You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
8 VoIP Availability Manager Warm Failover 70
  Configure VoIP Availability Manager for failover 70

9 Trap Adapter Failover 75
  Configure Trap Adapter 75
  Verify failover status 77

10 Trap Exploder Failover 78
  Overview 78
  Configure the Trap Exploder for failover 78
  Verify failover status 81

11 Broker Failover 82
  Overview 82
  Broker failover scenarios 84
  Configure the Broker for failover 86
  Optional additional configuration tasks for Broker failover 89

12 Site Failover 91
  Overview 91
  Limitations 92

13 Failover Manager 93
  Failover Manager 93
  Validation 94
  Broker registration 94
  Polling monitored Domain Managers 94
  Periodic Backup 97
  Configure the Failover Manager 99
  Other administrator tasks 117

14 Advanced techniques: Hook scripts and VMware M&R collectors 122
  Overview 122
  Additional customizations with hook scripts 122
  VMware M&R collector scenarios used with hook scripts 124
  Configure VMware M&R collectors for an VMware Smart Assurance failover 124

15 Test and Verify the Failover System 130
  Failover system components 130
  Failover directories 131
  Verify failover status 134
Introduction to the Failover System

The Failover Manager is designed to automatically provide backup processes in the case of a failure while monitoring network infrastructures. It is one part of a complete failover solution or system that includes hot and warm failover processes. A failover is the act of switching to a standby software product or hardware device when a failure occurs.

This chapter includes the following topics:

- Supported products for failover
- Failover solution architecture
- Types of failover solutions
- Failover scenarios
- Differences in topology synchronization for hot and warm failover
- Administrative actions for Failover Manager

Supported products for failover

VMware Smart Assurance Failover Manager supports failover for the following products:

- VMware Smart Assurance Service Assurance Manager, including Business Impact Manager (BIM), Adapter Platform (OI), Trap Adapter, Trap Exploder, and the Broker
- VMware Smart Assurance Service Assurance Manager with Notification Cache Publishing Enabled for integration with the SolutionPack for VMware Smart Assurance for use with the VMware Smart Assurance M&R User Interface.
  
  Three additional components compose Service Assurance Manager with Notification Cache Publishing Enabled: VMware Smart Assurance Data Web Applications (Tomcat), VMware Smart Assurance Notification Exchange (Rabbit MQ), and VMware Smart Assurance Notification Cache (ElasticSearch). The EMC Data Access API (EDAA) with service name smarts-edaa resides in Tomcat.
  
- VMware Smart Assurance IP Manager
- VMware Smart Assurance MPLS Manager
- VMware Smart Assurance Server Manager (ESM)
VMware Smart Assurance Network Protocol Manager

VMware Smart Assurance VoIP Availability Manager

**Note**  VMware Smart Assurance Optical Transport Manager (OTM) is not supported for failover. IP Configuration Manager is not supported for failover. VMware Smart Assurance M&R failover is not covered in this guide and it is a custom solution.

**Failover solution architecture**

The failover system or solution includes three sets of components:

- **Active set**
- **Standby set**
- **Failover Manager**

Active and Standby sets operate in different locations. The Failover Manager may reside in a separate location or on the Standby side. The VMware Smart Assurance administrator specifies the components and their locations in the failover.conf file. Deployment considerations and the procedure for setting up the failover system are provided in Chapter 2 Configure the Failover System.

The Failover Manager initially detects one set of components to be the Active set and then detects the other set to be the Standby set. If the sets are not in the Active or Standby state at the time of Failover Manager initialization, the Failover Manager promotes the set in Location-A to Active state and the set in Location-B to the Standby state.

A failover system supports:

- A single-layer Service Assurance Manager architecture.
- A hierarchical SAM architecture.
- Service Assurance Manager with Notification Cache Publishing Enabled (with its associated services Tomcat, Rabbit MQ, and ElasticSearch) for integration with the SolutionPack for VMware Smart Assurance for use with the VMware Smart Assurance M&R User Interface. The architecture can be single-layer or hierarchical.

For example, in the Active location, a hierarchical SAM architecture may consist of one or more Service Assurance Managers deployed above any number of subordinate Domain Managers like IP Availability Manager for analysis or Adapter Platform servers which receive events from trap or syslog adapters. The Standby location has the exact same hierarchy. After the failover occurs, the Standby components can manage the exact same set of devices as the Active components. The Standby components do not manage any devices while the Active components are operational.

Multiple VMware Smart Assurance components may run on one machine within a location.
The Failover Manager monitors all Active and Standby components of the deployment. The Failover Manager also manages registration with the Broker. The Failover Manager registers only Active Managers to communicate with the Broker.

**Note** Unless otherwise noted, Service Assurance Manager (SAM) applies to Service Assurance Manager with and without Notification Cache Publishing Enabled.

### Types of failover solutions

The Failover Manager monitors the operational state of the Broker, Trap Adapters, Trap Exploder, and the Active and Standby Managers—Service Assurance Manager, IP Manager, MPLS Manager, Network Protocol Manager (NPM), Server Manager (ESM), Business Impact Manager (BIM), Adapter Platform, and VoIP Availability Manager.

To monitor these components, the following types of failover solutions are implemented:

- **Hot failover for SAM and Adapter Platform** where the Standby counterparts are running and operational. The Active and Standby SAM and Adapter Platform synchronize instantaneously. Failover Manager activates the Standby SAM and Adapter Platform automatically without requiring manual intervention.

  Information, such as event acknowledgement, data, and topology, is synchronized between the Active and Standby Service Assurance Managers. This ensures that Standby Service Assurance Managers have accurate information if a failover occurs.

  - The Active Service Assurance Manager communicates with the Active Adapter Platform and the Active IP Availability Manager.
  - The Standby Adapter Platform and the Standby Service Assurance Manager instantaneously synchronize with the Active Adapter Platform and Service Assurance Manager, respectively.

  Synchronization is implemented by means of subscription. For example, Standby Service Assurance Manager and Adapter Platform subscribe to their Active counterparts, and receive notifications and topology from them rather than from underlying analysis Domain Managers like IP Availability Manager and Server Manager (ESM).

  In addition for an Active SAM with Notification Cache Publishing that fails, Failover Manager:

  - Promotes the Standby SAM and Standby Tomcat, Rabbit MQ, and ElasticSearch services to Active.
  - Reconfigures the SolutionPack for VMware Smart Assurance to point to the new location of VMware Smart Assurance Tomcat.

  **Warm failover for BIM, IP Manager, MPLS, ESM, NPM, and VoIP Availability Manager** where the Active and Standby Domain Managers synchronize only at stipulated intervals of time. Failover Manager activates the Standby Domain Managers automatically without requiring manual intervention.

  For a warm failover, Standby analysis Domain Managers do not poll devices and polling is suspended in the Domain Managers.
- Failover for Broker where Failover Manager activates the Standby Broker automatically without requiring manual intervention.

- Failover for Trap Exploder where the Failover Manager automatically enables trap forwarding in the newly-promoted Active Trap Exploder or enables trap processing in the newly-promoted Active Trap Adapter. The Failover Manager also registers the promoted Trap Exploder and Trap Adapter with the Broker.

Under normal operating conditions when no failover occurs, the Standby Trap Exploder and Standby Trap Adapter remain in suspend mode. This means that the Standby Trap Exploder and Trap Adapter receive traps, but the Trap Exploder does not forward them and the Trap Adapter does not process them.

**Failover scenarios**

Failover Manager actions for various failure scenarios are described in [Failure scenarios and Failover Manager actions](#).

### Table 1.1. Failure scenarios and Failover Manager actions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Failover Manager action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Smart Assurance Manager fails</td>
<td>Failover Manager initiates an automatic failover to use the corresponding Standby for the failed component.</td>
</tr>
<tr>
<td>Host where the VMware Smart Assurance Manager is running fails</td>
<td>Failover Manager initiates an automatic failover to use the corresponding Standby for the failed component.</td>
</tr>
<tr>
<td>SAM with Notification Cache Publishing Enabled fails or any one of its services (Tomcat, Rabbit MQ, and ElasticSearch) fail</td>
<td>The Failover Manager treats any single component failure as a collective failure of all components and initiates automatic failover to use the corresponding Standby components. The Failover Manager also initiates a reconfigure on the SolutionPack for VMware Smart Assurance to point to the new location of the VMware Smart Assurance Tomcat.</td>
</tr>
<tr>
<td>VMware Smart Assurance Domain Manager fails and it is associated with an VMware M&amp;R collector</td>
<td>When one of the analysis Domain Managers fails, a custom hook script can stop the smarts-collector and start another smarts-collector to collect data from the newly-promoted Domain Manager in the Standby location, provided that you configured the hook script for the Failover Manager. The Failover Manager monitors the Domain Managers and does not monitor the VMware M&amp;R collectors. Typically, a hook script is configured for deployments where delays due to high latency are a concern. <a href="#">Chapter 14 Advanced techniques: Hook scripts and VMware M&amp;R collectors</a> provides more information about scenarios and a hook script procedure.</td>
</tr>
<tr>
<td>VMware Smart Assurance Broker fails</td>
<td>If the host where the Broker resides is running and the Broker is down, Failover Manager initiates an automatic failover to promote the Standby Broker as Active and attempts to restart the failed Active Broker. If the attempt to restart the failed Broker is successful, then both Active and Standby Brokers maintain the same list of active Managers. The Failover Manager registers the promoted Active Broker with the Active Managers. Also, if there is a SolutionPack for VMware Smart Assurance that interacts with the Broker, the Failover Manager is not able to update the SolutionPack. The SolutionPack continues to use the restarted Broker.</td>
</tr>
</tbody>
</table>

---

**VMware Smart Assurance Failover System User Guide**

VMware, Inc.  9
Table 1-1. Failure scenarios and Failover Manager actions (Continued)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Failover Manager action</th>
</tr>
</thead>
</table>
| Host where the Broker is running fails or the Broker cannot be restarted | If the host where the Broker resides is down or the Broker is down, Failover Manager initiates an automatic failover to promote the Standby Broker as Active and attempts to restart the failed Active Broker. If the attempt to restart the failed Broker is not successful:  
  - The newly-promoted Active Broker maintains the list of active Managers. The Failover Manager registers the promoted Active Broker with the Active Managers.  
  - User intervention is required to reconfigure the SolutionPack for VMware Smart Assurance with information about the newly-promoted Active Broker on Site B (Standby). |
| VMware Smart Assurance Manager or Broker is running but is not responding or is intermittently responding | No failover is initiated. The Failover Manager sends an email message to indicate that the VMware Smart Assurance component is not responding. |
| Intermittent network communication failure with the host where a VMware Smart Assurance component is running | No failover is initiated. The Failover Manager attempts to send an email message to indicate this issue. |
| Communication between the Active and Standby location is lost | No failover is initiated. The Failover Manager attempts to send an email message to indicate this issue. |
| VMware Smart Assurance Trap Exploder stops | Failover Manager restarts the Trap Exploder. If the two attempts fail, the Failover Manager proceeds to fail over to the Standby Trap Exploder. The Failover Manager registers the Standby Trap Exploder with the Broker and un-suspends trap forwarding in it and changes its role to Active.  
  Chapter 10 Trap Exploder Failover provides more information. |
| The site fails (all components in Location A fail) | Failover Manager switches the components, including the Broker, to the Standby location. |

In the case of a failover:

- If a failover is initiated, Failover Manager checks the state of the corresponding Standby component prior to the failover completion. If, for any reason, the Standby component is not operational, failover is not performed.

  If the Standby component is operational, the failover continues. When the failover is completed, the Failover Manager automatically changes the configuration of the solution so that the corresponding Standby component becomes the new Active component. The Broker registration is changed to list the location of the new Active component.

  If the Failover Manager cannot reach the Broker or the Broker is down at the time of an VMware Smart Assurance Manager failover, the VMware Smart Assurance Manager failover is not initiated. Instead, the Failover Manager performs a Broker failover. Once the Broker failover is completed, Failover Manager continues with the VMware Smart Assurance Manager failover.
All clients, including Global Consoles and other VMware Smart Assurance components, automatically reconnect to the new Active component. If you open another Global Console, the new console connection needs to be established. To do so, specify the new Active Broker value in the Attach Manager dialog box.

When the failed component is restarted, it automatically resumes the Standby role. Also, in the case of SAM and Adapter Platform, it is automatically configured to listen to the Active component.

- If the Failover Manager fails, no failover is initiated.

- If the Failover Manager monitoring process exits for some reason, you are notified and you must restart Failover Manager manually.

- If a network component fails and causes the failure of multiple VMware Smart Assurance components, all affected VMware Smart Assurance components are switched to the Standby, provided that communications between locations to the Failover Manager and to the Broker are operating correctly.

- The Failover Manager generates email to notify administrators of a failure situation.

- The Failover Manager periodically synchronizes configuration files from an Active component to the Standby counterpart. Passwordless communication is required for this automatic action. Set up passwordless communication between Active and Standby hosts provides instructions for configuring passwordless communication and the SSH connection.

Additionally:

- In a warm failover for IP Manager, MPLS, Server Manager, NPM, and VoIP Availability Manager, only the Active Domain Manager monitors the network.

- Host configurations for Active and Standby VMware Smart Assurance components have to be the same. This is necessary because the roles of Active and Standby components will switch from one host to another when a failover occurs.

**Differences in topology synchronization for hot and warm failover**

For components deployed in the hot failover mode (SAM and Adapter Platform), topology and notification synchronization happens instantaneously using a data exchange file (DXA) between the Active components and their Standby counterparts.

By contrast, for components deployed in the warm failover mode (BIM, IP Manager, Server Manager, VoIP Availability Manager, Network Protocol Manager, and MPLS Manager), the latest topology in the Active component is transferred to the Standby counterpart only during a specified backup interval. During a backup:

- Failover Manager copies all RPS files from the Active location to the Standby location.

- The delta between the files in Active and Standby Domain Managers is incrementally restored on the Standby Domain Manager.

This ensures that the changes in topology are updated in the Standby Domain Manager.
If the failover happens before the topology changes are loaded from the Active to the Standby Domain Manager, then the newly-promoted Active IP Manager will not have the latest topology.

However, the newly-promoted Service Assurance Manager might still continue to display notifications corresponding to devices which were existing in the earlier Active SAM before the failover happened.

**Administrative actions for Failover Manager**

The Failover Manager performs many actions automatically for a failover. The following are additional administrative tasks that an VMware Smart Assurance administrator can perform:

- You can manually perform changes related to configuration, such as adding or deleting devices, and change polling intervals or thresholds on the Active Managers. These changes are synchronized with the Standby Managers during periodic backups.

- You can manually initiate a failback action (or a manual failover) to change a newly-promoted Active component back to the Standby role. When a Standby component changes to an Active role, the component remains in the Active role until it fails or you manually initiate a failback. To perform a failback, use the ic-failover-server script as described in *Initiate failback (or manual failover) of SAM or a Domain Manager*.

