Firepower Management Center High Availability

The following topics describe how to configure Active/Standby high availability of Cisco Firepower Management Centers:

About Firepower Management Center High Availability

To ensure the continuity of operations, the high availability feature allows you to designate redundant Firepower Management Centers to manage devices. Firepower Management Centers support Active/Standby high availability where one appliance is the active unit and manages devices. The standby unit does not actively manage devices. The active unit writes configuration data into a data store and replicates data for both units, using synchronization where necessary to share some information with the standby unit.

Active/Standby high availability lets you configure a secondary Firepower Management Center to take over the functionality of a primary Firepower Management Center if the primary fails. When the primary Firepower Management Center fails, you must promote the secondary Firepower Management Center to become the active unit.

Event data streams from managed devices to both Firepower Management Centers in the high availability pair. If one Firepower Management Center fails, you can monitor your network without interruption using the other Firepower Management Center.

Note that Firepower Management Centers configured as a high availability pair do not need to be on the same trusted management network, nor do they have to be in the same geographic location.

Caution Because the system restricts some functionality to the active Firepower Management Center, if that appliance fails, you must promote the standby Firepower Management Center to active.

About Remote Access VPN High Availability

If the primary device has Remote Access VPN configuration with an identity certificate enrolled using a CertEnrollment object, the secondary device must have an identity certificate enrolled using the same CertEnrollment object. The CertEnrollment object can have different values for the primary and secondary devices due to device-specific overriddes. The limitation is only to have the same CertEnrollment object enrolled on the two devices before the high availability formation.

SNMP Behavior in Firepower Management Center High Availability

In an SNMP-configured HA pair, when you deploy an alert policy, the primary Firepower Management Center sends the SNMP traps. When the primary Firepower Management Center fails, the secondary Firepower Management Center, which becomes the active unit, sends the SNMP traps without the need for any additional configuration.

Roles v. Status in Firepower Management Center High Availability

Primary/Secondary Roles

When setting up Firepower Management Centers in a high availability pair, you configure one Firepower Management Center to be primary and the other as secondary. During configuration, the primary unit's policies are synchronized to the secondary unit. After this synchronization, the primary Firepower Management Center becomes the active peer, while the secondary Firepower Management Center becomes the standby peer, and the two units act as a single appliance for managed device and policy configuration.

Active/Standby Status

The main differences between the two Firepower Management Centers in a high availability pair are related to which peer is active and which peer is standby. The active Firepower Management Center remains fully functional, where you can manage devices and policies. On the standby Firepower Management Center, functionality is hidden; you cannot make any configuration changes.

Event Processing on Firepower Management Center High Availability Pairs

Since both Firepower Management Centers in a high availability pair receive events from managed devices, the management IP addresses for the appliances are not shared. This means that you do not need to intervene to ensure continuous processing of events if a Firepower Management Center fails.

AMP Cloud Connections and Malware Information

Although they share file policies and related configurations, Firepower Management Centers in a high availability pair share neither Cisco AMP cloud connections nor malware dispositions. To ensure continuity of operations, and to ensure that detected files' malware dispositions are the same on both Firepower Management Centers, both primary and secondary Firepower Management Centers must have access to the AMP cloud.

URL Filtering and Security Intelligence

URL filtering and Security Intelligence configurations and information are synchronized between Firepower Management Centers in a high availability deployment. However, only the primary Firepower Management Center downloads URL category and reputation data for updates to Security Intelligence feeds.

If the primary Firepower Management Center fails, not only must you make sure that the secondary Firepower Management Center can access the internet to update threat intelligence data, but you must also use the web interface on the secondary Firepower Management Center to promote it to active.

User Data Processing During Firepower Management Center Failover

If the primary Firepower Management Center fails, the Secondary Firepower Management Center propagates to managed devices user-to-IP mappings from the TS Agent identity source; and propagates SGT mappings from the ISE/ISE-PIC identity source. Users not yet seen by identity sources are identified as Unknown.

After the downtime, the Unknown users are re identified and processed according to the rules in your identity policy.

Configuration Management on Firepower Management Center High Availability Pairs

In a high availability deployment, only the active Firepower Management Center can manage devices and apply policies. Both Firepower Management Centers remain in a state of continuous synchronization.

