FMCv upgraden en migreren van VMware ESXi 7.0 naar ESXi 8.0: gefaseerde aanpak en best practices

Inhoud

uitgifte

Een beheerder met Firewall Management Center virtual (FMCv) versie 7.3.1 op VMware ESXi 7.0 is van plan de FMC te upgraden naar een hoger ondersteunde versie en vervolgens de FMCv virtuele machine te migreren naar een nieuw VMware ESXi 8.0-cluster. Deze punten van zorg werden tijdens deze planning naar voren gebracht:

- Of het veilig is om eerst FMCv te upgraden van 7.3.1 naar 7.4.2 en vervolgens de VM naar het ESXi 8.0-cluster te migreren voordat u verdere upgrades uitvoert.
- Of er bekende compatibiliteitsproblemen of -beperkingen zijn bij het migreren van een FMCv met versie 7.3.1 of 7.4.2 naar een VMware ESXi 8.0-omgeving.
- Of VMware vMotion kan worden gebruikt om een naadloze, same-IP-migratie van de virtuele FMCv-machine naar het nieuwe cluster uit te voeren zonder een nieuwe VM-instantie te maken.
- Of VMware-momentopnamen kunnen worden gebruikt als back-up- en terugdraaimechanisme in het geval dat de upgrade of migratie mislukt.
- Wat de best ondersteunde FMC-versie is voor het bestaande landschap van beheerde apparaten, waaronder Firewall Threat Defense (FTD)-apparaten, variërend van versie 7.2.8 tot 7.4.2.
- Hoe IP-adresconflicten te voorkomen bij het overschakelen naar de nieuwe FMCv-instantie op het nieuwe cluster terwijl hetzelfde beheer van IP-adres en hostnaam wordt behouden.
- Wat de juiste volgorde is voor een gefaseerd upgrade- en migratieplan dat risico's en downtime minimaliseert.

milieu

- Product: FMCv
- Huidige FMC-softwareversie: 7.3.1
- Huidig hypervisorplatform: VMware ESXi 7.0
- Doelhypervisorplatform: VMware ESXi 8.0.3 (nieuw cluster)
- FMC-implementatietype: Standalone (geen onderdeel van een paar met hoge beschikbaarheid)
- Beheerde apparaten: meerdere FTD-apparaten, variërend van versie 7.2.8 tot 7.4.2

resolutie

De aanbevolen aanpak voor deze omgeving is een gefaseerd upgrade- en migratieplan. In dit plan worden de FMC-software-upgrade, de migratie van het hypervisorplatform en alle daaropvolgende FMC-versie-upgrades gescheiden in afzonderlijke onderhoudsgebeurtenissen. Deze aanpak vermindert het risico in elke fase en zorgt voor duidelijke terugdraaipunten. Het gebruik van VMware vMotion, momentopnamen, klonen of directe migratie op VM-niveau is expliciet niet de ondersteunde methode voor het migreren van FMCv tussen clusters of versies.

Belangrijk: VMware-momentopnamen, vMotion en klonen worden niet ondersteund voor FMCv-migratie

Alvorens verder te gaan met een fase van dit plan, is het van cruciaal belang om deze beperkingen met betrekking tot VMware-native migratiemethoden te begrijpen:

- VMware-momentopnamen zijn geen ondersteunde back-up-, herstel- of terugdraaimethode voor FMCv-upgrades of -migraties. Het terugzetten van een FMCv naar een VMware-momentopname kan leiden tot beschadiging van de database, mismatches tussen versie- en inhoudsupdates of een niet-ondersteunde systeemstatus.
- VMware vMotion, klonen en directe migratie van virtuele machines tussen clusters zijn niet de ondersteunde methode voor het migreren van FMCv naar een nieuw hypervisorplatform. Deze methoden omzeilen de interne gegevensintegriteitsmechanismen van het VCC.
- De enige ondersteunde methode voor het migreren van FMCv naar een nieuw cluster of een nieuwe host is de FMC-workflow voor back-up en herstel, gecombineerd met het implementeren van een nieuwe FMCv-instantie op het doelplatform.