- You can add components or make modifications to the failover.conf file while the Failover Manager is already running. If you make changes to the failover.conf file, you need to reload the file. You do not need to restart the Failover Manager.

- You can manually turn on and off the managing of the components by Failover Manager. If the components defined in the failover.conf file were not up and running during Failover Manager startup, then the Failover Manager marks them as unmanaged. Once the components are up and running, you can right-click Manage on the Service Assurance Manager or Domain Manager in the Domain Manager Administration Console. *Setting the management state of individual objects* provides instructions.

- You can use hook scripts to specify additional steps to occur at the beginning or the end of the failover process as described in “*Additional customizations with hook scripts*” on page 59.

  *Chapter 13 Failover Manager* provides information about manual failback, backups, the reload option, and other tasks.
Configure the Failover System

This chapter includes the following topics:

- Deployment considerations
- Set up the failover system
- Set up passwordless communication between Active and Standby hosts
- Additional configuration tasks for Failover Manager on Windows

Deployment considerations

When you are planning your failover system, consider the following:

- Ensure that you have superuser (User ID 0) or administrative privileges to perform the procedures to set up a failover system.
- Failover Manager is supported for Linux and Windows platform versions listed in the VMware Smart Assurance Support Matrix for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers.
- For Windows failover support, the Failover Manager and all components need to be installed and running on Windows. Cross-platform is not supported. For example, Failover Manager on Linux and Domain Managers on Windows is not supported.
- Determine where to install the components of the VMware Smart Assurance Failover System.

VMware Smart Assurance products installed in the Active location must have corresponding products installed in the Standby location, except for IP Configuration Manager. Since IP Configuration Manager is not supported for failover, only one instance is allowed.

In this document, all instructions assume that Location A or Side A is the Active site and Location B or Side B is the Standby site. For example, instructions about domain configuration changes on the Active side, assume that the changes are made on the host defined as Site A.
Each Active and Standby component that is a part of the VMware Smart Assurance Failover System can be installed on a separate host or multiple components can be installed on one host. At the very least, an Active component and its Standby component should operate from distinct installation areas. Ensure that your hosts have sufficient resources.

- It is recommended that installation locations are the same in the Active and Standby sides. If that is not possible, set the StrictSitemod parameter to False in the BASEDIR/conf/failover/failover.conf file.

- The mixing of hardware is not allowed. Failover support is available from one physical box to another physical box, or from one virtual machine to another virtual machine, only if they are running the same operating system.

- Both, the Active and Standby components must be running the same version of VMware Smart Assurance software.

Supported products for failover on page 13 provides a list of supported VMware Smart Assurance products. The VMware Smart Assurance Support Matrix for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers provides resource (hardware and memory) information.

- Determine which ports to use for Active and Standby components.

Service Assurance Manager, Adapter Platform, BIM, and all Domain Managers must be started on predefined ports. The ports are also specified in the ServerSection entries in the failover.conf file.

For Linux, the sm_service install --port value for the Broker and the sm_service install --port value and the --sport value for the Trap Exploder must be changed to values greater than 1024. The Failover Manager uses a non-root user account when restarting these components, so privileged ports (below 1024) cannot be used. For Windows, this restriction is not applicable. Failover Manager on Windows cannot be configured with a non-administrator user account to perform failover actions.

- The Failover Manager software is included in any VMware Smart Assurance product installation. No additional installation task for Failover Manager is required. Later, for one of the deployment tasks, you issue a command to manually install the service for the Failover Manager and then start the service.

When deciding on where to run the Failover Manager, consider the following scenario:

- If the Failover Manager is running with Standby SAM from the host on Location B and the Active SAM on Location A fails, the failover occurs and Standby SAM on Location B is promoted to Active. Then, if the newly-promoted Active SAM host on Location B fails, the Failover Manager will fail with it. You lose the capability to failover.

  To avoid losing failover capability, you need to initiate a failback as soon as the failed SAM on Location A is operational.

- If the Failover Manager is running on a separate dedicated host, you do not lose the capability to failover. The Failover Manager will change the failed SAM host on Location B to Active.

  The Failover Manager may reside in a separate location or on the Standby side. Ideally, the Failover Manager should run on a highly available host that is separate from the components it monitors.
- If you plan to run the Failover Manager on a separate host, you need to install an VMware Smart Assurance product on that host.
- If you do not plan to run the Failover Manager from a separate host, start the Failover Manager service from the host where the Standby SAM is running.
- Determine which ports to use for Active and Standby components.
- For SAM with Notification Cache Publishing that is configured in the SolutionPack for VMware Smart Assurance for use with the VMware M&R UI, you need to determine VMware M&R and SolutionPack block information for the Failover Manager configuration file. MNRSection describes the information that is required.

**Note** Also, if you have upgraded VMware M&R, check the version information after the upgrade. You might need to update version information in the MNRSection of the failover.conf file.

- In a SAM with Notification Cache Publishing Enabled scenario, where Domain Managers are geographically dispersed and VMware M&R collectors are not located near the Domain Managers, delays due to high latency may be a concern when an Active Domain Manager in the Active location (Site A) fails. For latency reasons, you should consider installing a second collector near the Standby (Site B). “Example of smarts-collector messages that indicate high latency” on page 69 provides additional information about high latency.

  The Failover Manager monitors the Domain Managers and does not monitor the VMware M&R collectors. You can configure a hook script so that the script stops the smarts-collector and starts a second smarts-collector to collect data from the newly-promoted Domain Manager in the Standby location.

  Not all scenarios require multiple VMware M&R collectors. Chapter 14 Advanced techniques: Hook scripts and VMware M&R collectors provides more information about scenarios and a hook script procedure.

- The Failover Manager monitors any number of Brokers you have defined. The Brokers can be running on the same host as the Failover Manager or on different hosts. VMware recommends that the Broker operate on the same host as the Failover Manager. The Broker requires minimal resources and recovers very quickly after a failure.

- The Active Broker to which the Failover Manager is connected must be specified as the default Broker for every component in the runcmd_env.sh file. The Failover Manager checks for this default Broker when it monitors the components.

- Run the Linux hostname command for each host. The output is used later when you configure the failover.conf file.

  The host name specified in the ServerSection of the failover.conf file must exactly match the name displayed when you run the Linux hostname command. If the host names do not match, the hosts will not be registered with the Failover Manager.
In Windows, the recommended equivalent of the Linux hostname command is to use the Fully Qualified Domain Name (FQDN) for the host. Although both shortname and FQDN are supported, the best practice is to use FQDN in all places like runcmd_env.sh, failover.conf, and trusted host entries. To locate the FQDN, use the Full Computer name in the Control Panel > System and Security > System.

**Set up the failover system**

Follow this procedure to set up your failover system:

1. Set up a passwordless communications.
   - For Linux, use the instructions in “Set up passwordless communication between Active and Standby hosts” on page 20.
   - For Windows, passwordless communication is achieved by setting up trusted hosts. Use the instructions in Configure hosts for PowerShell remote communication.
     If you plan to run the Failover Manager on a separate dedicated host, you need to set up passwordless communications between the Failover Manager host and between Standby and Active locations as well.

2. Install the VMware Smart Assurance products on the assigned hosts for the Active and Standby locations.
   The *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* provides detailed installation and migration instructions.
   The installation locations of both the Active and Standby Managers must be identical on different hosts. For example:
   - For Active SAM on Host A, use: `/opt/InCharge/SAM` or `C:\InCharge\SAM`
   - For Standby SAM on Host B, use: `/opt/InCharge/SAM` or `C:\InCharge\SAM`

   By default, Failover Manager assumes that software is installed in the same directory in the Active and Standby locations. If you decide not to use identical directories, you need to change the `StrictSitemod` parameter to `False` in the `BASEDIR/conf/failover/failover.conf` file. *SettingSection* provides details on the `StrictSitemod` parameter.

**Note** All hosts taking part in failover must be SSH and SCP-enabled to avoid the requirement for any additional authentication.

3. Configure the following VMware Smart Assurance products in the Active and Standby locations.

**Table 2-1. Product configuration list**

<table>
<thead>
<tr>
<th>Product</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM and Adapter Platform</td>
<td>Configure SAM, Adapter Platform, and BIM for failover</td>
</tr>
<tr>
<td>BIM</td>
<td>Configure SAM, Adapter Platform, and BIM for failover</td>
</tr>
</tbody>
</table>
Table 2.1. Product configuration list (Continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Manager</td>
<td>Configure IP Manager for failover</td>
</tr>
<tr>
<td>MPLS</td>
<td>Configure MPLS Manager for failover</td>
</tr>
<tr>
<td>Server Manager</td>
<td>Configure Server Manager for failover</td>
</tr>
<tr>
<td>NPM</td>
<td>Configure Network Protocol Manager for failover</td>
</tr>
<tr>
<td>VoIP</td>
<td>Configure VoIP Availability Manager for failover</td>
</tr>
<tr>
<td>Trap Adapter</td>
<td>Configure Trap Adapter</td>
</tr>
<tr>
<td>Trap Exploder</td>
<td>“Configure the Trap Exploder for failover” on page 51</td>
</tr>
<tr>
<td>Broker</td>
<td>Configure the Broker for failover</td>
</tr>
<tr>
<td>Failover Manager</td>
<td>Configure the Failover Manager</td>
</tr>
</tbody>
</table>

1. Verify the roles assigned by the Failover Manager to the Active and Standby components using the `ic-failover-server` command as described in Display failover status.

2. Start a topology synchronization on the Active IP Availability Manager. Type:

   ```
   ./dmctl.exe -s INCHARGE-AM invoke ICF_TopologyManager::ICF-TopologyManager
   updateDiscoveryTimers
   ```

3. Perform a manual backup after the first discovery cycle completes for Domain Managers like IP Manager, NPM, Server Manager, and VoIP Availability Manager. Performing a manual backup at this point ensures that the Standby components have saved the latest repository (RPS) files.

   For Standby Service Assurance Managers, it means that all users, profiles, notification lists and escalation policies, and so on will be synchronized with the Active SAM. The source domains will also be synchronized but they will be added as disabled.

   Consult Initiate manual backup for instructions.

4. Verify failover status.

   Check the failover logs in the `BASEDIR/smarts/local/logs` directory for any startup errors and to verify Failover Manager actions. The status of Active components must be UP/ACTIVE and the status of the Standby components must be UP/STANDBY:

   - By default, the `BASEDIR/smarts/local/logs/<failover_manager>_en_US_UTF-8.log` file lists startup messages for the Failover Manager.
   - The `BASEDIR/smarts/local/logs/<Failover_manager>.actions.log` file lists Failover Manager actions. The action logging is optional. To enable it, set the ActionLogging parameter to True in the failover.conf file.

5. Test the failover system as described in Chapter 15 Test and Verify the Failover System
Set up passwordless communication between Active and Standby hosts

For Linux, to ensure that configuration files are synchronized between the Active and Standby locations, set up passwordless access between the hosts on Location A and Location B. This way, all file changes made for components on the Active location are propagated to the Standby location. An additional advantage is that you only need to perform configuration changes once. Passwordless communication is also used for the Failover Manager copy actions which keep Active and Standby /local directories synchronized.

If you plan to run the Failover Manager on a separate dedicated host, you need to set up passwordless communications between the Failover Manager host and between Standby and Active locations.

Note For Windows, passwordless communication is achieved by setting up trusted hosts as described in Configure hosts for PowerShell remote communication.

Set up passwordless SSH access to the Failover Manager servers for root users

To set up passwordless SSH access to the Failover Manager servers for root users:

1. Login to the Active and Standby servers as a root user. If you are logged in as a non-root user, type `sudo su` at the command prompt in both the machines to get the root privileges.

   Note You must have root privileges to transfer files using ssh and scp commands.

2. Type the following command to generate a private or public RSA key pair for both Active and Standby servers:

   ```
   # ssh-keygen -t rsa
   ```

3. In both machines, type the name of the file in which you want to save the key. By default, the key is saved at `/root/.ssh/id_rsa`.

4. At the prompt for setting a passphrase, press ENTER.

   Note You must not provide a passphrase.

5. The key is displayed.

   The public keys are saved in the file, `/root/.ssh/id_rsa.pub` on both machines.

6. Copy the keys from `/root/.ssh/id_rsa.pub` on the Active server to a directory on the Standby server, and vice versa using the following command:

   ```
   #scp /root/.ssh/id_rsa.pub root@<host name>:/<dir>/
   ```
Add the keys to the .ssh/authorized_keys file using the following command:

```
cat /<dir>/id_rsa.pub >> /root/.ssh/authorized_keys
```

To verify that passwordless SSH access has been set up on both the Failover Managerservers, initiate an SSH connection from each of the servers using the command,

```
ssh root@<host name>
```

HostName is the DNS name of the system on which the server is running. The host name provided in the ServerSection of the failover.conf file must exactly match the name displayed when you run the `hostname` command. If the host names do not match, the hosts will not get registered with the Failover Manager server.

EMC recommends that you run the `hostname` command first and use that output to provide the host name in the failover.conf file.

**Set up passwordless SSH access to the Failover Manager servers for non-root users**

For Linux, perform the following procedure on both Active and Standby machines for non root users:

1. Select or create a non-root group to be used by Failover Manager for passwordless communication (for example, `smartsgrp`). Type:

   ```
   groupadd smartsgrp
   ```

2. Select or create a non-root account to be used by Failover Manager for passwordless communication (for example, `smartsusr`). Type:

   ```
   adduser smartsusr -g smartsgrp
   ```

3. Verify that passwordless SSH access is set up for the Failover Manager. To do so, initiate an SSH connection from:

   4. Failover manager to all of the hosts used in failover.conf file
   5. To the failover manager host itself
   6. Between all of the Active and Standby Hosts used in the failover.conf file

   Using the command:

   ```
   ssh smartsusr@<host_name>
   ```
Where `<host_name>` is the DNS name of the machine on which the VMware Smart Assurance component is running.

**Note** On initial connection you will be prompted to add a known host and asked to continue, type 'yes'. The authenticity of host 'apollo (10.241.215.34)' can't be established. RSA key fingerprint is e5:a9:32:3f:0e:bf:53:87:97:ce:8e:6c:29:34:93. Are you sure you want to continue connecting (yes/no)?