If the active Firepower Management Center fails, the high availability pair enters a degraded state until you manually promote the standby appliance to the active state. Once the promotion is complete, the appliances leave maintenance mode.

Threat Intelligence Director and High Availability Configurations

If you host TID on the active Firepower Management Center in a high availability configuration, the system does not synchronize TID configurations and TID data to the standby Firepower Management Center. We recommend performing regular backups of TID data on your active Firepower Management Center so that you can restore the data after failover.

For details, see About Backing Up and Restoring TID Data.

Single Sign-On and High Availability Pairs

FMCs in a high availability configuration can support Single Sign-On, but you must keep the following considerations in mind:

- SSO configuration is not synchronized between the members of the high availability pair; you must configure SSO separately on each member of the pair.
- Both FMCs in a high availability pari must use the same identity provider (IdP) for SSO. You must configure a service provider application at the IdP for each FMC configured for SSO.
- In a high availabilty pair of FMCs where both are configured to support SSO, before a user can use SSO to access the secondary FMC for the first time, that user must first use SSO to log into the primary FMC at least once.
- When configuring SSO for FMCs in a high availability pair:
  - If you configure SSO on the primary FMC, you are not required to configure SSO on the secondary FMC.
  - If you configure SSO on the secondary FMC, you are required to configure SSO on the primary FMC as well. (This is because SSO users must log in to the primary FMC at least once before logging into the secondary FMC.)

Related Topics

Configure SAML Single Sign-On

Firepower Management Center High Availability Behavior During a Backup

When you perform a Backup on a Firepower Management Center high availability pair, the Backup operation pauses synchronization between the peers. During this operation, you may continue using the active Firepower Management Center, but not the standby peer.

After Backup is completed, synchronization resumes, which briefly disables processes on the active peer. During this pause, the High Availability page briefly displays a holding page until all processes resume.

Firepower Management Center High Availability Split-Brain

If the active Firepower Management Center in a high-availability pair goes down (due to power issues, network/connectivity issues), you can promote the standby Firepower Management Center to an active state. When the original active peer comes up, both peers can assume they are active. This state is defined as 'split-brain'. When this situation occurs, the system prompts you to choose an active appliance, which demotes the other appliance to standby.

If the active Firepower Management Center goes down (or disconnects due to a network failure), you may either break high availability or switch roles. The standby Firepower Management Center enters a degraded state.

Note Whichever appliance you use as the secondary loses all of its device registrations and policy configurations when you resolve split-brain. For example, you would lose modifications to any policies that existed on the secondary but not on the primary. If the Firepower Management Center is in a high availability split-brain scenario where both appliances are active, and you register managed devices and deploy policies before you resolve split-brain, you must export any policies and unregister any managed devices from the intended standby Firepower Management Center before re-establishing high availability. You may then register the managed devices and import the policies to the intended active Firepower Management Center.

Upgrading Firepower Management Centers in a High Availability Pair

Cisco electronically distributes several different types of updates periodically. These include major and minor upgrades to the system software. You may need to install these updates on Firepower Management Centers in a high availability setup.

Warning Make sure that there is at least one operational Firepower Management Center during an upgrade.

Before you begin

Read the release notes or advisory text that accompanies the upgrade. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

Procedure

Step 1 Access the web interface of the active Firepower Management Center and pause data synchronization; see Pausing Communication Between Paired Firepower Management Centers, on page 14.

Step 2 Upgrade the standby Firepower Management Center; see the upgrade guide.
When the upgrade completes, the standby unit becomes active. When both peers are active, the high availability pair is in a degraded state (split-brain).

Step 3 Upgrade the other Firepower Management Center.

Step 4 Decide which Firepower Management Center you want to use as the standby. Any additional devices or policies added to the standby after pausing synchronization are not synced to the active Firepower Management Center. Unregister only those additional devices and export any configurations you want to preserve.

When you choose a new active Firepower Management Center, the Firepower Management Center you designate as secondary will lose device registrations and deployed policy configurations, which are not synced.

Step 5 Resolve split-brain by choosing the new active Firepower Management Center which has all the latest required configurations for policies and devices.

Troubleshooting Firepower Management Center High Availability

This section lists troubleshooting information for some common Firepower Management Center high availability operation errors.

