nicht als Hypervisor-Plattform. Das FMCv muss auf Version 7.4.2 (oder höher) aktualisiert werden, bevor es auf ESXi 8.0.x bereitgestellt oder betrieben werden kann. Der Versuch, die VM FMCv 7.3.1 direkt auf ESXi 8.0 zu migrieren, ohne zuerst die FMC-Software zu aktualisieren, birgt ein Kompatibilitätsrisiko.
- Nicht unterstützte VM-Migrationsmethoden: VMware vMotion, Snapshots, Klonen und direkte VM-Migration werden für die Migration von FMCv zwischen Clustern oder Hypervisor-Versionen nicht unterstützt. Diese Methoden können zu Datenbankbeschädigungen, Versionskonflikten oder einem nicht unterstützten Systemstatus führen. Der einzige unterstützte Migrationspfad ist der native Backup- und Wiederherstellungs-Workflow des FMC in Kombination mit einer neuen FMCv-Bereitstellung auf der Zielplattform.

Verwandte Inhalte

- Upgrade-Leitfaden für Cisco Secure Firewall Management Center, Version 7.4 - Upgrade-Planung und unterstützte Pfade
- Upgrade-Leitfaden für Cisco Secure Firewall Management Center, Version 7.6 - Upgrade-Planung und unterstützte Pfade
- Kompatibilitätsleitfaden für Cisco Secure Firewall Management Center (FMC- und FTD-Kompatibilitätsmatrix)
- Cisco Secure Firewall Management Center Neue Funktionen nach Version 7.4.2
- Cisco FirePOWER Management Center Upgrade-Leitfaden - Upgrade-Planung

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.