7 Later when you are configuring the Failover Manager, edit the `failover.conf` file as follows. This ensures that the root process executes commands for non-root user. Also, it specifies the location of the security key.

```bash
TransferCmd="/usr/bin/scp -i /home/smartsusr/.ssh/id_rsa";
RemoteLogin="/usr/bin/ssh -i /home/smartsusr/.ssh/id_rsa";
```

8 Change the ownership of the directory `<BASEDIR>/smarts/local` to `smartsusr` and `smartsgrp` on both machines Active and Standby, so that users in the group can alter local smarts folder. Type:

```bash
# usermod -G smartsgrp smartsusr
# chown -R smartsusr:smartsgrp <install_path>/smarts/local
# chmod -R g+w <install_path>/smarts/local
# chmod 444 <install_path>/smarts/local/conf/%Connect.conf
# chmod 444 <install_path>/smarts/local/conf/imk.dat
# chmod 644 <install_path>/smarts/local/conf/runcmd_env.sh
```

9 Log in as `smartsusr` and set the permission for `.ssh` folder to 700 on both machines Active and Standby. Type:

```bash
# chmod 700 /home/smartsusr/.ssh
```

10 Log in as `smartsusr` and set the permission for `.ssh/authorized_keys` to 600 on both machines Active and Standby. Type:

```bash
# chmod 600 /home/smartsusr/.ssh/authorized_keys
```

11 Execute the `ssh` command manually from `root` to check that the `ssh` command works correctly:

```bash
# ssh -i /home/smartsusr/.ssh/id_rsa -n -l smartsusr itops-qa-108 ls -lrt
```

12 Once the above step is successful, edit the `BASEDIR/smarts/conf/failover/failover.conf` file with the following content:

13 Comment the root user `TransferCmd` and `RemoteLogin` and enable it for non-root user as below:

```bash
TransferCmd = "/usr/bin/scp -p -i /home/smartsusr/.ssh/id_rsa";
RemoteLogin = "/usr/bin/ssh -i /home/smartsusr/.ssh/id_rsa";
```

14 Change the user as `smartsusr`. 
15 Change the ownership to the smartsgp. Type:

```
#chown -R root:smartsgrp /var/smarts/
```

16 Change the permissions for sm_service. Type:

```
#chmod 770 /var/smarts/pipes/sm_service
```

17 To ensure that passwordless communication is working after a host reboot, modify the `/etc/init.d/ic_serviced` file on all hosts.

18 Edit `/etc/init.d/ic-serviced`.

19 Find the following line:

```
check_startup(){
```

20 Add the following code (in bold):

```
check_startup(){
    COUNT=1
    while true
    do
        sleep 1
        isRunning
        if [ $? -eq 1 ]; then
            [ "$OS" = "Linux" ] && touch $LOCKFILE
            break
        fi
        COUNT=`expr ${COUNT} + 1`
        if [ ${COUNT} -gt 60 ];
        then
            echo "$SERVICED failed to start."
            exit 1
        fi
    done
    sleep 5
    chown -R root:smartsgrp /var/smarts
    sleep 5
    chown -R smartsusr:smartsgrp <BASEDIR>/smarts/local
    sleep 5
    chmod 770 /var/smarts/pipes/sm_service
}
```

21 Save the file and exit.

22 Verify that the non-root setup is working properly. Log in as a non-root user and run the following remote command:

```
sm_service show
[smartsusr@wpl-019-072 bin]$ /usr/bin/ssh -i /home/smartsusr/.ssh/id_rsa -n -l smartsusr wpl-019-071.lss.emc.com 2>&1 /opt/InCharge/SAM/smarts/bin/sm_service show
RUNNING ic-trapd-exploder
```
Additional configuration tasks for Failover Manager on Windows

In addition to the procedure described in Set up the failover system, for the Failover Manager or other components running on Windows, you need to perform these tasks:

- Configure hosts for PowerShell remote communication
- Setting up Administrator service for PowerShell remoting (Windows only)
- Set up shared drives and permissions
- Security
- Configure Domain Managers 9.3 or earlier for the failover backup

Configure hosts for PowerShell remote communication

On Windows, Failover Manager uses PowerShell to execute commands on remote hosts. The PowerShell remote execution uses Windows Remote Management (WinRM) to execute commands on a remote host.

You need to configure WinRM to accept remote requests on each host running an VMware Smart Assurance Manager (Domain Managers and Service Assurance Managers). Use PowerShell 3.0 or later.

Also, you need to include the hosts in the Active Directory domains or the PowerShell TrustedHosts list. Each VMware Smart Assurance Manager host needs to trust the Failover Manager host, and the Failover Manager host needs to trust each VMware Smart Assurance Manager host. Two methods are available:

- The preferred method is to include the hosts in Active Directory domains.
If this is not possible, add the Failover Manager host to the TrustedHosts list on each VMware Smart Assurance Manager host, and add each VMware Smart Assurance Manager host to the TrustedHosts list on the Failover Managers host.

**Procedure to configure PowerShell remote communication**

To configure hosts for PowerShell remote communication:

1. Configure WinRM to accept remote requests on each host running an VMware Smart Assurance product (for example, Failover Manager, Service Assurance Manager, Domain Managers, Trap Exploder, and Trap Adapter). Type the following command:

   ```powershell
   enable-psremoting
   ```

2. Add the Fully Qualified Domain Name (FQDN) for the Failover Manager host to the TrustedHosts list on each VMware Smart Assurance Manager host. For example, type the following command as one line:

   ```powershell
   Set-Item wsman:\localhost\Client\TrustedHosts itops-qa-148.lss.emc.com -Concatenate -Force
   ```

3. Add the FQDN for each VMware Smart Assurance Manager host to the TrustedHosts list on the Failover Managers host.

**Set up shared drives and permissions**

Failover Manager on Windows uses Server Message Block (SMB) protocol to copy repository and configuration files when backing up data from an Active component to its Standby component.

You need to share the drive where each VMware Smart Assurance product is installed and give permission to the Administrator account to read and write files on the drive.

**Security**

Install the VMware Smart Assurance products on a logical drive instead of the drive where Windows is installed. This allows you to share the logical drive while protecting the drive where Windows is installed.

SMB 3.0, available starting in Windows 2012, can be configured to encrypt data sent between hosts. SMB 3.0 also supports a more secure signing algorithm than SMB 2.0 does.

Remote execution of scripts and the results of those scripts are sent in clear text over an HTTP connection to the WinRM listener on the remote host. The options needed to use HTTPS for Invoke-Command are not included in the scripts. The *VMware Smart Assurance Release Notes for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* provides information and a security resolution in the topic, “Failover Manager sends data in clear text between Windows hosts” (SND-1848).
SAM, Adapter Platform, and BIM Failover

This chapter includes the following topics:
- SAM hierarchical hot failover setup
- Active SAM with Notification Cache Publishing hot failover setup
- Active SAM failure scenario
- BIM failover scenarios and failover actions
- Configure SAM, Adapter Platform, and BIM for failover
- Next steps

**SAM hierarchical hot failover setup**

SAM hierarchical hot-hot failover setup illustrates the components of the Failover System in their various locations.
Active SAM with Notification Cache Publishing hot failover setup

SAM with Notification Cache Publishing hot-hot failover setup illustrates the components of the Failover System in their various locations.
The Active SAM server with Notification Cache Publishing Enabled is the SAM that is configured in the SolutionPack for VMware Smart Assurance for use with the VMware M&R User Interface.

Figure 3-2. SAM with Notification Cache Publishing hot-hot failover setup

Active SAM failure scenario

In case of an Active SAM failure, the Failover Manager forces a reconfiguration of the newly-promoted Active SAM to cause it to reconnect to the Active underlying analysis Domain Managers and Adapter Platform servers. At this point, the new Active SAM remains the Active SAM until it fails, or you manually initiate a failback.

The Active SAM server with Notification Cache Publishing Enabled is the SAM that is configured in the SolutionPack for VMware Smart Assurance for use with the VMware M&R User Interface. Sometimes, this SAM is referred to as the Presentation SAM server and its service name is ic-sam-server-pres. Three additional components compose this SAM:

- VMware Smart Assurance Data Web Applications (Tomcat)—Service name is smarts-tomcat.

  The EMC Data Access API (EDAA) with service name smarts-edaa resides in Tomcat.

- The EMC Data Access API (EDAA) with service name smarts-edaa resides in Tomcat.
VMware Smart Assurance Notification Exchange (Rabbit MQ)—Service name is smarts-rabbitmq.

VMware Smart Assurance Notification Cache (ElasticSearch)—Service name is smarts-elasticsearch.

If the Active SAM or any of the three components go down, Failover Manager considers the Active SAM to be down and performs the following:

- Promotes the Standby SAM and Standby Tomcat, Rabbit MQ, and ElasticSearch services to Active.
- Reconfigures the SolutionPack for VMware Smart Assurance to point to the new location of VMware Smart Assurance Tomcat.
- Forces a reconfiguration of the newly-promoted Active SAM to cause it to reconnect to the Active underlying analysis Domain Managers and Adapter Platform servers.

At this point, the new Active SAM remains the Active SAM until it fails, or you manually initiate a failback.

**Note**  Presentation SAM server is the server that is configured in the SolutionPack for VMware Smart Assurance for use with the VMware M&R UI. This does not mean that a hierarchical SAM is required.

### BIM failover scenarios and failover actions

The failover solution supports the following BIM failover scenarios:

- **Scenario 1: Active BIM is down on page 27**
- **Scenario 2: Both Active BIM and Active SAM are down on page 27**

#### Scenario 1: Active BIM is down

In this scenario, when an Active BIM attached to an Active SAM is down, then the Standby BIM attached to the Standby SAM disconnects and connects to the Active SAM. This scenario is illustrated below:

1. All components are up and running. Active BIM talks to Active SAM and vice versa. Similarly, Standby BIM talks to Standby SAM and vice versa.
2. Active BIM goes down.
3. Standby BIM is dissociated from Standby SAM.
4. Standby BIM is associated with Active SAM.

#### Scenario 2: Both Active BIM and Active SAM are down

In this scenario, when both an Active SAM and its corresponding BIM fails, then both Standby SAM and BIM becomes active. This scenario is illustrated below:

1. All components are up and running. Active BIM talks to Active SAM and vice versa. Similarly, Standby BIM talks to Standby SAM and vice versa.
2. Both Active SAM and Active BIM are down.
3. Standby SAM and Standby BIM become Active.
Configure SAM, Adapter Platform, and BIM for failover

This section describes how to configure Active and Standby components for failover. The Failover Manager does not need to be running for you to perform these tasks.

1. Configure the Active and Standby components
2. Start the services for SAM, Adapter Platform, and BIM
3. Configure the failover.conf file for SAM, Adapter Platform, and BIM
4. Create subscriptions with the sm_configureFailover.pl script on page 27

Additional information about escalation is provided in Escalation policy changes.

Configure the Active and Standby components

In a hot failover, each monitored Active component has a hot Standby sibling that must be kept up-to-date at all times. The Standby component gets its topology and event data from the Active component. Thus, while the Active component is connected to the underlying Domain Managers, the Standby only connects to the Active component to synchronize with it. On the Standby component, Failover Manager automatically disables all underlying Domain Managers. Therefore, the configuration procedure of the Active component and that of the Standby component differ slightly.

- Configure an Active SAM
- Configure a Standby SAM
- Configure Active Adapter Platform
- Configure Standby Adapter Platform
- Configure Active BIM
- Configure Standby BIM

Configure an Active SAM

This procedure applies to both SAM and SAM with Notification Cache Publishing. It includes some additional steps for SAM with Notification Cache Publishing.

To configure an Active SAM:

1. Disable topology synchronization in the Active location so that the Active SAM does not synchronize with the underlying Domain Managers while the Domain Managers are still starting up. The Failover Manager synchronizes the Active SAM with the underlying Domain Managers.

   In the installation area where the Active SAM is running, go to the BASEDIR/smarts/bin directory and open the bootend.conf file. Type:

   ```
   ./.sm_edit conf/ics/bootend.conf
   ```

2. Change the value of suspendTopologyManager to TRUE. The value is FALSE by default.
4. Save the file and exit.

5. For Active SAM with Notification Cache Publishing only, use sm_edit to open the `<BASEDIR>/smarts/bin/local/runcmd_env.sh` file and add the VMware Smart Assurance environment variables listed in Environment variables specified for Host A in the runcmd_env.sh file.

Table 3-1. Environment variables specified for Host A in the runcmd_env.sh file

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM_EDAA_NAME</td>
<td>Identifies the EDAA for Host A. For example:</td>
</tr>
<tr>
<td></td>
<td><code>SM_EDAA_NAME=SMARTS-EDAA-A</code></td>
</tr>
<tr>
<td></td>
<td>Each EDAA has a name. The value specified for SM_EDAA_NAME should match the</td>
</tr>
<tr>
<td></td>
<td>value used in the sm_service command. By default, the name for the EMC Data</td>
</tr>
<tr>
<td></td>
<td>Access API (EDAA) is SMARTS-EDAA.</td>
</tr>
<tr>
<td>SM_CAS_SERVER</td>
<td>Identifies the VMware M&amp;R host. For example:</td>
</tr>
<tr>
<td></td>
<td><code>SM_CAS_SERVER=http://&lt;M&amp;RHostName&gt;:58080</code></td>
</tr>
<tr>
<td>SM_TOMCAT_SERVER</td>
<td>Is the name of the host where Smarts EDAA is running which is the same host</td>
</tr>
<tr>
<td></td>
<td>as SAM with Notification Cache Publishing. For example:</td>
</tr>
<tr>
<td></td>
<td><code>SM_TOMCAT_SERVER=http://&lt;smarts_tomcat_hostname&gt;:8080</code></td>
</tr>
</tbody>
</table>

1. Install the service for the Active SAM on an Active server (host A).

Example for Active SAM without Notification Cache Publishing:

```
./sm_service install --force --unmanaged --startmode=runonce
  '--name=ic-sam-server'
  '--description=EMC Smarts Service Assurance Manager Server'
  '/<BASEDIR>/SAM/smarts/bin/sm_server'
  '-n' 
  'INCHARGE-SA'
  '--config=ics'
  '--port=1751'
  '--ignore-restore-errors'
  '--noregister'
  '--output

./sm_service install --force --unmanaged --startmode=runonce
  '--name=ic-sam-server-pres'
  '--description="EMC Smarts Service Assurance Manager Server (notification cache publishing)"
  '/<BASEDIR>/SAM/smarts/bin/sm_server'
  '-n INCHARGE-SA-PRES
  '--config=ics
  '--port=1751
  '--edaa=sam-presentation/2.0@SMARTS-EDAA-A
  '--bootstrap=bootstrap-amqp.conf
  '--ignore-restore-errors
  '--output
```
For Active SAM with Notification Cache Publishing only, if you did not install the services for smarts-tomcat, smarts-rabbitmq, and smarts-elasticsearch during the SAM installation, you need to manually install them. The *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* describes how to manually install these services.

For Active SAM with Notification Cache Publishing only, use sm_edit to open the `<BASEDIR>/smarts/conf/local/clientConnect.conf` file.

These sections are configured with default admin/changeme credentials. If the VMware M&R or EDAA user name and passwords have been changed from the defaults, update the values in this file and save the file. When sm_edit is used again, passwords will be encrypted.

In the Webservices Access section, specify the credentials for VMware M&R frontend (Tomcat) and VMware M&R Webservice Gateway.