Error	Description	Solution
You must reset your password on the active Firepower Management Center before you can log into the standby	You attempted to log into the standby FMC when a force password reset is enabled for your account.	As the database is read-only for a standby FMC, reset the password on the login page of the active FMC.

Error	Description	Solution
500 Internal	May appear when attempting to access the web interface while performing critical Firepower Management Center high availability operations, including switching peer roles or pausing and resuming synchronization.	Wait until the operation completes before using the web interface.
System processes are starting, please wait Also, the web interface does not respond.	May appear when the Firepower Management Center reboots (manually or while recovering from a power down) during a high availability or data synchronization operation.	1. Access the Firepower Management Center shell and use the `manage_hadc.pl` command to access the Firepower Management Center high availability configuration utility. **Note** Run the utility as a root user, using `sudo`. 2. Pause mirroring operations by using option 5. Reload the Firepower Management Center web interface. 3. Use the web interface to resume synchronization. Choose **System** > **Integration**, then click the **High Availability** tab and choose **Resume Synchronization**.

Requirements for Firepower Management Center High Availability

Model Support

See Hardware Requirements, on page 7.

Virtual Model Support

See Virtual Platform Requirements, on page 7.

Supported Domains

Global

User Roles

Admin

Hardware Requirements

- Supported hardware models:

  MC1000, MC1600, MC2500, MC2600, MC4500, MC4600

- The two Firepower Management Centers in a high availability configuration must be the same model.
- The primary Firepower Management Center backup must not be restored to the secondary Firepower Management Center.
- Bandwidth requirement for high availability configuration depends on various factors such as the size of the network, the number of managed devices, the volume of events and logs, and the size and frequency of configuration updates. For a typical Firepower Management Center high availability deployment, a minimum of 5 Mbps network bandwidth between the peers is recommended.
- The two Firepower Management Centers in a high availability configuration may be physically and geographically separated from each other in different data centers.
- See also License Requirements for FMC High Availability Configurations, on page 8.

Virtual Platform Requirements

Requirements for establishing high availability (HA) using two FMCv virtual appliances:

- FMCv must be running on VMware ESXi.
- FMCv-HA is supported on FMCv 10, 25, and 300.
- The two FMCv virtual appliances in a high availability configuration must have the same device management capacity. For example, you cannot pair an FMCv 25 with an FMCv 300.
- High availability licensing requirements are different for virtual vs hardware FMC. See License Requirements for FMC High Availability Configurations, on page 8.

Software Requirements

Access the **Appliance Information** widget to verify the software version, the intrusion rule update version and the vulnerability database update. By default, the widget appears on the **Status** tab of the **Detailed Dashboard** and the**Summary Dashboard**. For more information, see The Appliance Information Widget

- The two Firepower Management Centers in a high availability configuration must have the same major (first number), minor (second number), and maintenance (third number) software version.
- The two Firepower Management Centers in a high availability configuration must have the same version of the intrusion rule update installed.
- The two Firepower Management Centers in a high availability configuration must have the same version of the vulnerability database update installed.
- The two Firepower Management Centers in a high availability configuration must have the same version of the LSP (Lightweight Security Package) installed.

Warning If the software versions, intrusion rule update versions and vulnerability database update versions are not identical on both Firepower Management Centers, you cannot establish high availability.

License Requirements for FMC High Availability Configurations

Hardware Firepower Management Center: All Licensing Types

No special license is required for Firepower Management Center hardware appliances in a high availability pair.

A device managed with Firepower Management Center hardware appliances in a high availability configuration requires the same number of feature licenses and subscriptions as a device managed by a single Firepower Management Center hardware appliance.

In Specific License Reservation deployments, only the primary FMC requires a Specific License Reservation.

The system automatically replicates all feature licenses from active to standby Firepower Management Center when the high-availability pair is formed, and updates license changes during ongoing data synchronization, so the licenses are available on failover.

Virtual Firepower Management Center (FMCv): All Licensing Types

You will need two identically licensed FMCv's (with entitlements for 10, 25, or 300 managed devices.)

Example: For an FMCv high availability pair managing 10 FTD devices and 3 NGIPS devices, you need:

- Two (2) FMCv25 entitlements
- 10 FTD entitlements, as described below under Smart Licensing
- 3 NGIPS entitlements, as described below under Classic Licensing

If you break the high availability pair, the FMCv entitlements associated with the secondary FMCv are released. (In the example, you would then have two standalone FMCv25's.)