De juiste terugdraaistrategie is om, als de validatie mislukt na het afsnijden, de nieuwe FMCv-instantie uit te schakelen en de oorspronkelijke FMCv weer in gebruik te nemen. Vertrouw niet op snapshot-teruggangen voor dit doel.

Fase 1: Compatibiliteitscontrole vóór de upgrade

Voordat u een FMC-software-upgrade start, controleert u de exacte softwareversies van alle beheerde FTD-apparaten in de omgeving.

- FMC 7.4.2 ondersteunt het beheer van FTD-apparaten met versie 7.0 en hoger.
- FMC 7.6.6 ondersteunt het beheer van FTD-apparaten met versie 7.1 en hoger.
- Als een FTD-apparaat in de omgeving een versie < 7.0 uitvoert, moet dat apparaat worden geüpgraded naar ten minste versie 7.0 terwijl de FMC op versie 7.3.1 blijft, voordat de FMC zelf wordt geüpgraded.
- Voor de gedocumenteerde omgeving (FTD-bereik: 7.2.8 tot 7.4.2) vallen alle beheerde apparaten binnen het compatibiliteitsbereik voor zowel FMC 7.4.2 als FMC 7.6.6. In dit geval is geen FTD-pre-upgrade vereist.

Bevestig deze ook voordat u verder gaat:

- Het FMC is op zichzelf staand en maakt geen deel uit van een paar met hoge beschikbaarheid (HA).
- De exacte VMware ESXi 8.0 is gebaseerd op het nieuwe cluster (in deze omgeving bevestigd als ESXi 8.0.3).
- Het FMCv-bronprofiel (vCPU's, geheugen, schijf) voldoet aan de vereisten voor de FMC-doelversie. De huidige specificatie van 4 vCPU's, 32 GB RAM en 250 GB schijf moet worden beoordeeld in het licht van de huidige implementatierichtlijnen, met name voordat een upgrade naar FMC 7.6.6 wordt uitgevoerd.
- Of het IP-adres en de hostnaam van het FMC-beheer na de migratie hetzelfde blijven (sterk aanbevolen om te voorkomen dat updates van het beheeradres op alle beheerde FTD-apparaten nodig zijn).

Fase 2: Upgrade bestaande FMCv van 7.3.1 naar 7.4.2 op het huidige ESXi 7.0-cluster

In deze fase wordt de FMCv-software geüpgraded naar versie 7.4.2, terwijl deze op de bestaande ESXi 7.0-infrastructuur blijft. FMCv 7.4.2 voegt expliciete ondersteuning toe voor VMware ESXi 8.0, die vereist is voordat de platformmigratie in fase 3 plaatsvindt.

Stap 1: Bevestig dat er momenteel geen beleidsimplementaties in behandeling zijn, geen actieve back-uptaken of achtergrondtaken worden uitgevoerd op de FMC voordat de upgrade wordt gestart.

Stap 2: Voer een volledige native FMC-back-up uit met het ingebouwde FMC-hulpprogramma voor back-ups. Bewaar de back-up op een veilige, externe locatie buiten de virtuele FMCv-machine. Controleer of de back-up is voltooid voordat u verdergaat.

Stap 3: Voltooi alle upgradegereedheidscontroles zoals beschreven in de FMC 7.4-gids voor upgradeplanning. Los gemarkeerde problemen op voordat u de upgrade start.

Stap 4: Upgrade de bestaande FMCv van versie 7.3.1 naar versie 7.4.2. Dit maakt gebruik van het ondersteunde upgradetransitiepad: 7,3 → 7,4.