In the Smarts EDAA Access section, provide the Broker information as credentials to access the VMware Data Access API (smarts-edaa). Replace the default password (changeme) with the Broker password. The EMC Data Access API (EDAA) uses this information during a Broker failover.

```
# Credentials to access MNR.
# This is used by Failover Manager.
# You should change the password!
*:http://\*:58889/*:admin:<E-1.0>94DA919F35977FF903835AB67EDD7F6CA24EDCAF8D6088D5760141A008D8CE

# Credentials to access MNR webservice-gateway.
# This is used by Failover Manager.
# You should change the password!
*:https://\*:48443/*:admin:<E-1.0>94C6DAE69612883C06CB84683BC906DA2C27202FF3426BCD7801989BD62594

# Credentials to access the smarts-edaa.
# This is used by the Failover Manager to update
# the broker location when the broker fails over.
# You should change the password!
*:http://\*:949E62F64CE41435C58105E538A1DAC5A6D6B7CC8A74B16580DC344E6F9C716A3

# Credentials to access the smarts-edaa.
# This is used by the Failover Manager to update
# the broker location when the broker fails over.
# You should change the password!
*:https://\*:949E62F64CE41435C58105E538A1DAC5A6D6B7CC8A74B16580DC344E6F9C716A3
```

Start the Active SAM service in *Start the services for SAM, Adapter Platform, and BIM*.

For Active SAM with Notification Cache Publishing, in addition to the SAM service, you need to start the services for smarts-tomcat, smarts-rabbitmq, and smarts-elasticsearch.

Attach a Global Console to the Active SAM by specifying “<FQDN hostA>:<portA>/<ServerName>” in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.Iss.emc.com:1751/INCHARGE-SA.

From the menu, select *Configure > Global Manager Administration Console*.

For the Active Service Assurance Manager, define the Active Adapter Platform and the Active BIM as sources.
Add the Active Adapter Platform details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.

Specify the Active Adapter Platform domain name, leaving this connection initially enabled.

In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select **INCHARGE-OI**, and click **Finish**.

Add Active BIM details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.

Specify the Active BIM domain name and leave the **Enabled** checkbox selected for this connection. Specify the domain name in the format hostname:port/domain (for example, itops-tco-223.lss.emc.com:1612/INCHARGE-MBIM). The hostname specified here should match the hostname in the entry of the failover.conf file.

In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select **INCHARGE-MBIM**, and click **Finish**.

For the Active Service Assurance Manager, define the other Active Domain Managers like IP Manager as sources. **Configure sources for Active Service Assurance Manager** provides a list. **Table 3-2**. Configure sources for Active Service Assurance Manager

<table>
<thead>
<tr>
<th>Product</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Manager</td>
<td>Configure the IP Manager as a source for SAM</td>
</tr>
<tr>
<td>MPLS Manager</td>
<td>Configure the MPLS Manager as a source for SAM</td>
</tr>
<tr>
<td>Server Manager (ESM)</td>
<td>Configure the Server Manager as a source for SAM</td>
</tr>
<tr>
<td>NPM</td>
<td>Configure the Network Protocol Manager as a source for SAM</td>
</tr>
<tr>
<td>VoIP Availability Manager</td>
<td>Configure the VoIP Availability Manager as a source for SAM</td>
</tr>
</tbody>
</table>

Apply the configuration change and reconfigure the Service Assurance Manager.

**Note** Configurations such as underlying Domain Managers (sources), user groups, notification lists, and escalation policies only need to be configured on the Active Service Assurance Manager. During synchronization between Active and Standby Service Assurance Managers, the Failover Manager creates these configurations in the Standby Service Assurance Manager.

### Configure a Standby SAM

To configure a Standby SAM:

1. For the Standby SAM with Notification Cache Publishing only, use sm_edit to open the `<BASEDIR>/smarts/bin/local/runcmd_env.sh` file and add the VMware Smart Assurance environment variables listed in **Environment variables specified for Host B in the runcmd_env.sh file**.
Table 3-3. Environment variables specified for Host B in the runcmd_env.sh file

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM_EDAA_NAME</td>
<td>Identifies the EDAA for Host B. For example:</td>
</tr>
<tr>
<td></td>
<td>SM_EDAA_NAME=SMARTS-EDAA-B</td>
</tr>
<tr>
<td></td>
<td>Each EDAA has a name. The value specified for SM_EDAA_NAME should match the value used in the sm_service command. By default, the name for the EMC Data Access API (EDAA) is SMARTS-EDAA.</td>
</tr>
<tr>
<td>SM_CAS_SERVER</td>
<td>Identifies the EMC M&amp;R host. For example:</td>
</tr>
<tr>
<td></td>
<td>SM_CAS_SERVER=http://&lt;M&amp;RHostName&gt;:58080</td>
</tr>
<tr>
<td>SM_TOMCAT_SERVER</td>
<td>Is the name of the host where Smarts EDAA is running which is the same host as SAM with Notification Cache Publishing. For example:</td>
</tr>
<tr>
<td></td>
<td>SM_TOMCAT_SERVER=http://&lt;smarts_tomcat_hostname&gt;:8080</td>
</tr>
</tbody>
</table>

1 Install the service for the Standby SAM on a Standby server (host B).
   - For the Standby SAM without Notification Cache Publishing, use the sm_service install command provided in step 3 in the Configure an Active SAM.
   - For the Standby SAM with Notification Cache Publishing, specify host B for the --edaa option. For example:

   ```bash
   ./sm_service install --force --unmanaged --startmode=runonce
   --name=ic-sam-server-pres
   --description="EMC Smarts Service Assurance Manager Server (notification cache publishing)"
   /<BASEDIR>/SAM/smarts/bin/sm_server
   -n INCHARGE-SA-PRES
   --config=ics
   --port=1751
   --edaa=sam-presentation/2.0@SMARTS-EDAA-B
   --bootstrap=bootstrap-amqp.conf
   --ignore-restore-errors
   --output
   ```

2 For Standby SAM with Notification Cache Publishing only, if you did not install the services for smarts-tomcat, smarts-rabbitmq, and smarts-elasticsearch during the SAM installation, you need to manually install them. The *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* describes how to manually install these services.

3 Start the Standby SAM service in Start the services for SAM, Adapter Platform, and BIM.

   For Standby SAM with Notification Cache Publishing, in addition to the SAM service, you need to start the services for smarts-tomcat, smarts-rabbitmq, and smarts-elasticsearch.
At this point, additional manual configuration is no longer required.

- Later, after you modify the failover.conf file and run the sm_configureFailover.pl script, the script automatically creates all necessary subscriptions to the counterparts.
- Later, when you run the manual backup, the Failover Manager adds the underlying source Domain Managers from the Active location to the Standby location.

**Configure Active Adapter Platform**

To configure an Active Adapter Platform:

1. Disable topology synchronization in the Active location so that the Active Adapter Platform does not synchronize with the underlying Domain Managers while the Domain Managers are still starting up. The Failover Manager synchronizes the Active Adapter Platform with the underlying Domain Managers.

2. In the installation area where the Active Adapter Platform is running, go to the `BASEDIR/smarts/bin` directory and open the `bootend.conf` file. Type:

```
./sm_edit conf/icoi/bootend.conf
```

3. Change the value of `suspendTopologyManager` to **TRUE**. The value is **FALSE** by default.

4. Save the file and exit.

5. Install the service for the Active Adapter Platform on an Active server (host A) with the `--noregister` mode using the command below. Also, install the service for the Standby Adapter Platform on the Standby server (host B) with the `--noregister` mode.

   Example:

   ```
   ./sm_service install --force --unmanaged --startmode=manual
   '---name=ic-icoi-server' \n   '---description=EMC Smarts SAM Adapter Platform Server' \n   '/InCharge/SAM/smarts/bin/sm_server' \n   'n' \n   'INCHARGE-OI' \n   'config=icoi' \n   'port=11308' \n   'ignore-restore-errors' \n   'noregister' \n   'output'
   ```

6. Start the service in **Start the services for SAM, Adapter Platform, and BIM.**

7. For the Active Adapter Platform, add the underlying IP Managers.

8. Attach a Global Console to the Active Adapter Platform by specifying "<FQDN hostA>:<portA>/<ServerName>" in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.lss.emc.com:11308/INCHARGE-OI.

9. From the menu, select **Configure > Global Manager Administration Console.**
10 Add the IP Manager details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.

11 Specify the Active IP Manager domain name, leaving this connection initially enabled.

12 In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select the Domain Manager and click **Finish**.

13 Apply the configuration change and reconfigure the Active Adapter Platform.

### Configure Standby Adapter Platform

To configure a Standby Adapter Platform:

1 Install the service for the Standby Adapter Platform as outlined in **Configure Active Adapter Platform**.

2 Start the service in **Start the services for SAM, Adapter Platform, and BIM**.

   At this point, additional manual configuration is no longer required.

   - Later, after you modify the failover.conf file and run the sm_configureFailover.pl script, the script automatically creates all necessary subscriptions to the counterparts.

   - Later, when you run the manual backup, the Failover Manager adds the underlying source Domain Managers from the Active location to the Standby location.

### Configure Active BIM

Configuring the Active and Standby BIM components are optional.

1 For the BIM service, use:

   ```
   ./sm_service install --force --unmanaged --startmode=runonce \
   '---name=ic-mbim-server' \n   '---description=EMC Smarts MBIM - Maintenance and Business Impact Manager Server' \n   '/<BASEDIR>/SAM/smarts/bin/sm_server' \n   'n' \n   'INCHARGE-MBIM' \n   '---config=bim' \n   '---port=1752' \n   '---ignore-restore-errors' \n   '---noregister' \n   '---output'
   ```

2 Start the service in **Start the services for SAM, Adapter Platform, and BIM**.

3 For the Active BIM, add the Active Service Assurance Manager as a source.

4 Attach a Global Console to the Active BIM by specifying "<FQDN hostA>:<portA>/<ServerName>" in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.lss.emc.com:1752/INCHARGE-MBIM.

5 In the Domain **Manager Administration Console**, select **INCHARGE-MBIM**.

6 Select **Topology > Add Source**.
Specify INCHARGE-SA as a topology source for the Active BIM.

Apply the configuration change and reconfigure BIM.

**Configure Standby BIM**

To configure a Standby BIM:

1. Install the service for the Standby BIM as outlined in Configure Active BIM.
2. Start the service in Start the services for SAM, Adapter Platform, and BIM.

At this point, additional manual configuration is no longer required.

- Later, after you modify the failover.conf file and run the sm_configureFailover.pl script, the script automatically creates all necessary subscriptions to the counterparts.
- Later, when you run the manual backup, the Failover Manager adds the underlying source Domain Managers from the Active location to the Standby location.

**Start the services for SAM, Adapter Platform, and BIM**

Start the service for each Vmware Smart Assurance product in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the BASEDIR/smarts/bin directory for the product.
2. Type: `./sm_service start < service_name >`
3. Press Enter.
4. Repeat Steps 2-3 for each service name that is installed for your deployment.

**Table 3-4. SAM service names**

<table>
<thead>
<tr>
<th>Product</th>
<th>Service name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Assurance Manager</td>
<td>ic-sam-server</td>
</tr>
<tr>
<td>SAM with Notification Cache Publishing</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>ic-sam-server-pres</td>
</tr>
<tr>
<td>VMware Smart Assurance Data Web Applications (Tomcat)</td>
<td>smarts-tomcat</td>
</tr>
<tr>
<td>EMC Data Access API (EDAA)</td>
<td>smarts-edaa</td>
</tr>
<tr>
<td>VMware Smart Assurance Notification Exchange (Rabbit MQ)</td>
<td>smarts-rabbitmq</td>
</tr>
<tr>
<td>VMware Smart Assurance Notification Cache (ElasticSearch)</td>
<td>smarts-elasticsearch</td>
</tr>
<tr>
<td>Adapter Platform</td>
<td>ic-icoi-server</td>
</tr>
<tr>
<td>Business Impact Manager</td>
<td>ic-mbim-server</td>
</tr>
</tbody>
</table>
Windows

To start the service from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services.**
2. Right-click `<EMC_Smarts_service>`.  
3. Select **Start.**  
4. Repeat Steps 2-3 for each service name that is installed for your deployment.

Configure the failover.conf file for SAM, Adapter Platform, and BIM

Configure Service Assurance Manager, Adapter Platform, and BIM in the failover.conf file.

1. In the installation area where the Failover Manager is running, go to the **BASEDIR/smarts/bin** directory and type the following command to open the **failover.conf** file:

   
   ```bash
   ./sm_edit /conf/failover/failover.conf
   ```

2. Under the Server section, add SAM, Adapter Platform, and BIM details with Server Type as SAM, OI, and BIM, respectively. For example:

   **SAM:**

   ```
   Server
   {
   DetachInterval = 300;
   Name = "INCHARGE-SA";
   ServerType = "SAM";
   LocationA
   {
   HostName = "itops-tco-217.lss.emc.com";
   PortNumber = 1751;
   Basedir = "/opt/InCharge/SAM/smarts";
   }
   LocationB
   {
   HostName = "itops-tco-223.lss.emc.com";
   PortNumber = 1751;
   Basedir = "/opt/InCharge/SAM/smarts";
   }
   Server
   {
   DetachInterval = 300;
   Name = "INCHARGE-SA-PRES";
   ServerType = "SAM";
   UIServices = "smarts-tomcat,smarts-rabbitmq,smarts-elasticsearch";
   LocationA
   ```
HostName   = "itops-tco-217.lss.emc.com";
PortNumber = 1751;
Basedir    = "/opt/InCharge/SAM/smarts";
}

LocationB
{
  HostName   = "itops-tco-223.lss.emc.com";
  PortNumber = 1751;
  Basedir    = "/opt/InCharge/SAM/smarts";
}
}

Server
{
  DetachInterval = 300;
  Name           = "INCHARGE-OI";
  ServerType     = "OI";
  LocationA
  {
    HostName   = "smartslin02.svtdomain.us.dg.com";
    PortNumber = 11308;
    Basedir    = "/opt/InCharge/SAM/smarts";
  }
  LocationB
  {
    HostName   = "smartslin04.svtdomain.us.dg.com";
    PortNumber = 11308;
    Basedir    = "/opt/InCharge/SAM/smarts";
  }
}
}

Server
{
  DetachInterval = 300;
  Name           = "INCHARGE-MBIM";
  ServerType     = "BIM";
  LocationA
  {
    HostName   = "itops-tco-217.lss.emc.com";
    PortNumber = 1752;
    Basedir    = "/opt/InCharge/SAM/smarts";
  }
  LocationB
  {
    HostName   = "itops-tco-223.lss.emc.com";
    PortNumber = 1752;
    Basedir    = "/opt/InCharge/SAM/smarts";
  }
}
3 Uncomment the MNRSection and specify values for the following parameters. The Failover Manager uses this information to set the Active EDAA and Active Broker in the SolutionPack for VMware Smart Assurance.

- **MNRHost**—Is the VMware M&R Frontend server (tomcat) host.
- **MNRPort**—Is the VMware M&R Frontend server (tomcat) port.
- **MNRProtocol**—Is the VMware M&R Frontend server (tomcat) protocol.
- **GatewayHost**—Is the VMware M&R web-service gateway host.
- **GatewayPort**—Is the VMware M&R web-service gateway port.
- **GatewayProtocol**—Is the VMware M&R web-service gateway protocol.