Smart Licensing

Each FTD device requires the same licenses whether managed by a single FMC or by FMCs in a high availability pair (hardware or virtual).

Example: If you want to enable advanced malware protection for two Firepower Threat Defense devices managed by a Firepower Management Center pair, buy two Malware licenses and two TM subscriptions, register the active Firepower Management Center with the Cisco Smart Software Manager, then assign the licenses to the two Firepower Threat Defense devices on the active Firepower Management Center.

Only the active Firepower Management Center is registered with Cisco Smart Software Manager. When failover occurs, the system communicates with Cisco Smart Software Manager to release the Smart License entitlements from the originally-active Firepower Management Center and assign them to the newly-active Firepower Management Center.

Classic Licensing

Each device requires the same licenses whether managed by a single FMC or by FMCs in a high availability pair (hardware or virtual).

Example: If you want to enable advanced malware protection for two devices managed by a Firepower Management Center pair, buy two Malware licenses and two TAM subscriptions, add those licenses to the Firepower Management Center, then assign the licenses to the two devices on the active Firepower Management Center.

Prerequisites for Firepower Management Center High Availability

Before establishing a Firepower Management Center high availability pair:

- Export required policies from the intended secondary Firepower Management Center to the intended primary Firepower Management Center. For more information, see Exporting Configurations.
- Make sure that the intended secondary Firepower Management Center does not have any devices added to it. Delete devices from the intended secondary Firepower Management Center and register these devices to the intended primary Firepower Management Center. For more information see Delete a Device from the FMC and Add a Device to the FMC.
- Import the policies into the intended primary Firepower Management Center. For more information, see Importing Configurations.
- On the intended primary Firepower Management Center, verify the imported policies, edit them as needed and deploy them to the appropriate device. For more information, see Deploy Configuration Changes.
- On the intended primary Firepower Management Center, associate the appropriate licenses to the newly added devices. For more information see Assign Licenses to Managed Devices from the Device Management Page.

You can now proceed to establish high availability. For more information, see Establishing Firepower Management Center High Availability, on page 9.

Establishing Firepower Management Center High Availability

Establishing high availability can take a significant amount of time, even several hours, depending on the bandwidth between the peers and the number of policies. It also depends on the number of devices registered to the active Firepower Management Center, which need to be synced to the standby Firepower Management Center. You can view the High Availability page to check the status of the high availability peers.

Before you begin

- Confirm that both the Firepower Management Centers adhere to the high availability system requirements. For more information , see Requirements for Firepower Management Center High Availability, on page 6.
- Confirm that you completed the prerequisites for establishing high availability. For more information, see Prerequisites for Firepower Management Center High Availability, on page 9.

Procedure

Step 1 Log into the Firepower Management Center that you want to designate as the secondary.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Under Role for this Firepower Management Center, choose **Secondary**.

Step 5 Enter the hostname or IP address of the primary Firepower Management Center in the **Primary Firepower Management Center Host** text box.

You can leave this empty if the primary Firepower Management Center does not have an IP address reachable from the peer FMC (which can be public or private IP address). In this case, use both the **Registration Key** and the **Unique NAT ID** fields. You need to specify the IP address of at least one FMC to enable HA connection.

Step 6 Enter a one-time-use registration key in the **Registration Key** text box.

The registration key is any user-defined alphanumeric value up to 37 characters in length. This registration key will be used to register both -the secondary and the primary Firepower Management Centers.

Step 7 If you did not specify the primary IP address, or if you do not plan to specify the secondary IP address on the primary Firepower Management Center, then in the **Unique NAT ID** field, enter a unique alphanumeric ID. See NAT Environments for more information.

Step 8 Click **Register**.

Step 9 Using an account with Admin access, log into the Firepower Management Center that you want to designate as the primary.

Step 10 Choose **System** > **Integration**.

Step 11 Choose **High Availability**.

Step 12 Under Role for this Firepower Management Center, choose **Primary**.

Step 13 Enter the hostname or IP address of the secondary Firepower Management Center in the **Secondary Firepower Management Center Host** text box.