Stap 5: Nadat de upgrade is voltooid, voert u de validatie na de upgrade uit:

- Controleer of alle beheerde FTD-apparaten opnieuw verbinding hebben gemaakt met de FMC.
- Bevestig dat de opname van een gebeurtenis actief is en dat er gebeurtenissen verschijnen in het VCC.
- Bevestig dat de licentiestatus juist is.
- Voer een implementatie van testbeleid uit op een beheerd apparaat en bevestig dat het is gelukt.

Ga niet door naar fase 3 totdat alle validatiestappen na de upgrade met succes zijn doorgegeven aan de geüpgradede FMCv 7.4.2.

Fase 3: migratie van FMCv naar het VMware ESXi 8.0.3-cluster met behulp van native back-up en herstel

In deze fase wordt de FMCv gemigreerd van het bestaande ESXi 7.0-cluster naar het nieuwe

ESXi 8.0.3-cluster. Dit wordt bereikt door een nieuwe FMCv-instantie op het doelcluster te implementeren en er een standaard FMC-back-up op terug te zetten. Hetzelfde beheer-IP-adres en dezelfde hostnaam worden behouden om te voorkomen dat wijzigingen in het beheeradres op alle beheerde FTD-apparaten nodig zijn.

Stap 1: Nadat de FMCv is bevestigd als stabiel op versie 7.4.2, genereert u een nieuwe native FMC-back-up. Bewaar het op een veilige, externe locatie. Controleer of de back-up volledig en geldig is voordat u verdergaat.

Stap 2: Implementeer een nieuwe FMCv-instantie op het ESXi 8.0.3-cluster. De softwareversie en de build van deze nieuwe installatie moeten exact overeenkomen met de versie van de FMCv (inclusief patches en hotfixes) van waaruit de back-up is gemaakt (FMCv 7.4.2). Zorg ervoor dat de nieuwe installatie is geconfigureerd met gelijkwaardige of grotere bronnen (vCPU's, geheugen, schijf) en dat de netwerkconfiguratie is gefaseerd, maar het IP-adres voor productiebeheer is op dit moment nog niet toegewezen aan de nieuwe installatie.

Stap 3: Herstel de oorspronkelijke FMC-back-up op de nieuwe FMCv-instantie op ESXi 8.0.3.

Stap 4: Voordat u de nieuwe FMCv online brengt met het IP-adres en de hostnaam van het productiebeheer, moet u de oorspronkelijke FMCv volledig uitschakelen of loskoppelen van het netwerk. Dit is een verplichte stap om een dubbele IP-voorwaarde te voorkomen en om te voorkomen dat twee FMC-instanties tegelijkertijd proberen te communiceren met dezelfde beheerde FTD-apparaten.

Tijdens de periode waarin de oorspronkelijke FMCv is uitgeschakeld en voordat de nieuwe FMCv online is, wordt dit gedrag verwacht voor de beheerde FTD-apparaten:

- Traffic Forwarding: FTD-apparaten bedienen gegevensvliegtuigen onafhankelijk van het FMC en blijven het verkeer naadloos doorsturen en het laatste met succes geïmplementeerde toegangscontrolebeleid handhaven, behalve de gevallen die hier worden genoemd.
- Wijzigingen in beheer en zichtbaarheid: beleidsimplementaties, configuratieaanpassingen, FMC-waarschuwingen en zichtbaarheid van apparaatbeheer zijn volledig niet beschikbaar.
- Eventbuffering en potentieel verlies: Real-time zichtbaarheid van gebeurtenissen bij het FMC wordt onderbroken. Hoewel de FTD probeert beveiligings- en verbindingsevenementen lokaal te registreren in zijn tijdelijke unified-bestanden, hebben deze bestanden strikte opslaglimieten en werken ze op een cirkelvormige overschrijvingsbasis. Verbindingslogboeken met een hoog volume kunnen worden overschreven of verloren gaan tijdens een verlengd migratievenster. Evenementen die in de lokale buffer blijven, worden naar het nieuwe FMC gestreamd zodra deze online is.
- Malware (AMP) regels: Real-time cloud opzoeken van verzoeken voor niet-gecachte