In case you have multiple SolutionPack instances, specify the SolutionPack that contains the Reports SolutionPack block.

For each SolutionPack block (Reports, Events, Data collection) specify the values exactly how they appear in the Centralized Management page in the VMware M&R UI. To locate and copy the values, navigate to the SolutionPacks page. (Log in to the VMware M&R UI and type `http://<Frontend IP address>:58080/centralized-management`. Click SolutionPacks and then click VMware Smart Assurance to locate the information.)

- **Component**—Is the component. For example: Reports, Events, Data collection.
- **ComponentVersion**—Is the component version.
- **SPInstance**—Is the SolutionPack instance. For example: VMware-smarts
- **SPVersion**—Is the SolutionPack version.
- **SPServer**—Is the SolutionPack server distribution.

If you have upgraded VMware M&R, check the version information after the upgrade. You might need to update version information in the MNRSection of the failover.conf file.

For example:

```plaintext
MNRSection
{
  MNRHost = "smartslin03.emc.com";
  MNRPort = 58080;
  MNRProtocol = "http";
  GatewayHost = "smartslin03.emc.com ";
  GatewayPort = 48443;
  GatewayProtocol = "https";
  SolutionPackBlock
  {
    Component = "Reports";
    ComponentVersion = "2.1.1";
    SPInstance = "emc-smarts";
    SPVersion = "2.1.1";
    SPServer = "smartslin02.emc.com";
  }
```
4 Save the failover.conf file and exit.

**Note** If you configure SAM for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.

## Create subscriptions with the sm_configureFailover.pl script

The sm_configureFailover.pl tool establishes connections between the Active and Standby locations for Service Assurance Manager, Adapter Platform, and BIM. The tool creates subscriptions that are predefined and, depending on the configuration, sets them to the Enable or Disable states. The tool eliminates the manual task of adding subscriptions to Active and Standby hosts.

This utility uses the values from the `<BASEDIR>/smarts/local/conf/failover.conf` file as input. As a prerequisite, if you have not configured the failover.conf file, go to Configure SAM, Adapter Platform, and BIM for failover.

To create subscriptions to SAM, Adapter Platform and BIM:

1 Type:

   ```bash
   .,/sm_perl sm_configureFailover.pl -s
   ```

2 For each connection you are prompted to enter the manager name (for example INCHARGE-SA, INCHARGE-OI) and the VMware Smart Assurance administrator credentials (for example, admin/changeme).

After the script exits, it creates the following subscriptions:

- Disabled direct connection from Active SAM to Standby SAM.
- Disabled direct connection from Active SAM to Standby BIM.
- Enabled direct Connection from Standby SAM to Active SAM.
- Disabled direct connection from Standby SAM to Standby BIM
- Disabled direct connection from Standby SAM to Active BIM
- Disabled direct connection from Active Adapter Platform to Standby Adapter Platform.
- Enabled direct Connection from Standby Adapter Platform to Active Adapter Platform.

The script also accommodates Hierarchical SAM setup as well.

**Note** You may observe that after importing the configurations from an Active Service Assurance Manager into the Standby Service Assurance Manager, the console connected to the Standby SAM in the Failover setup disconnects for a brief duration and automatically reconnects.

Also, you can use this tool to append Domain Manager information to the failover.conf file, instead of manually modifying the failover.conf file. For example, if you add more Domain Managers to your failover system after you deploy the Failover Manager, you can append the information. Use the options in Syntax for the sm_configureFailover.pl script.

### Syntax for the sm_configureFailover.pl script

This utility uses the values from the `<BASEDIR>/smarts/local/conf/failover.conf` file as input.

**Syntax:**

```bash
sm_perl sm_configureFailover.pl [options...]
```

Options for the utility are provided in Syntax options for the sm_configureFailover.pl utility.

#### Table 3-5. Syntax options for the sm_configureFailover.pl utility

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--subscribe</td>
<td>Required, only creates subscriptions by using the failover.conf file in the <code>&lt;BASEDIR&gt;/smarts/local/conf/failover</code> directory. Specify this option by itself to create subscriptions for SAM, Adapter Platform and BIM. Also -s.</td>
</tr>
<tr>
<td>--append</td>
<td>Optional, creates subscriptions and appends information to the Server section in the failover.conf file. Used with the --file option. Valid for SAM, Adapter Platform, BIM, and all Domain Managers. Also -a.</td>
</tr>
</tbody>
</table>
Table 3-5. Syntax options for the sm_configureFailover.pl utility (Continued)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| --file=<file_path>/<file_name> | The --file option is mandatory if --append is specified. This text file contains the configuration details that need to be appended to the failover.conf file. The information in text file must be listed in this format:  

```plaintext
#DomainType DomainName portA portB hostA hostB directoryPathA directoryPathB
```

Example:

```plaintext
AMPM AMPM-test 4300 4300 ITOPS-QA-106 ITOPS-QA-108 <BASEDIR>/smarts <BASEDIR>/smarts
```

Also -f <file_path>/<file_name>.

--help                       | Print help and exit. Also -h.                                                                                                             |

Examples:

- This command creates only subscriptions for Active and Standby SAM, Adapter Platform, and BIM:

  ```plaintext
  ./sm_perl sm_configureFailover.pl -s
  ``

- This command edits the Server sections in the failover.conf file and creates the subscriptions accordingly.

  ```plaintext
  ./sm_perl sm_configureFailover.pl -s -a -f <file_path>/file.txt  
  SAM INCHARGE-SA 2000 2000 wpl-019-090.lss.emc.com  
  wpl-019-091.lss.emc.com /opt/InCharge/SAM/smarts /opt/InCharge/SAM/smarts  
  BIM INCHARGE-MBIM 2010 2010 wpl-019-090.lss.emc.com  
  wpl-019-091.lss.emc.com /opt/InCharge/SAM/smarts /opt/InCharge/SAM/smarts
  ```

Escalation policy changes

Note  This section applies to only the Service Assurance Manager.

Escalation is a function within SAM that executes various automatic, user-defined actions at specified time intervals. Escalation, when it is used, requires care when implementing the hot-Standby failover solution. While the Standby SAM should mimic a parallel behavior in terms of moving the notifications along the levels of an escalation path, it should not allow the same actions to be executed in the Standby SAM as in the Active SAM. If it did, actions would be duplicated, such as sending an email back to back for the same reason. On the other hand, escalation in the Standby SAM cannot be completely disabled because escalation needs to work as configured after a failover occurs.
For example, a given escalation path has three levels: Level-0 (action invoked immediately), Level-1 (action invoked 1 minute after Level-0), and Level-2 (action invoked 10 minutes after Level-1). A notification occurs; it matches the path, in both the Active and Standby SAMs, and Level-0 actions are executed immediately (for example, setting a UserDefined field), on the Active SAM. A minute passes and the Level-1 actions are executed (for example, sending an email to an engineer). During the succeeding minute, the Active SAM dies and a failover occurs.

The Standby SAM did not execute Level-0 and Level-1 actions because they were disabled. But the same notification is now scheduled to invoke Level-2 actions in the Standby SAM (after the specified interval). In the meantime, the Failover Manager reconfigures the path definition so that the automatic escalation actions are enabled in the Standby SAM after the failover. When Level-2 is reached, its actions are executed (for example, sending an email to an engineering manager) by the Standby SAM. In this manner, the notification was not affected by the failover during the transition in terms of its escalation actions.

The Failover Manager periodically transfers Global Manager configurations (Notification Lists, User Profiles, Actions, Escalation Policies, and so on) from the Active Service Assurance Manager to the Standby counterpart. However, the importing of escalation definitions with certain changes, such as a policy filter, may be restricted by the system.

**Note** You may observe that the Global Console connected to the Standby SAM in the Failover setup disconnects for a brief duration of 30-seconds while taking a backup of the action script, which transfers the Escalation policy from the Active SAM to the Standby SAM. This disconnect is expected as Failover Manager runs the importConfigFromFile on the ICS_ConfigurationManager or sm_config import with the --force --replace option. The Domain Managers will be reconfigured after this step.

An escalation policy or path must be in a disabled state when a filter is changed. Likewise, it must be disabled to add or remove levels, or change level intervals in an existing path. Refer to the VMware Smart Assurance Service Assurance Manager Configuration Guide for detailed information about how to modify existing escalation policy and paths.

When escalation is used with the hot-Standby failover solution, the escalation definitions in the Standby SAM may be inconsistent with the ones in the Active SAM. They may be inconsistent because changes made in the Active SAM could not be reflected in the Standby SAM.

If, for example, an escalation path is disabled, changed, and re-enabled on the Active SAM, and is then automatically transferred to the Standby SAM, the automatic transfer by the Failover Manager will fail. It fails because the path is still enabled on the Standby SAM, and any changes to the path (filters or level modifications) cannot be applied. Thus, all of the corresponding escalation paths in the Standby SAM must be disabled after they are modified in the Active SAM unless they are retired.

If escalation changes are accomplished by retiring a current path, instead of disabling and enabling it, there are no issues with copying them to the Standby SAM.

**Note** Disabling an escalation policy or path cancels all scheduled actions for the existing notifications that currently match an entity.
When it is necessary to disable an escalation path in an Service Assurance deployment where the hot-Standby failover solution is in effect, perform the following:

- Attach to the Active Service Assurance Manager by using the Global Manager Administration Console.
- Disable the escalation path.
- Make the necessary filter changes in the path, and re-enable it.
- Attach to the Standby Service Assurance Manager using the Global Manager Administration Console.
- Disable the escalation path.
- Detach from the Standby SAM.

**Next steps**

At this point, the configuration files on the Active components are not synchronized with the Standby components.

Complete the remaining steps in Deployment considerations. Continue to configure the Domain Managers for the Failover System. Then, configure Failover Manager and start it.

Once the Failover Manager is started, the Standby components will be synchronized. A manual backup step (Initiate manual backup) ensures the synchronization.
IP Manager Warm Failover

This chapter includes the following topics:

- Overview
- Configure IP Manager for failover

Overview

In a warm failover setup, an Active IP Availability Manager, IP Availability and Performance Manager or IP Performance Manager run on the Active host, and a Standby IP Availability Manager, IP Availability and Performance Manager or IP Performance Manager run on the Standby host. Preference is given to Location A for the Active IP Manager if no IP Manager is registered with the Broker. If any IP Manager is already registered with the Broker, that IP Manager is marked as Active.

Both Active and Standby IP Managers can poll the network. Failover occurs when the Active Domain Manager fails and the Standby Domain Manager becomes the Active Domain Manager with its current loaded topology (RPS). The monitoring process will be enabled in the newly-promoted Active Domain Manager, and it will start polling the devices. Only the Active Domain Manager actively polls the network. Failover Manager disables polling in the Standby IP Manager. The Standby Domain Manager only synchronizes network topology with the Active Domain Manager.

When the failed Domain Manager starts up, it becomes the Standby Domain Manager. Then, the backup actions happen from current Active Domain Manager to the current Standby Domain Manager.

Note: The Configuration Manager itself does not participate in failover and, as a result, has only one instance. “Troubleshooting IP Configuration Manager when the Tomcat service fails over” on page 69 describes the affect of service failover if you are using the Configuration Manager in the VMware M&R UI to control discovery configuration settings. The Configuration Manager service must be installed to be registered with both primary EDAA and secondary EDAA.

Restore and reconfigure topology in the Standby IP Manager

After each backup of the RPS file, the delta of the RPS in the Active IP Manager is loaded in the Standby IP Manager and reconfigure happens in the Standby IP Manager (however, Reconfigure happens for the entire topology). This way, the Standby IP Manager will be always up-to-date with the Active IP Manager.
Configure IP Manager for failover

Use the following steps to configure IP Manager for failover:

1. Configure Active and Standby IP Managers
2. Start the service for IP Manager
3. Configure the IP Manager as a source for SAM
4. Add IP Managers to the Failover Manager

**Note** Be aware that polling is not turned off until a failover occurs and then the Failover Manager controls the polling by disabling it for the Standby IP Manager. For this reason, VMware recommends not having any topology in the Standby IP Manager when you first start the Standby IP Manager.

Configure Active and Standby IP Managers

Install the service for the Active IP Manager on an Active server (host A) and install the service for the Standby IP Manager on the Standby server (host B). Ensure that the services for both IP Managers use fixed ports (--port option) and the --noregister mode. Run the following command from IP Manager installation directory:

**Example:**

```bash
./sm_service install --force --unmanaged --startmode=runonce \
  --name=ic-am-pm-server ' \
  --description=EMC Smarts Availability and Performance Manager Server' \
  '/<BASEDIR>/IP/smarts/bin/sm_server' \
  '--name=INCHARGE-AM-PM' \
  '--config=icf' \
  '--bootstrap=bootstrap-am-pm.conf' \
  '--subscribe=default' \
  '--ignore-restore-errors' \
  '--noregister' \
  '--port=1682' \
  '--output'
```

Start the service for IP Manager

Start the service for the IP Manager in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the `BASEDIR/smarts/bin` directory for the product.
2. Type: `./sm_service start < service_name >`
3. Press `Enter`. 
Repeat Steps 2-3 for each service name that is installed for your deployment.

### Table 4-1. IP Manager service names

<table>
<thead>
<tr>
<th>Product</th>
<th>Service name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Availability Manager</td>
<td>ic-am-server</td>
</tr>
<tr>
<td>IP Performance Manager</td>
<td>ic-pm-server</td>
</tr>
<tr>
<td>IP Availability and Performance Manager</td>
<td>ic-am-pm-server</td>
</tr>
</tbody>
</table>

**Windows**

To start the service from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Right-click **<EMC_Smarts_service>**.
3. Select **Start**.
4. Repeat Steps 2-3 for each service name that is installed for your deployment.

**Configure the IP Manager as a source for SAM**

Configure the IP Manager as a source for the Active SAM:

1. Attach a Global Console to the Active SAM by specifying “<FQDN hostA>:<portA>/<ServerName>” in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.Iss.emc.com:1751/INCHARGE-SA.
2. From the menu, select **Configure > Global Manager Administration Console**.
3. For the Active Service Assurance Manager, define the IP Manager as a source.
4. Add the IP Manager details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.
5. Specify the IP Manager domain name, leaving this connection initially enabled.
   
   Do not specify the fully qualified host name (FQDN host), because the Broker recognizes whether the Active or Standby component is operational.
6. In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select **INCHARGE-AM** (or INCHARGE-PM or INCHARGE-AM-PM), and click **Finish**.
7. Apply the configuration change and reconfigure the Active Service Assurance Manager.
Add IP Managers to the Failover Manager

Use the following steps to configure monitoring for IP Manager on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ```
   ./sm_edit conf/failover/failover.conf
   ```

2. Under the Server section, add an entry for the IP Manager to be monitored. Specify the ServerType as AM, PM or AMPM.

   **Note**   The ServerType must be selected based on the bootstrap file (--bootstrap option) used to start the IP Manager.