You can leave this empty if the secondary Firepower Management Center does not have an IP address reachable from the peer FMC (which can be public or private IP address). In this case, use both the **Registration Key** and the **Unique NAT ID** fields. You need to specify the IP address of at least one FMC to enable HA connection.

Step 14 Enter the same one-time-use registration key in the **Registration Key** text box you used in step 6.

Step 15 If required, enter the same NAT ID that you used in step 7 in the **Unique NAT ID** text box.

Step 16 Click **Register**.

What to do next

After establishing a Firepower Management Center high availability pair, devices registered to the active Firepower Management Center are automatically registered to the standby Firepower Management Center.

Note When a registered device has a NAT IP address, automatic device registration fails and the secondary Firepower Management Center High Availablity page lists the device as local, pending. You can then assign a different NAT IP address to the device on the standby Firepower Management Center High Availability page. If automatic registration otherwise fails on the standby Firepower Management Center, but the device appears to be registered to the active Firepower Management Center, see Using CLI to Resolve Device Registration in Firepower Management Center High Availability, on page 13.

Viewing Firepower Management Center High Availability Status

After you identify your active and standby Firepower Management Centers, you can view information about the local Firepower Management Center and its peer.

Note In this context, Local Peer refers to the appliance where you are viewing the system status. Remote Peer refers to the other appliance, regardless of active or standby status.

Procedure

Step 1 Log into one of the Firepower Management Centers that you paired using high availability.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

You can view:

Summary Information

- The health status of the high availability pair. The status of a correctly functioning system will oscillate between "Healthy" and "Synchronization task is in progress" as the standby unit receives configuration changes from the active unit.
- The current synchronization status of the high availability pair
- The IP address of the active peer and the last time it was synchronized
- The IP address of the standby peer and the last time it was synchronized

System Status

- The IP addresses for both peers
- The operating system for both peers
- The software version for both peers
- The appliance model of both peers

Configurations Synced on Firepower Management Center High Availability Pairs

When you establish high availability between two Firepower Management Centers, the following configuration data is synced between them:

- License entitlements
- Access control policies
- Intrusion rules
- Malware and file policies
- DNS policies
- Identity policies
- SSL policies
- Prefilter policies
- Network discovery rules
- Application detectors
- Correlation policy rules
- Alerts
- Scanners
- Response groups
- Contextual cross-launch of external resources for investigating events
- Remediation settings, although you must install custom modules on both Firepower Management Centers. For more information on remediation settings, see Managing Remediation Modules.

Configuring External Access to the FMC Database in a High Availability Pair

In a high availability setup, we recommend you to use only the active peer to configure the external access to the database. When you configure the standby peer for external database access, it leads to frequent disconnections. To restore the connectivity, you must Pausing Communication Between Paired Firepower Management Centers and Restarting Communication Between Paired Firepower Management Centers the synchronization of the standby peer. For information on how to enable external database access to Firepower Management Centers, see Enabling External Access to the Database .

Using CLI to Resolve Device Registration in Firepower Management Center High Availability

If automatic device registration fails on the standby Firepower Management Center, but appears to be registered to the active Firepower Management Center, complete the following steps:

Warning If you do an RMA of Secondary Firepower Management Center or add a Secondary Firepower Management Center, the managed FTDs are unregistered and as a result, their configuration may be deleted.

Procedure

Step 1 Unregister the device from the active Firepower Management Center. See *Delete (Unregister) a Device from the Firepower Management Center* in Cisco Secure Firewall Management Center Device Configuration Guide.

Step 2 Log in to the CLI for the affected device.

Step 3 Run the CLI command: **configure manager delete**.

This command disables and removes the current Firepower Management Center.

Step 4 Run the CLI command: **configure manager add**.

This command configures the device to initiate a connection to a Firepower Management Center.

Tip Configure remote management on the device, only for the active Firepower Management Center. When you establish high availability, the devices are automatically registered to the standby Firepower Management Center.

Step 5 Log in to the active Firepower Management Center and register the device.

Switching Peers in a Firepower Management Center High Availability Pair

Because the system restricts some functionality to the active Firepower Management Center, if that appliance fails, you must promote the standby Firepower Management Center to active:

Procedure

Step 1 Log into one of the Firepower Management Centers that you paired using high availability.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Choose **Switch Peer Roles** to change the local role from Active to Standby, or Standby to Active. With the Primary or Secondary designation unchanged, the roles are switched between the two peers.