bestanden zijn tijdelijk niet beschikbaar omdat de FMC deze reputatie query's proxyt naar de AMP Cloud. De FTD blijft blokkering afdwingen of regels toestaan alleen voor bestanden die al zijn opgeslagen in de lokale on-box dispositie cache. Niet-gecachte bestanden omzeilen de cloudanalyse en gebruiken de faalveilige instellingen van uw beleid (meestal niet geopend om verkeersverstoring te voorkomen). Sandboxing-inzendingen bij Threat Grid en retrospectieve waarschuwingen worden gepauzeerd totdat het nieuwe FMC operationeel is.

- Identiteitsgebaseerde regels: Gebruikers die al zijn ingelogd en toegewezen aan een IP-adres ervaren geen onderbreking, omdat de FTD actieve toewijzingen in het lokale geheugen behoudt. Omdat de FMC echter fungeert als de broker voor identiteitsbronnen (bijvoorbeeld Cisco ISE of Active Directory Agents), kunnen nieuwe gebruikersaanmeldingen of IP-wijzigingen tijdens dit venster niet door de FTD worden geleerd. Deze onbekende sessies vallen terug op de standaard- of gastregels van uw beleid.
- URL-filtering: Live cloud-zoekopdrachten voor volledig onbekende websites zijn tijdelijk niet beschikbaar omdat de FMC onbekende URL-verzoeken naar de Cisco Talos-cloud proxyt. De FTD blijft het beleid alleen volledig filteren en handhaven voor websites die al zijn gevonden in zijn gepushte lokale dataset of zijn actieve lokale geheugencache. Webverkeer dat een niet-gecachte, onbekende URL raakt, omzeilt de cloudclassificatie en komt overeen met de fallback-instellingen van uw beleid voor niet-gecategoriseerd verkeer (meestal toegestaan). Updates van URL-databasepakketten worden onderbroken totdat het nieuwe FMC online is.

Stap 5: Wijs het IP-adres en de hostnaam van het productiebeheer toe aan de herstelde FMCv op ESXi 8.0.3 en breng het online. Omdat hetzelfde IP-adres en dezelfde hostnaam worden gebruikt, kunnen de beheerde FTD-apparaten automatisch opnieuw verbinding maken met de FMC zonder dat er wijzigingen in het beheeradres op afzonderlijke FTD-apparaten nodig zijn.

Stap 6: Validering na migratie uitvoeren:

- Controleer of alle beheerde FTD-apparaten opnieuw verbinding hebben gemaakt met de nieuwe FMCv-instantie.
- Controleer de licentiestatus en controleer of alle licenties correct zijn toegepast.
- Bevestig dat de gebeurtenisstroom en eventuele externe integraties correct werken.
- Voer een beheerste beleidsimplementatie uit op een beheerd apparaat en bevestig dat het is gelukt.

Als de validatie op enig moment tijdens deze fase mislukt, schakelt u de nieuwe FMCv-instantie uit, zet u de oorspronkelijke FMCv op ESXi 7.0 terug in bedrijf en lost u problemen op voordat u de migratie opnieuw probeert. Gebruik een VMware-momentopname niet als terugdraaimechanisme.

Fase 4: upgrade FMCv van 7.4.2 naar 7.6.6 (nadat de migratie stabiel is bevestigd)

Zodra de FMCv-migratie naar ESXi 8.0.3 volledig is gevalideerd en stabiel is bevonden, kan een verdere upgrade naar FMC 7.6.6 worden overwogen. Het wordt sterk aanbevolen om de migratie van het hypervisorplatform (fase 3) en deze extra FMC-versie-upgrade niet te combineren tot één onderhoudsgebeurtenis. Als u de migratie eerst voltooit, krijgt u een schoon controlepunt met een laag risico voordat u verder gaat.