   The mapping is as follows:
   - AM - bootstrap-am.conf
   - PM - bootstrap-pm.conf
   - AMPM - bootstrap-am-pm.conf

   An example is provided below:

   ```
   Server
     {  
     DetachInterval = 480;
     Name           = "INCHARGE-AM";
     ServerType     = "AM";
     LocationA      
     {  
     HostName   = "itops-tco-212.lss.emc.com";
     PortNumber = 1682;
     Basedir    = "/opt/InCharge/IP/smarts";
     }
     LocationB      
     {  
     HostName   = "itops-tco-213.lss.emc.com";
     PortNumber = 1682;
     Basedir    = "/opt/InCharge/IP/smarts";
     }
     }
   ```

3. Save the failover.conf file and exit.

   **Note**   If you configure IP Manager for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.
MPLS Manager Warm Failover

This chapter includes the following topics:

- Overview
- MPLS Manager failover deployment scenarios
- Configure MPLS Manager for failover

Overview

The MPLS Manager is split into the following three components:

- **MPLS Topology Server**: This discovers the MPLS and VPN topology. The topology server works with the IP Availability Manager to discover the logical and physical objects in the physical-transport domain, the MPLS domain, and the VPN domain.

- **MPLS Monitoring Server**: This monitors the topology for status updates.

- **MPLS Analysis Server**: This analyzes the status updates to diagnose MPLS and VPN impacts.

A Failover solution for the MPLS manager comprises of the following components:

- Active and Standby **MPLS Topology Server**
- Active and Standby **MPLS Monitoring Server**
- Active and Standby **MPLS Analysis Server**

In the Standby **MPLS Topology Server**, auto-discovery and auto-pending discovery is disabled. In the Standby **MPLS Monitoring Server**, device polling and monitoring is disabled.

In all the Standby MPLS servers (Topology, Analysis and Monitoring) auto-synchronization is disabled for all the underlying Domain Managers. That means,

- The Standby **MPLS Topology Server** will not synchronize with Active IP Availability Manager or Standby IP Availability Manager.

- The Standby **MPLS Monitoring Server** will not synchronize with Active IP Availability Manager, Standby IP Availability Manager, Active **MPLS Topology Server**, or Standby **MPLS Topology Server**.
Standby MPLS Monitoring Server will not synchronize with Active MPLS Topology Server, Standby MPLS Topology Server, Active MPLS Monitoring Server, or Standby MPLS Monitoring Server.

After each backup interval, the backup will happen from the Active MPLS Topology Server to the Standby MPLS Topology Server, from Active MPLS Monitoring Server to Standby MPLS Monitoring Server, and from Active MPLS Analysis Server to Standby MPLS Analysis Server.

**MPLS Manager failover deployment scenarios**

This section illustrates the following MPLS Manager failover deployment scenarios:

- MPLS servers failover
- MPLS Topology Server Failover
- MPLS Monitoring Server Failover
- MPLS Analysis Server Failover

**MPLS servers failover**

MPLS servers failover deployment depicts the MPLS servers failover deployment.
MPLS Topology Server deployment

When Active MPLS Topology Server goes down, Standby MPLS Topology Server becomes Active. Auto-discovery, auto-pending discovery and topo-synchronization are enabled in the current Active MPLS Topology Server. MPLS Topology Server failover depicts the MPLS Topology Server deployment.
Figure 5-2. MPLS Topology Server failover

MPLS Monitoring Server failover

When Active MPLS Monitoring Server goes down, Standby MPLS Monitoring Server becomes Active. Polling, monitoring, and topo-synchronization are enabled in the current Active MPLS Monitoring Server. MPLS Monitoring Server failover depicts the MPLS Monitoring Server deployment.
MPLS Analysis Server failover

When Active MPLS Analysis Server goes down, Standby MPLS Analysis Server becomes Active. Polling, monitoring, and topo-synchronization are enabled in the current Active MPLS Analysis Server. **MPLS Analysis Server failover** depicts the MPLS Analysis Server deployment.
Configure MPLS Manager for failover

Use the following steps to configure MPLS Manager for failover:

1. Disable discovery and topology synchronization in MPLS Manager
2. Configure the MPLS Manager in the Active and Standby locations
3. Start the service for MPLS Manager
4. Configure the MPLS Manager as a source for SAM
5. Add the MPLS Manager to the Failover Manager
Disable discovery and topology synchronization in MPLS Manager

By default, the MPLS servers connect to the configured underlying IP Managers to fetch initial topology for MPLS discovery. This functionality needs to be disabled on both the Active and Standby MPLS Managers in a failover deployment before starting them.

The Failover Manager determines the MPLS component where the topology synchronization and discovery is enabled. Discovery or topology synchronization is always enabled on the Active MPLS Managers and disabled on the Standby MPLS Managers.

For both Active and Standby locations, use the following steps to disable discovery or topology synchronization for all three MPLS servers.

1. In the installation area where MPLS is running, go to the BASEDIR/smarts/bin directory and open the bootend.conf file for MPLS Topology Server. Type:

   ```
   ./sm_edit conf/mpls-t/bootend.conf
   ```

2. Navigate to the following section in the bootend.conf file and change the value of suspendTopologyManager from False to TRUE.

   ```
   ICF_TopologyManager::ICF-TopologyManager {
   # suspendTopologyManager
   # Suspends all topology manager operations
   # Set this to TRUE if you are using the MPLS Topology Server
   # in a failover configuration
   # Default value is FALSE
   suspendTopologyManager = TRUE
   }
   ```

3. Save the file and exit.

4. Repeat Steps 1-3 for the MPLS Monitoring Server. Change the value of suspendTopologyManager in the mpls-m/bootend.conf file.

5. Repeat Steps 1-3 for the MPLS Analysis Server. Change the value of suspendTopologyManager in the mpls-a/bootend.conf file.

Configure the MPLS Manager in the Active and Standby locations

**Note** A prerequisite for this step is that the Active and Standby IP Availability Managers and Active and Standby SAM are started.
Install the service for the Active MPLS Manager on an Active server (host A) with the --noregister option. Also, install the service for the Standby MPLS Manager on Standby server (host B) with the --noregister option.

- **For MPLS Topology Server example:**

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-mpls-topology' 
  '  --description=EMC Smarts MPLS Topology Server' 
  '<BASEDIR>/MPLS/smarts/bin/sm_server' 
  '  --name=INCHARGE-MPLS-TOPOLOGY' 
  '  --config=mps-t' 
  '  --ignore-restore-errors' 
  '  --noregister' 
  '  --port=1679' 
  '  --output'
  ```

- **For MPLS Monitoring Server example:**

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-mpls-monitoring' 
  '  --description=EMC Smarts MPLS Monitoring Server' 
  '<BASEDIR>/MPLS/smarts/bin/sm_server' 
  '  --name=INCHARGE-MPLS-MONITORING' 
  '  --config=mps-m' 
  '  --ignore-restore-errors' 
  '  --noregister' 
  '  --port=1680' 
  '  --output'
  ```

- **For MPLS Analysis Server example:**

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-mpls-analysis' 
  '  --description=EMC Smarts MPLS Analysis Server' 
  '<BASEDIR>/MPLS/smarts/bin/sm_server' 
  '  --name=INCHARGE-MPLS-ANALYSIS' 
  '  --config=mps-a' 
  '  --ignore-restore-errors' 
  '  --noregister' 
  '  --port=1681' 
  '  --output'
  ```

**Start the service for MPLS Manager**

Start the service for the MPLS Manager in the Active and Standby locations.
Linux

To start the service on Linux:

1. Navigate to the `BASEDIR/smarts/bin` directory for the product.
2. Type: `.sm_service start <service_name>`
3. Press `Enter`.

<table>
<thead>
<tr>
<th>Product</th>
<th>Service names</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Analysis Server</td>
<td>ic-mpls-analysis</td>
</tr>
<tr>
<td>MPLS Monitoring Server</td>
<td>ic-mpls-monitoring</td>
</tr>
<tr>
<td>MPLS Topology Server</td>
<td>ic-mpls-topology</td>
</tr>
</tbody>
</table>

1. Repeat Steps 2-3 for each service name that is installed for your deployment.

Windows

To start the service from the Windows desktop:

2. Right-click `<EMC_Smarts_service>`.
3. Select `Start`.
4. Repeat Steps 2-3 for each service name that is installed for your deployment.

Configure the MPLS Manager as a source for SAM

Configure the MPLS Manager as a source for the Active SAM:

1. Attach a Global Console to the Active SAM by specifying “<FQDN hostA>:<portA>/<ServerName>” in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.Iss.emc.com:1751/INCHARGE-SA.
2. From the menu, select `Configure > Global Manager Administration Console`.
3. For the Active Service Assurance Manager, define the MPLS components as a group for the source.
   - Under `ICS Configuration > IC Domain Configuration`, scroll down to Domain Groups and add a Group. Or if the default domain names are used, make sure that the group is enabled.
4. Apply the configuration change and reconfigure the Active Service Assurance Manager.

The `EMC Smarts MPLS Manager User Guide` provides additional information about configuring MPLS groups with Service Assurance Manager.
Add the MPLS Manager to the Failover Manager

Use the following steps to configure monitoring for MPLS Manager on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file.
   Type:
   ```
   ./sm_edit /conf/failover/failover.conf
   ```

2. Add entries for MPLS Topology, Monitoring, and Analysis servers in the ServerSection of the failover.conf file.

   **Example:**

   ```
   ServerSection
   {
   Server
   {
   DetachInterval = 300;
   Name = "INCHARGE-MPLS-TOPOLOGY";
   ServerType = "MPLS";
   LocationA
   {
   HostName = "itops-tco-100.lss.emc.com";
   PortNumber = 1679;
   Basedir = "/opt/In Charge/MPLS/smarts";
   }
   LocationB
   {
   HostName = "itops-tco-101.lss.emc.com";
   PortNumber = 1679;
   Basedir = "/opt/In Charge/MPLS/smarts";
   }
   }
   Server
   {
   DetachInterval = 300;
   Name = "INCHARGE-MPLS-MONITORING";
   ServerType = "MPLS";
   LocationA
   {
   HostName = "itops-tco-100.lss.emc.com";
   PortNumber = 1679;
   Basedir = "/opt/In Charge/MPLS/smarts";
   }
   LocationB
   {
   HostName = "itops-tco-101.lss.emc.com";
   PortNumber = 1679;
   Basedir = "/opt/In Charge/MPLS/smarts";
   }
   }
   ```
Server
{
  DetachInterval = 300;
  Name           = "INCHARGE-MPLS-ANALYSIS";
  ServerType     = "MPLS";
  LocationA
  {
      HostName   = "itops-tco-100.lss.emc.com";
      PortNumber = 1681;
      Basedir    = "/opt/InCharge/MPLS/smarts";
  }
  LocationB
  {
      HostName   = "itops-tco-101.lss.emc.com";
      PortNumber = 1681;
      Basedir    = "/opt/InCharge/MPLS/smarts";
  }
}

3 Save the failover.conf file and exit.

Note If you configure MPLS Manager for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.
Server Manager (ESM) Warm Failover

This chapter includes the following topics:
- Overview
- Configure Server Manager for failover

Overview

In a warm failover setup, an Active Server Manager runs on the Active host, and a Standby Server Manager runs on the Standby host. Preference is given to Location A for the Active Server Manager if no Server Manager is registered with the Broker. If any Server Manager is already registered with the Broker, that Server Manager is marked as Active.

Configure Server Manager for failover

Use the following steps to configure Server Manager for failover:

1. **Disable discovery and topology synchronization in the Server Manager**
2. **Configure the Server Manager in the Active and Standby locations**
3. **Start the service for Server Manager**
4. **Configure the Server Manager as a source for SAM**
5. **Add the Server Manager to the Failover Manager**

**Disable discovery and topology synchronization in the Server Manager**

By default, the Server Manager connects to the configured underlying IP Managers to fetch initial topology for ESM discovery. This functionality needs to be disabled on both the Active and Standby Server Managers in a failover deployment before starting them.

The Failover Manager determines the Server Manager where the topology synchronization and discovery is enabled. Discovery or topology synchronization is always enabled on the Active Server Manager and disabled on the Standby Server Manager.
For both Active and Standby locations, use the following steps to disable discovery or topology synchronization in the Server Manager:

1. In the installation area where the Server Manager is running, go to the `BASEDIR/smarts/bin` directory and open the `bootend.conf` file for Server Manager. Type:

   ```bash
   ./sm_edit conf/esm/bootend.conf
   ```

2. Navigate to the following section in the `bootend.conf` file and change the value of `suspendTopologyManager` from False to `TRUE`.

   ```bash
   ICF_TopologyManager::ICF-TopologyManager {
     # suspendTopologyManager
     # Suspends all topology manager operations
     # Set this to TRUE if you are using the ESM Server in a failover configuration
     # Default value is FALSE
     suspendTopologyManager = TRUE
   }
   ```

3. Save the file and exit.

**Configure the Server Manager in the Active and Standby locations**

Install the service for the Active Server Manager on an Active server (host A) and install the service for the Standby Server Manager on the Standby server (host B). Ensure that the services for both Server Managers use fixed ports (`--port` option) and the no register mode (`--noregister`). Run the following command from ESM installation directory:

Example:

```bash
./sm_service install --force --unmanaged --startmode=runonce --name=ic-esm-server --description=EMC Smarts Server Manager (ESM) --port=2640
```

**Start the service for Server Manager**

Start the service for the Server Manager in the Active and Standby locations.
Linux

To start the service on Linux:

1. Navigate to the BASEDIR/smarts/bin directory for the product.
2. Type: `./sm_service start ic-esm-server`
3. Press Enter.

Windows

To start the service from the Windows desktop:

2. Right-click Smart Assurance Server Manager.
3. Select Start.

Configure the Server Manager as a source for SAM

Configure the Server Manager as a source for the Active SAM:

1. Attach a Global Console to the Active SAM by specifying "<FQDN hostA>:<portA>/<ServerName>" in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.lss.emc.com:1751/INCHARGE-SA.
2. From the menu, select Configure > Global Manager Administration Console.
3. For the Active Service Assurance Manager, define the Server Manager as a source.
5. Specify the Server Manager domain name, leaving this connection initially enabled.
6. In the Domain Creation Wizard, under Copy existing drop-down list, select INCHARGE-ESM, and click Finish.
7. Apply the configuration change and reconfigure the Active Service Assurance Manager.

Add the Server Manager to the Failover Manager

Use the following steps to configure monitoring for Server Manager on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ```bash
   .sm_edit conf/failover/failover.conf
   ```
2 Under the Server section, add an entry for the Server Manager to be monitored. Specify the ServerType as ESM.