Pausing Communication Between Paired Firepower Management Centers

If you want to temporarily disable high availability, you can disable the communications channel between the Firepower Management Centers. If you pause synchronization on the active peer, you can resume synchronization on either the standby or active peer. However, if you pause synchronization on the standby peer, you only can resume synchronization on the standby peer.

Procedure

Step 1 Log into one of the Firepower Management Centers that you paired using high availability.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Choose **Pause Synchronization**.

Restarting Communication Between Paired Firepower Management Centers

If you temporarily disable high availability, you can restart high availability by enabling the communications channel between the Firepower Management Centers. If you paused synchronization on the active unit, you can resume synchronization on either the standby or active unit. However, if you paused synchronization on the standby unit, you only can resume synchronization on the standby unit.

Procedure

Step 1 Log into one of the Firepower Management Centers that you paired using high availability.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Choose **Resume Synchronization**.

Changing the IP address of a Firepower Management Center in a High Availability Pair

If the IP address for one of the high availability peers changes, high availability enters a degraded state. To recover high availability, you must manually change the IP address.

Procedure

Step 1 Log into one of the Firepower Management Centers that you paired using high availability.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Choose **Peer Manager**.

Step 5 Choose **Edit** ( ).

Step 6 Enter the display name of the appliance, which is used only within the context of the Firepower System.

Entering a different display name does not change the host name for the appliance.

Step 7 Enter the fully qualified domain name or the name that resolves through the local DNS to a valid IP address (that is, the host name), or the host IP address.

Step 8 Click **Save**.

Disabling Firepower Management Center High Availability

Procedure

Step 1 Log into one of the Firepower Management Centers in the high availability pair.

Step 2 Choose **System** > **Integration**.

Step 3 Choose **High Availability**.

Step 4 Choose **Break High Availability**.

Step 5 Choose one of the following options for handling managed devices:

- To control all managed devices with this Firepower Management Center, choose **Manage registered devices from this console**. All devices will be unregistered from the peer.
- To control all managed devices with the other Firepower Management Center, choose **Manage registered devices from peer console**. All devices will be unregistered from this Firepower Management Center.
- To stop managing devices altogether, choose **Stop managing registered devices from both consoles**. All devices will be unregistered from both Firepower Management Centers.

Note If you choose to manage the registered devices from the secondary Firepower Management Center, the devices will be unregistered from the primary Firepower Management Center. The devices are now registered to be managed by the secondary Firepower Management Center. However the licenses that were applied to these devices are deregistered on account of the high availability break operation. You must now proceed to re-register (enable) the licenses on the devices from the secondary Firepower Management Center. For more information see Move or Remove Licenses from FTD Devices.

Step 6 Click **OK**.

Replacing FMCs in a High Availability Pair

If you need to replace a failed unit in a Firepower Management Center high availability pair, you must follow one of the procedures listed below. The table lists four possible failure scenarios and their corresponding replacement procedures.

Failure Status	Data Backup Status	Replacement Procedure
Primary FMC failed	Data backup successful	Replace a Failed Primary FMC (Successful Backup), on page 16
	Data backup not successful	Replace a Failed Primary FMC (Unsuccessful Backup), on page 17
Secondary FMC failed	Data backup successful	Replace a Failed Secondary FMC (Successful Backup), on page 18
	Data backup not successful	Replace a Failed Secondary FMC (Unsuccessful Backup), on page 19

Replace a Failed Primary FMC (Successful Backup)

Two Firepower Management Centers, FMC1 and FMC2, are part of a high availability pair. FMC1 is the primary and FMC2 is the secondary. This task describes the steps to replace a failed primary Firepower Management Center, FMC1, when data backup from the primary is successful.

Before you begin

Verify that the data backup from the failed primary Firepower Management Center is successful.

Procedure

Step 1 Contact Support to request a replacement for a failed Firepower Management Center - FMC1.

Step 2 When the primary Firepower Management Center - FMC1 fails, access the web interface of the secondary Firepower Management Center - FMC2 and switch peers. For more information, see Switching Peers in a Firepower Management Center High Availability Pair, on page 13.

This promotes the secondary Firepower Management Center - FMC2 to active.