Voordat u de upgrade naar 7.6.6 start, moet u de volgende voorwaarden bevestigen:

- Elk beheerd FTD-apparaat in de omgeving draait versie 7.1 of hoger. FMC 7.6.6 ondersteunt geen beheer van FTD-apparaten < versie 7.1. In de gedocumenteerde omgeving (FTD-bereik: 7.2.8 tot 7.4.2) voldoen alle apparaten aan deze vereiste.
- Het FMCv-bronprofiel (4 vCPU's, 32 GB RAM, 250 GB schijf) is gevalideerd volgens de implementatierichtlijnen van FMC 7.6.6 voor het totale aantal beheerde apparaten en de vereisten voor het bewaren van gebeurtenissen in deze omgeving.
- Het ondersteunde upgradetransitiepad wordt bevestigd: 7,4 → 7,6.
- De FMC wordt bevestigd als standalone (geen onderdeel van een High Availability-paar).

Stap 1: Maak en verifieer een nieuwe native FMC-back-up vanaf de stabiele FMCv 7.4.2-instantie op ESXi 8.0.3. Bewaar het op een veilige, externe locatie.

Stap 2: Upgrade de FMCv van versie 7.4.2 naar versie 7.6.6.

Stap 3: Voer de laatste validatie na de upgrade uit:

- Controleer of alle beheerde FTD-apparaten opnieuw verbinding hebben gemaakt met de FMC.
- Bevestig dat gebeurtenisafhandeling en gebeurtenisinname correct werken.
- Bevestig dat de licentiestatus juist is.
- Voer een beheerste beleidsimplementatie uit om te bevestigen dat de beleidstoepassing succesvol is.

Overzicht van het upgradepad en de overgangsreeks

De tabel geeft een overzicht van het volledige stappenplan, de ondersteunde upgradeovergangen en de belangrijkste actie in elke fase:

fase	Actie	FMC-versie	hypervisor	Ondersteunde overgang
Fase 1	Compatibiliteitscontrole vóór upgrade; FTD-versies, FMC HA-status en bronprofiel bevestigen	7.3.1 (actueel)	ESXi 7.0	N.v.t. — alleen voorbereiding
Fase 2	FMCv-software upgraden; native back-up uitvoeren; beheerde apparaten en beleidsimplementatie valideren	7.3.1 → 7.4.2	ESXi 7.0	7,3 → 7,4 (ondersteund)
Fase 3	Nieuwe FMCv implementeren op ESXi 8.0.3; native back-up terugzetten; overschakelen met dezelfde IP/hostnaam; valideren	7.4.2 (geen wijzigingen in de versie)	ESXi 7.0 → ESXi 8.0.3	Standaard back-up/herstel — ondersteunde methode
Fase 4	Nadat de migratie stabiel is: upgrade FMCv; valideer apparaatconnectiviteit, licenties, gebeurtenissen, beleid	7.4.2 → 7.6.6	ESXi 8.0.3	7,4 → 7,6 (ondersteund)

Belangrijkste overwegingen

- Upgrade Path Compliance: De volledige upgradevolgorde — 7.3.1 → 7.4.2 → 7.6.6 — maakt gebruik van de ondersteunde FMC-upgradeovergangspaden (7.3 → 7.4 en 7.4 → 7.6). Het overslaan van tussenversies of het combineren van fasen tot één gebeurtenis wordt niet aanbevolen.
- FMC-FTD-compatibiliteit: FMC 7.6.6 behoudt volledige beheercompatibiliteit met FTD-apparaten met versies 7.2.8 tot en met 7.4.2. Voor FMC 7.6 moeten alle beheerde FTD-apparaten versie 7.1 of hoger hebben.
- Hetzelfde IP-adresprogramma: de oorspronkelijke FMCv moet volledig worden uitgeschakeld of losgekoppeld van het netwerk voordat de vervangende FMCv online wordt gebracht met het IP-adres voor productiebeheer. Dit voorkomt een duplicate-IP-voorwaarde en voorkomt dat twee beheercentra tegelijkertijd proberen te communiceren met dezelfde FTD-apparaten. Wanneer de teruggezette FMCv terugkeert met hetzelfde IP-adres en dezelfde hostnaam, kunnen beheerde FTD-apparaten opnieuw verbinding maken zonder

wijzigingen in het beheerdersadres.