Example:

```plaintext
Server
{
    DetachInterval = 300;
    Name           = "INCHARGE-ESM";
    ServerType     = "ESM";
    DetachInterval = 300;
    LocationA
        {
            HostName   = "itops-tco-212.lss.emc.com";
            PortNumber = 2640;
            Basedir    = "/opt/InCharge/ESM/smarts";
        }
    LocationB
        {
            HostName   = "itops-tco-213.lss.emc.com";
            PortNumber = 2640;
            Basedir    = "/opt/InCharge/ESM/smarts";
        }
}
```

3 Save the `failover.conf` file and exit.

**Note** If you configure Server Manager for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.
Network Protocol Manager
Warm Failover

This chapter includes the following topics:
- Overview
- Configure Network Protocol Manager for failover

Overview

The Network Protocol Manager is split into the following four components:

- **BGP server**: Network Protocol Manager for BGP diagnoses connectivity failures for an exterior gateway protocol known as Border Gateway Protocol. NPM for BGP works with IP Availability Manager to discover and monitor network devices that are running BGP services, diagnoses BGP-related failures, and exports the results of its analysis to the Global Manager.

- **EIGRP server**: Network Protocol Manager for EIGRP diagnoses connectivity failures for a Cisco proprietary interior gateway protocol known as Enhanced Interior Gateway Routing Protocol. NPM for EIGRP works with IP Availability Manager to discover and monitor Cisco devices that are running EIGRP services, diagnoses EIGRP-related failures, and exports the results of its analysis to the Global Manager.

- **IS-IS**: Network Protocol Manager for IS-IS diagnoses connectivity failures for an interior gateway protocol known as Intermediate System to Intermediate System. Network Protocol Manager for IS-IS works with IP Availability Manager to discover and monitor network devices that are running IS-IS services, diagnoses IS-IS-related failures, and exports the results of its analysis to the Global Manager.

- **OSPF server**: Network Protocol Manager for OSPF diagnoses connectivity failures for an interior gateway protocol known as Open Shortest Path First. NPM for OSPF works with IP Availability Manager to discover and monitor network devices that are running OSPF services, diagnoses OSPF-related failures, and exports the results of its analysis to the Global Manager.

A failover solution for the Network Protocol Manager comprises of the following components:

- Active and Standby BGP Server
- Active and Standby EIGRP Server
- Active and Standby IS-IS Server
Active and Standby OSPF Server

Configure Network Protocol Manager for failover

Use the following steps to configure Network Protocol Manager for failover:

1. Disable discovery and topology synchronization in Network Protocol Manager
2. Configure NPM in the Active and Standby locations
3. Start the service for Network Protocol Manager
4. Configure the Network Protocol Manager as a source for SAM
5. Add Network Protocol Manager to the Failover Manager

Disable discovery and topology synchronization in Network Protocol Manager

By default, the Network Protocol Manager connects to the configured underlying IP Managers to fetch initial topology for NPM discovery. This functionality needs to be disabled on both the Active and Standby Network Protocol Managers in a failover deployment before starting them.

The Failover Manager determines the NPM component where the topology synchronization and discovery is enabled. Discovery or topology synchronization is always enabled on the Active Network Protocol Managers and disabled on the Standby Network Protocol Managers.

For both Active and Standby locations, use the following steps to disable discovery or topology synchronization in Network Protocol Manager:

1. In the installation area where NPM is running, go to the BASEDIR/smarts/bin directory and open the bootend.conf file for NPM BGP Server. Type:

   ```
   ./sm_edit conf/bgp/bootend.conf
   ```

2. Navigate to the following section in the `bootend.conf` file and change the value of `suspendTopologyManager` from False to TRUE.

   ```
   ICF_TopologyManager::ICF-TopologyManager {
   # suspendTopologyManager
   # Suspends all topology manager operations
   # Set this to TRUE if you are using the BGP Server
   # in a failover configuration
   # Default value is FALSE
   suspendTopologyManager = TRUE
   }
   ```

3. Save the file and exit.

4. Repeat Steps 1-3 for the NPM EIGRP Server. Change the value of `suspendTopologyManager` in the `eigrp/bootend.conf` file.
5 Repeat Steps 1-3 for the NPM IS-IS Server. Change the value of suspendTopologyManager in the
  isis/bootend.conf file.

6 Repeat Steps 1-3 for the NPM OSPF Server. Change the value of suspendTopologyManager in the
  ospf/bootend.conf file.

Configure NPM in the Active and Standby locations

Note A prerequisite for this step is that the Active and Standby IP Availability Managers and Active and
Standby SAM are started.

Install the service for the Active Network Protocol Manager on an Active server (host A) with the
  --noregister option. Also, install the service for the Standby Network Protocol Manager on Standby server
  (host B) with the --noregister option.

  For NPM BGP Server example:

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-npm-bgp-server' 
  '  --description=EMC Smarts NPM for BGP Server' 
  '<BASEDIR>/MPLS/smarts/bin/sm_server' 
  '  --name=INCHARGE-BGP' 
  '  --config=bgp' 
  '  --ignore-restore-errors' 
  '  --noregister' 
  '  --port=1679' 
  '  --output' 
  ```

  For NPM EIGRP Server example:

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-npm-eigrp-server' 
  '  --description=EMC Smarts NPM for EIGRP Server' 
  '<BASEDIR>/NPM/smarts/bin/sm_server' 
  '  --name=INCHARGE-EIGRP' 
  '  --config=eigrp' 
  '  --ignore-restore-errors' 
  '  --noregister' 
  '  --port=1681' 
  '  --output' 
  ```

  For NPM IS-IS Server example:

  ```
  ./sm_service install --force --unmanaged --startmode=runonce 
  '  --name=ic-npm-isis-server' 
  '  --description=EMC Smarts NPM for ISIS Server' 
  '<BASEDIR>/NPM/smarts/bin/sm_server' 
  '  --name=INCHARGE-ISIS' 
  '  --config=isis' 
  '  --ignore-restore-errors' 
  ```
For NPM OSPF Server example:

```bash
./sm_service install --force --unmanaged --startmode=runonce \
  --name=ic-npm-ospf-server' \
  --description=EMC Smarts OSPF Server' \
  '<BASEDIR>/NPM/smarts/bin/sm_server' \
  --name=INCHARGE-OSPF' \
  --config=ospf' \
  --ignore-restore-errors' \
  --noregister'\n  --port=1680'\n  --output'
```

Start the service for Network Protocol Manager

Start the service for the Network Protocol Manager in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the `BASEDIR/smarts/bin` directory for the product.
2. Type: `./sm_service start < service_name >`
3. Press Enter.

**Windows**

To start the service from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services.**
2. Right-click `<EMC_Smarts_service>`.
3. Select **Start.**
4 Repeat Steps 2-3 for each service name that is installed for your deployment.

**Configure the Network Protocol Manager as a source for SAM**

Configure the Network Protocol Manager as a source for the Active SAM:

1 Attach a Global Console to the Active SAM by specifying “<FQDN hostA>:<portA>/<ServerName>” in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.iss.emc.com:1751/INCHARGE-SA.

2 From the menu, select **Configure > Global Manager Administration Console**.

3 For the Active Service Assurance Manager, define the Network Protocol Manager as a source.

4 Add the NPM BGP Server details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.

5 Specify the NPM BGP Server domain name, leaving this connection initially enabled.

6 In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select **INCHARGE-BGP**, and click **Finish**.

7 Repeat Steps 3a-c for the NPM EIGRP Server. Select **INCHARGE-EIGRP**.

8 Repeat Steps 3a-c for the NPM IS-IS Server. Select **INCHARGE-ISIS**.

9 Repeat Steps 3a-c for the NPM OSPF Server. Select **INCHARGE-OSPF**.

10 Apply the configuration change and reconfigure the Active Service Assurance Manager.

**Add Network Protocol Manager to the Failover Manager**

Use the following steps to configure monitoring for Network Protocol Manager on the Failover Manager:

1 From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ./sm_edit conf/failover/failover.conf

2 Add entries for BGP, EIGRP, IS-IS, and OSPF servers in the ServerSection of the failover.conf file.

   **Example:**

   ```
   ServerSection
   {
   Server
   {
   DetachInterval = 300;
   Name           = "INCHARGE-BGP";
   ServerType     = "NPM";
   LocationA
   {
   HostName   = "host-NPM-A";
   PortNumber = 1679;
   }
   }...
   ```
Basedir = "/opt/InCharge/NPM/smarts";

LocationB
{
  HostName = "host-NPM-B";
  PortNumber = 1679;
  Basedir = "/opt/InCharge/NPM/smarts";
}
}
Server
{
  DetachInterval = 300;
  Name = "INCHARGE-EIGRP";
  ServerType = "NPM";
  LocationA
  {
    HostName = "host-NPM-A";
    PortNumber = 1681;
    Basedir = "/opt/InCharge/NPM/smarts";
  }
  LocationB
  {
    HostName = "host-NPM-B";
    PortNumber = 1681;
    Basedir = "/opt/InCharge/NPM/smarts";
  }
}
}
Server
{
  DetachInterval = 300;
  Name = "INCHARGE-ISIS";
  ServerType = "NPM";
  LocationA
  {
    HostName = "host-NPM-A";
    PortNumber = 1681;
    Basedir = "/opt/InCharge/NPM/smarts";
  }
  LocationB
  {
    HostName = "host-NPM-B";
    PortNumber = 1681;
    Basedir = "/opt/InCharge/NPM/smarts";
  }
}
}
Server
{
  DetachInterval = 300;
  Name = "INCHARGE-OSPF";
  ServerType = "NPM";
  LocationA
  {
    HostName = "host-NPM-A";
    PortNumber = 1680;
    Basedir = "/opt/InCharge/NPM/smarts";
  }
}
3 Save the failover.conf file and exit.

**Note** If you configure Network Protocol Manager for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.
VoIP Availability Manager Warm Failover

Configure VoIP Availability Manager for failover

Use the following steps to configure VoIP Availability Manager for failover:

1. Disable discovery and topology synchronization in VoIP Availability Manager
2. Configure the VoIP Availability Manager in the Active and Standby locations
3. Configure VoIP Trap Adapter on Active and Standby hosts
4. Start the services for VoIP Availability Manager and VoIP Trap Adapter
5. Configure the VoIP Availability Manager as a source for SAM
6. Add VoIP Availability Manager and VoIP Trap Adapter to the Failover Manager

Disable discovery and topology synchronization in VoIP Availability Manager

By default, the VoIP Availability Manager connects to the configured underlying IP Managers to fetch initial topology for VoIP Availability Manager discovery. This functionality needs to be disabled on both the Active and Standby VoIP Availability Managers in a failover deployment before starting them.

The Failover Manager determines the VoIP Availability Manager where the topology synchronization and discovery is enabled. Discovery or topology synchronization is always enabled on the Active VoIP Availability Manager and disabled on the Standby VoIP Availability Manager.

For both Active and Standby locations, use the following steps to disable discovery or topology synchronization in VoIP Availability Manager:

1. In the installation area where VoIP Availability Manager is running, go to the BASEDIR/smarts/bin directory and open the bootend.conf file for VoIP Availability Manager. Type:

   ```bash
   ./sm_edit conf/voip/bootend.conf
   ```
2 Navigate to the following section in the `bootend.conf` file and change the value of `suspendTopologyManager` from False to TRUE.

```
ICF_TopologyManager::ICF-TopologyManager {
# suspendTopologyManager
# Suspends all topology manager operations
# Set this to TRUE if you are using the VoIP Server
# in a failover configuration
# Default value is FALSE
    suspendTopologyManager = TRUE
}
```

3 Save the file and exit.

**Configure the VoIP Availability Manager in the Active and Standby locations**

Install the service for the Active VoIP Availability Manager on an Active server (host A) and install the service for the Standby VoIP Availability Manager on the Standby server (host B). Ensure that the services for both VoIP Availability Managers use fixed ports (--port option) and the no register mode (--noregister). Run the following command from VoIP Availability Manager installation directory:

Example:

```
./sm_service install --force --unmanaged --startmode=runonce \
    '--name=ic-voip-server' \
    '--description=EMC Smarts VoIP Availability Manager' \
    '--env=SM_JAVA_ENABLED=YES' \
    '<BASEDIR>/VoIP/smarts/bin/sm_server' \
    '--noregister' \
    '--name=VoIP-AM' \
    '--config=voip' \
    '--subscribe=default' \
    '--output' \
    '--port=2700' \
    '--ignore-restore-errors'
```

The *VMware Smart Assurance System Administration Guide* provides complete information about the `sm_service` command options.
Configure VoIP Trap Adapter on Active and Standby hosts

A VoIP Trap Adapter, like any other trap adapter can be configured for failover. If the Active VoIP Trap Adapter fails, the Failover Manager tries to restart the Active VoIP Trap Adapter.

1 Install the service for the VoIP Trap Adapter on both the Active (Host A) and Standby (Host B) servers using the following command:

Example:

```bash
./sm_service install --force --unmanaged --startmode=runonce
--name=ic-voip-notification-trapd-receiver
--description="EMC VoIP Notification Trap Adapter"
<BASEDIR>/VoIP/smarts/bin/sm_trapd
--name=TRAP-INCHARGE-VOIP
--server=INCHARGE-OI
--config=voip
--port=9002
--model=sm_actions
--rules=voip/voip_trap_mgr_parse.asl
--output=TRAP-INCHARGE-VOIP
```

2 Also, configure the Active and Standby VoIP Trap Adapters to forward traps to the VoIP Availability Manager. Use the instructions in the VMware Smart Assurance VoIP Availability Manager Configuration Guide.

3 Use the service name ic-voip-notification-trapd-receiver to start the VoIP Trap Adapter as described in Start the services for VoIP Availability Manager and VoIP Trap Adapter.

   The VoIP Availability Manager processes the traps from the VoIP Trap Adapter. For more information, consult the VMware Smart Assurance VoIP Availability Manager documentation.

Start the services for VoIP Availability Manager and VoIP Trap Adapter

Start the services for the VoIP Availability Manager and the VoIP Trap Adapter in the Active and Standby locations.

Linux

To start the service on Linux:

1 Navigate to the BASEDIR/smarts/bin directory for the product.

2 Type: ./sm_service start < service_name >

3 Press Enter.

4 Repeat Steps 2-3 for each service name that is installed for your deployment.
<table>
<thead>
<tr>
<th>Product</th>
<th>Service name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Availability Manager</td>
<td>ic-voip-server</td>
</tr>
<tr>
<td>VoIP Trap Adapter</td>
<td>ic-voip-notification-trapd-receiver</td>
</tr>
</tbody>
</table>

**Windows**

To start the service from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Right-click `<EMC_Smarts_service>`.
3. Select **Start**.
4. Repeat Steps 2-3 for each service name that is installed for your deployment.

**Configure the VoIP Availability Manager as a source for SAM**

Configure the VoIP Availability Manager as a source for the Active SAM:

1. Attach a Global Console to the Active SAM by specifying “<FQDN hostA>:<portA>/<ServerName>” in the Manager Name field of the Attach Manager Dialog Box. For example, itops-tco-217.lss.emc.com:1751/INCHARGE-SA.
2. From the menu, select **Configure > Global Manager Administration Console**.
3. For the Active Service Assurance Manager, define the VoIP Availability Manager as a source.
4. Add the VoIP Availability Manager details under **ICS Configuration > IC Domain Configuration**. Right-click **Domains** and select **New Domain**.
5. Specify the VoIP Availability Manager domain name, leaving this connection initially enabled.
6. In the **Domain Creation Wizard**, under **Copy existing** drop-down list, select **VoIP-AM**, and click **Finish**.
7. Apply the configuration change and reconfigure the Active Service Assurance Manager.