You can use FMC2 as the active Firepower Management Center until the primary Firepower Management Center - FMC1 is replaced.

Caution Do not break Firepower Management Center High Availability from FMC2, since licenses that were synced to FMC2 from FMC1 (before failure), will be removed from FMC2 and you will be unable to perform any deploy actions from FMC2.

Step 3 Reimage the replacement Firepower Management Center with the same software version as FMC1.

Step 4 Restore the data backup retrieved from FMC1 to the new Firepower Management Center.

Step 5 Install required Firepower Management Center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match FMC2.

The new Firepower Management Center and FMC2 will now both be active peers, resulting in a high availability split-brain.

Step 6 When the Firepower Management Center web interface prompts you to choose an active appliance, select FMC2 as active.

This syncs the latest configuration from FMC2 to the newFirepower Management Center - FMC1.

Step 7 When the configuration syncs successfully, access the web interface of the secondary Firepower Management Center - FMC2 and switch roles to make the primaryFirepower Management Center - FMC1 active. For more information, see Switching Peers in a Firepower Management Center High Availability Pair, on page 13.

Step 8 Apply Classic licenses received with the new Firepower Management Center - FMC1 and delete the old licenses. For more information, see Generate a Classic License and Add It to the Firepower Management Center.

Smart licenses work seamlessly.

What to do next

High availability has now been re-established and the primary and the secondary Firepower Management Centers will now work as expected.

Replace a Failed Primary FMC (Unsuccessful Backup)

Two Firepower Management Centers - FMC1 and FMC2 are part of a high availability pair. FMC1 is the primary and FMC2 is the secondary. This task describes the steps to replace a failed primary Firepower Management Center -FMC1 when data backup from the primary is unsuccessful.

Procedure

Step 1 Contact Support to request a replacement for a failed Firepower Management Center - FMC1.

Step 2 When the primary Firepower Management Center - FMC1 fails, access the web interface of the secondary Firepower Management Center - FMC2 and switch peers. For more information, see Switching Peers in a Firepower Management Center High Availability Pair, on page 13.

This promotes the secondary Firepower Management Center - FMC2 to active.

You can use FMC2 as the active Firepower Management Center until the primary Firepower Management Center - FMC1 is replaced.

Caution Do not break Firepower Management Center High Availability from FMC2, since classic and smart licenses that were synced to FMC2 from FMC1 (before failure), will be removed from FMC2 and you will be unable to perform any deploy actions from FMC2.

Step 3 Reimage the replacement Firepower Management Center with the same software version as FMC1.

Step 4 Install required Firepower Management Center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match FMC2.

Step 5 Deregister the Firepower Management Center - FMC2 from the Cisco Smart Software Manager. For more information, see Deregister a Firepower Management Center from the Cisco Smart Software Manager.

Deregistering a Firepower Management Center from the Cisco Smart Software Manager removes the Management Center from your virtual account. All license entitlements associated with the Firepower Management Center release back to your virtual account. After deregistration, the Firepower Management Center enters Enforcement mode where no update or changes on licensed features are allowed.

Step 6 Access the web interface of the secondary Firepower Management Center - FMC2 and break Firepower Management Center high availability. For more information, see Disabling Firepower Management Center High Availability, on page 15. When prompted to select an option for handling managed devices, choose **Manage registered devices from this console**.

As a result, classic and smart licenses that were synced to the secondary Firepower Management Center-FMC2, will be removed and you cannot perform deployment activities from FMC2.

Step 7 Re-establish Firepower Management Center high availability, by setting up the Firepower Management Center - FMC2 as the primary and Firepower Management Center - FMC1 as the secondary. For more information , see Establishing Firepower Management Center High Availability, on page 9.

Step 8 Apply Classic licenses received with the new Firepower Management Center - FMC1 and delete the old licenses. For more information, see Generate a Classic License and Add It to the Firepower Management Center.

Step 9 Register a Smart License to the primary Firepower Management Center - FMC2. For more information see Register Smart Licenses.

What to do next

High availability has now been re-established and the primary and the secondary Firepower Management Centers will now work as expected.

Replace a Failed Secondary FMC (Successful Backup)

Two Firepower Management Centers - FMC1 and FMC2 are part of a high availability pair. FMC1 is the primary and FMC2 is the secondary. This task describes the steps to replace a failed secondary Firepower Management Center -FMC2 when data backup from the secondary is successful.