- Vóór 7.6.6: Het FMCv-bronprofiel (4 vCPU's, 32 GB RAM, 250 GB schijf) moet worden beoordeeld aan de hand van de huidige implementatierichtlijnen voordat een upgrade naar FMC 7.6.6 wordt uitgevoerd, waarbij rekening wordt gehouden met het totale aantal beheerde apparaten en de vereisten voor het bewaren van gebeurtenissen voor de omgeving.
- Verificatie van native back-up: in elke fase waarin een native FMC-back-up wordt gemaakt, moet de back-up worden geverifieerd als voltooid en geldig voordat u verdergaat. Back-ups moeten worden opgeslagen op een veilige, externe locatie buiten de virtuele FMCv-machine.
- Migratie en upgrade niet combineren: de platformmigratie (fase 3) en de daaropvolgende FMC-versie-upgrade naar 7.6.6 (fase 4) moeten als afzonderlijke onderhoudsgebeurtenissen worden uitgevoerd. Dit zorgt ervoor dat er een schoon controlepunt bestaat bij FMCv 7.4.2 op ESXi 8.0.3 voordat er verdere wijzigingen worden aangebracht.

Oorzaak

Dit is geen probleem met de oplossing van een defect of een verkeerde configuratie van de software. De onderliggende oorzaak die deze richtlijnen vereist, is een combinatie van vereisten voor versiecompatibiliteit en beperkingen voor platformmigratie die specifiek zijn voor de Cisco FMCv op VMware:

- FMC-versie compatibiliteit met FTD 7.4.2: De aanwezigheid van een beheerd FTD-apparaat met versie 7.4.2 in de omgeving vereist dat de FMC wordt opgewaardeerd naar een minimum van versie 7.4.2, omdat eerdere FMC-versies FTD-apparaten niet kunnen beheren met een hogere versie dan de FMC zelf.
- FMCv-ondersteuning voor VMware ESXi 8.0: FMCv 7.3.1 ondersteunt VMware ESXi 8.0 niet als hypervisorplatform. De FMCv moet worden geüpgraded naar versie 7.4.2 (of hoger) voordat deze kan worden geïmplementeerd of gebruikt op ESXi 8.0.x. Als u probeert de VM van FMCv 7.3.1 rechtstreeks naar ESXi 8.0 te migreren zonder eerst een upgrade van de FMC-software uit te voeren, loopt u een compatibiliteitsrisico.
- Niet-ondersteunde VM-migratiemethoden: VMware vMotion, momentopnamen, klonen en directe VM-migratie worden niet ondersteund voor het migreren van FMCv tussen clusters of hypervisorversies. Deze methoden kunnen leiden tot beschadiging van de database, mismatches van versies of een niet-ondersteunde systeemstatus. Het enige ondersteunde migratiepad is de standaard FMC-workflow voor back-up en herstel in combinatie met een nieuwe FMCv-implementatie op het doelplatform.

Gerelateerde inhoud

- Cisco Secure Firewall Management Center Upgradehandleiding, versie 7.4 — Upgradeplanning en ondersteunde paden
- Cisco Secure Firewall Management Center Upgradehandleiding, versie 7.6 — Upgradeplanning en ondersteunde paden
- Compatibiliteitsgids voor Cisco Secure Firewall Management Center (FMC- en FTD-compatibiliteitsmatrix)
- Cisco Secure Firewall Management Center Nieuwe functies per release — versie 7.4.2
- Upgradehandleiding Cisco Firepower Management Center — Upgradeplanning
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.