Before you begin

Verify that the data backup from the failed secondary Firepower Management Center is successful.

Procedure

Step 1 Contact Support to request a replacement for a failed Firepower Management Center - FMC2.

Step 2 Continue to use the primary Firepower Management Center - FMC1 as the active Firepower Management Center.

Step 3 Reimage the replacement Firepower Management Center with the same software version as FMC2.

Step 4 Restore the data backup from FMC2 to the new Firepower Management Center.

Step 5 Install required Firepower Management Center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match FMC1.

Step 6 Resume data synchronization (if paused) from the web interface of the new Firepower Management Center - FMC2, to synchronize the latest configuration from the primary Firepower Management Center - FMC1. For more information, see Restarting Communication Between Paired Firepower Management Centers, on page 14.

Classic and Smart Licenses work seamlessly.

What to do next

High availability has now been re-established and the primary and the secondary Firepower Management Centers will now work as expected.

Replace a Failed Secondary FMC (Unsuccessful Backup)

Two Firepower Management Centers - FMC1 and FMC2 are part of a high availability pair. FMC1 is the primary and FMC2 is the secondary. This task describes the steps to replace a failed secondary Firepower Management Center -FMC2 when data backup from the secondary is unsuccessful.

Procedure

Step 1 Contact Support to request a replacement for a failed Firepower Management Center - FMC2.

Step 2 Continue to use the primary Firepower Management Center - FMC1 as the active Firepower Management Center.

Step 3 Reimage the replacement Firepower Management Center with the same software version as FMC2.

Step 4 Install required Firepower Management Center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match FMC1.

Step 5 Access the web interface of the primary Firepower Management Center - FMC1 and break Firepower Management Center high availability. For more information, see Disabling Firepower Management Center High Availability, on page 15. When prompted to select an option for handling managed devices, choose **Manage registered devices from this console**.

Step 6 Re-establish Firepower Management Center high availability, by setting up the Firepower Management Center - FMC1 as the primary and Firepower Management Center - FMC2 as the secondary. For more information , see Establishing Firepower Management Center High Availability, on page 9.

- When high availability is successfully established, the latest configuration from the primary Firepower Management Center - FMC1 is synchronized to the secondary Firepower Management Center - FMC2.

- Classic and Smart Licenses work seamlessly.

What to do next

High availability has now been re-established and the primary and the secondary Firepower Management Centers will now work as expected.

Restoring Management Center in a High Availability Pair (No Hardware Failure)

To restore a FMC high availability pair when there is no hardware failure, follow these procedures:

- Restore Backup on the Primary Management Center , on page 20
- Restore Backup on the Secondary Management Center, on page 20

Restore Backup on the Primary Management Center

Before you begin

- There is no hardware failure and replacement of the management center.
- You are familiar with the backup and restore process. See Backup and Restore.

Procedure

Step 1 Verify if backup of the primary FMC is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then go to the **High Availability** tab to pause synchronization.

Step 3 Restore the backup on the primary FMC. The FMC reboots when the restoration is complete.

Step 4 Once the primary FMC is active and its user interface is reachable, resume synchronization on the secondary FMC. Choose **System** (⚙) > **Integration**, and then go to the **High Availability** tab to resume synchronization.

Restore Backup on the Secondary Management Center

Before you begin

- There is no hardware failure and replacement of the management center.
- You are familiar with the backup and restore process. See Backup and Restore.

Procedure

Step 1 Verify if backup of the secondary FMC is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then go to the **High Availability** tab to pause synchronization.

Step 3 Restore the backup on the secondary FMC. The FMC reboots when the restoration is complete.

Step 4 Once the secondary FMC is active and its user interface is reachable, resume synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then go to the **High Availability** tab to resume synchronization.

History for FMC High Availability

Feature	Version	Details
FMC high availability with FMCv on VMWare	6.7	You can now achieve FMC high availability using FMCv running on VMWare. See requirements at Virtual Platform Requirements, on page 7. Supported platforms: FMCv 10, 25, and 300 for VMWare
Single Sign-On	6.7	When configuring one or both members of a high-availability pair for single sign-on, you must take into account special considerations. Supported platforms: FMC.