**Add VoIP Availability Manager and VoIP Trap Adapter to the Failover Manager**

To configure monitoring for VoIP Availability Manager and the VoIP Trap Adapter on the Failover Manager:

1. From the installation directory of failover monitor (BASEDIR/smarts/bin), open the failover.conf file. Type:

```
./sm_edit conf/failover/failover.conf
```
2. Under the Server section, add an entry for the VoIP Availability Manager to be monitored. Specify the ServerType as VoIP. Example:

```plaintext
Server
{
  DetachInterval = 300;
  Name           = "VoIP-AM";
  ServerType     = "VoIP";
  LocationA
  {
    HostName   = "host-VOIP-A";
    PortNumber = 2700;
    Basedir    = "/opt/InCharge/VoIP/smarts";
  }
  LocationB
  {
    HostName   = "host-VOIP-B";
    PortNumber = 2700;
    Basedir    = "/opt/InCharge/VoIP/smarts";
  }
}
```

3. Add an entry for the VoIP Trap Adapter to be monitored. Specify the ServerType as TRAPD. Example:

```plaintext
Server
{
  Name           = "TRAP-INCHARGE-VOIP";
  ServerType     = "TRAPD";
  LocationA
  {
    HostName   = "host-VOIP-A";
    PortNumber = 9002;
    Basedir    = "/opt/InCharge/VoIP/smarts";
    InstalledServiceName = "ic-voip-notification-trapd-receiver";
  }
  LocationB
  {
    HostName   = "host-VOIP-B";
    PortNumber = 9002;
    Basedir    = "/opt/InCharge/VoIP/smarts";
    InstalledServiceName = "ic-voip-notification-trapd-receiver";
  }
}
```

4. Save the failover.conf file and exit.

**Note**: If you configure VoIP Availability Manager for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.
This chapter discusses the configuration of a Trap Adapter failover. Topics include:

- Configure Trap Adapter
- Verify failover status

This chapter includes the following topics:

- Configure Trap Adapter
- Verify failover status

### Configure Trap Adapter

The Failover Manager registers the Active Trap Adapter with a Broker. The Standby Trap Adapter is not registered with a Broker until the Standby Trap Adapter changes to an Active state. When no failover occurs, the Standby Trap Adapter only receives the traps and does not forward them to SAM.

Use the following steps to configure Trap Adapter, acting as a trap receiver, for failover:

1. **Configure the Trap Adapter service on Active and Standby locations**
2. **Start the Trap Adapter service**
3. **Add the Trap Adapter to the Failover Manager**

### Configure the Trap Adapter service on Active and Standby locations

1. Install the service for the Trap Adapter on both the Active (Host A) and Standby (Host B) servers using the following command:

   **Example:**

   ```bash
   ./sm_service install --force --unmanaged --startmode=runonce
   '---name=ic-trapd-receiver' \
   '---description=EMC Smarts SNMP Trap Adapter' \
   '/<BASEDIR>
   /SAM/smarts/bin/sm_trapd' \
   '---name=TRAP-INCHARGE-OI' \
   '---server=INCHARGE-OI'
   ```

 VMware, Inc.  75
Configure the Active and Standby Trap Exploders to forward traps to Active and Standby Trap Adapters. Configure trap forwarding to Active and Standby Trap Adapters provides this information.

**Start the Trap Adapter service**

Start the service for the Trap Adapter in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the BASEDIR/smarts/bin directory for the product.
2. Type: `.sm_service start ic-trapd-receiver`
3. Press `Enter`.

**Windows**

To start the service from the Windows desktop:

2. Right-click `EMC Smarts SNMP Trap Adapter`.
3. Select `Start`.

**Add the Trap Adapter to the Failover Manager**

Use the following steps to configure monitoring for the Trap Adapter on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ```bash
   ./sm_edit /conf/failover/failover.conf
   ```

2. Under the Server section, add Trap Adapter details with Server Type as TRAPD. An example is provided below:

   ```json
   Server
   {
     Name           = "TRAP-INCHARGE-OI";
     ServerType     = "TRAPD";
   }
   ```
3  Save the failover.conf file and exit.

Note  If you configure Trap Adapter for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.

Verify failover status

Check the failover log in the BASEDIR/smarts/local/logs directory for the monitoring status and role of the Active and Standby Trap Adapter (TRAPD). The status of the Active Trap Adapter must be UP/ACTIVE and the status of the Standby Trap Adapter must be UP/STANDBY, respectively.
This chapter includes the following topics:

- Overview
- Configure the Trap Exploder for failover
- Verify failover status

Overview

The Trap Exploder failover setup includes two hosts with an identical configuration for starting the Trap Exploder. Traps are sent to both Trap Exploders. Both Trap Exploders are receiving traps, but only the Active Trap Exploder is forwarding traps. The Active Trap Exploder forwards traps to both, active and standby, Trap Adapters. Failover Manager suspends trap forwarding in the Standby Trap Exploder.

If the Active Trap Exploder fails, the Failover Manager makes two attempts to restart it. If the two attempts fail, the Failover Manager proceeds to fail over to the Standby Trap Exploder. The Failover Manager registers the Standby Trap Exploder with the Broker and un-suspends trap forwarding in it and changes its role to Active. The FailoverRetries parameter in the failover.conf file determines the number of failover attempts.

If the Standby Trap Exploder fails, the current Active Trap Exploder continues to forward the traps, the Failover Manager attempts to restart the Standby Trap Exploder. If restart is successful, the Failover Manager makes sure that trap forwarding is suspended in the Standby Trap Exploder. If the Failover Manager fails to restart the Standby Trap Exploder, there are no entries taken and you will need to manually restart the Standby Trap Exploder.

Configure the Trap Exploder for failover

Use the following steps to configure the Trap Exploder for failover:

1. Configure the Trap Exploder service on Active and Standby locations
2. Start the Trap Exploder service
3. Configure trap forwarding to Active and Standby Trap Adapters
4. Add the Trap Exploder to the Failover Manager
Configure the Trap Exploder service on Active and Standby locations

Install the service for the Trap Exploder on both the Active (Host A) and Standby (Host B) servers in the --noregister mode, using the following command:

Example:

```
./sm_service install --force --unmanaged --startmode=runonce
  --name=ic-trapd-exploder
  --description=EMC Smarts SNMP Trap Exploder
  /<BASEDIR>/SAM/smarts/bin/sm_trapd
  --name=TRAP-INCHARGE-Exploder
  --config=trapd
  --sport=2999
  --port=1025
  --model=sm_actions
    --rules=default
    --seed=seedfile
    --noregister
  --output=TRAP-EXPLODER-OI.log
```

Start the Trap Exploder service

Start the service for the Trap Exploder in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the BASEDIR/smarts/bin directory for the product.
2. Type: `./sm_service start ic-trapd-exploder`
3. Press Enter.

**Windows**

To start the service from the Windows desktop:

2. Right-click EMC Smarts SNMP Trap Exploder.
3. Select Start.
Configure trap forwarding to Active and Standby Trap Adapters

To forward traps from the Trap Exploder to Active and Standby Trap Adapters, perform these steps on both Active and Standby Trap Exploder:

1. From the `<BASEDIR>/SAM/smarts/bin` directory, type:

   ```
   ./sm_edit ../conf/trapd/trapd.conf
   ```

2. Add the following forwarding line:

   ```
   FORWARD: *.*.*.* .* * * <host1>:162 <host2>:162
   ```

3. Save the file and exit.

Add the Trap Exploder to the Failover Manager

Use the following steps to configure monitoring for the Trap Exploder on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ```
   ./sm_edit /conf/failover/failover.conf
   ```

2. Under the Server section, add Trap Exploder details with Server Type as TRAPE. An example is provided below:

   ```
   Server
   {
   Name           = "TRAP-INCHARGE-EXPLODER";
   ServerType     = "TRAPE";
   LocationA
   {
   HostName   = "host-TRAPE-A";
   PortNumber = 2999;
   Basedir    = "/opt/InCharge/SAM/smarts";
   InstalledServiceName = "ic-trapd-exploder";
   }
   LocationB
   {
   HostName   = "host-TRAPE-B";
   PortNumber = 2999;
   Basedir    = "/opt/InCharge/SAM/smarts";
   InstalledServiceName = "ic-trapd-exploder";
   }
   }
3 Save the failover.conf file and exit.

**Note** If you configure Trap Exploder for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.

### Verify failover status

Check the failover log in the BASEDIR/smarts/local/logs directory for the monitoring status and role of the Active and Standby Trap Exploder (TRAPE). The status of the Active Trap Exploder must be UP/ACTIVE and the status of the Standby Trap Exploder must be UP/STANDBY, respectively.
This chapter includes the following topics:
- Overview
- Broker failover scenarios
- Configure the Broker for failover
- Optional additional configuration tasks for Broker failover

Overview

The VMware Smart Assurance Failover solution includes automatic failover for the Broker in a failover deployment. The Failover Manager treats Brokers as Active or Standby. The Failover Manager monitors the Active Broker, detects when an Active Broker fails, and switches the newly-promoted Broker for other Active Domain Managers.

Figure 7 shows the deployment of the failover solution to support Broker failover.
The Broker failover setup includes two or more hosts with identical configuration. Each host can run one or more Brokers. All Brokers that are configured on these hosts are running at all times.

The Failover Manager monitors any number of Brokers you have defined. If the Active host has multiple Brokers configured, the Failover Manager recognizes them in the order of their entries in the failover.conf as Broker0 (first entry), Broker1, and so on. Typically, the Broker is deployed on the same host as the Service Assurance Manager and the Failover Manager.

**Failover Manager initialization and Broker registration**

When you start the Failover Manager, it determines the status of each Broker and the running Broker that has the lowest priority (for example, Broker0) is designated as Active. The Failover Manager treats all other Brokers as Standby.

Next, the Failover Manager registers all Active components, that it monitors, to all Brokers. At any given time, all Brokers know the location of all Active components. The information in the Brokers allows the consoles and other clients to attach to the Active processes.

Since the Broker is critical to the Failover System, the Failover Manager periodically verifies the Broker's operational state.

During a failover, the Failover Manager registers the newly-promoted Broker with the Active components. It switches the Broker in the memory of all Active components to the Broker that is currently active.

All Brokers will list the current set of active domains.

*Broker failover scenarios on page 53* describes the failover scenarios for the Broker.
Monitoring the Broker

The monitoring of the Broker is performed in the same way as the VMware Smart Assurance products: the Broker and its host are periodically checked for responsiveness.

InChargeBroker class attributes

The following InChargeBroker class attributes are available when you attach the console to the Failover Manager:

- **BrokerPriority**—The priority number that is assigned to the Broker.
- **BrokerRole**—The Failover role that the Broker is assigned.
  - **UNKNOWN**—The Broker role is not determined.
  - **ACTIVE**—The Broker has the active role.
  - **STANDBY**—The Broker has the standby role.
- **InstalledServiceName**—The name of the Broker service as registered with the sm_service daemon on the Host that the Broker is running on. This attribute can be defined in the failover.conf file for each Broker entry.

Broker failover scenarios

The Failover Manager handles the failover for a Broker differently depending on whether it is an Active or Standby Broker.

**Broker host fails**

If the host on which the Broker is installed fails, Failover Manager sends a Warning email that the Broker host has failed. Also, the Failover Manager initiates a failover.

**Active Broker fails**

When a Broker that is currently assigned an Active role fails, the Failover Manager takes the following actions:

1. The Failover Manager determines the next candidate to make Active based on the priority and running states of other Brokers.
After identifying the new Active Broker, the Failover Manager updates the Broker on all other Active components (SAM and Domain Managers) and within the Failover Manager as well. This ensures that any component that wants to synchronize with another component will have a Broker that can be used.

For the SAM server with Notification Cache Publishing, when the Active Broker fails,

- The Failover Manager uses the OnChangePOST value from the failover.conf file to update the new Broker URL location in the EMC Data Access API (smarts-edaa).
- User intervention is required to reconfigure the SolutionPack for EMC Smarts to point to the Broker on the Standby site. In the SolutionPack, the Failover Manager updates the new EDAA details in the Report Section automatically. In the Data Collection and Events sections, you need to manually update the new Broker details.

   This may depend on the version of EMC M&R as described in Failover of UI services is supported with Service Assurance Manager (SAM) 9.4 and VMware M&R 6.5u1.

The Failover Manager tries to restart the failed Broker if the host where it resides is functioning.

- If the InstalledServiceName attribute is defined, the Failover Manager tries to restart the failed Broker service.
- If the InstalledServiceName attribute is not defined, the Failover Manager tries to start the failed Broker using the brstart command.

If restarting the failed Broker is successful, the Failover Manager marks the restarted Broker as Standby.

The Failover Manager sends a Broker Restart email that an error occurred during the restart of the Broker <host:port> or the restart of the Broker <host:port> successfully completed.

If you want to switch the newly-promoted Broker back to Standby and the Standby Broker back to Active, perform a failback action as described in Optional additional configuration tasks for Broker failover.

Standby Broker fails

If a Standby Broker fails, the Failover Manager tries to restart the Broker if the host where it resides is functioning. The restart method used by the Failover Manager depends on the value assigned to the InstalledServiceName attribute.

Failover of other Domain Managers

Handling failover of other Domain Managers includes an additional step.

When an Active Domain Manager such as IP Manager or SAM fails, the Failover Manager switches the Broker on the peer domain before performing a failover. For example, the IP Manager on Location A is active and the IP Manager on Location B is standby. If the IP Manager on Location A fails, the Failover Manager switches the Broker for the IP Manager on Location B to point to the Active Broker first before the failover to the IP Manager on Location B is initiated.
Limitations

While the Active Broker is unavailable, the following limitations have been observed on components in a failover deployment.

The Failover Manager polls each Domain Manager and Broker at fixed intervals to determine their status. Consequently, a few polling cycles pass before the Failover Manager determines that an Active Broker has failed. During this time frame, the Active Domain Managers may not be able to communicate with each other until the Broker for them is switched by the Failover Manager to point to another running Broker. This behavior occurs only with topology-synchronization among Domain Managers.

To overcome the impact due to this limitation, configure separate polling intervals for Brokers and other Domain Managers. For example, if the Failover Manager polls IP Manager, SAM, and other Domain Managers at an interval of 4 minutes, then configure the polling interval for Brokers at 1 minute.

Failover of UI services is supported with Service Assurance Manager (SAM) 9.4 and VMware M&R 6.5u1

When a SAM server with Notification Cache Publishing Enabled or any of the associated UI services (Tomcat, Rabbit MQ, and ElasticSearch) fail, the EMC Data Access API (EDAA) is pointed to other servers listed in the Reports configuration screen in the Solutionpack for VMware Smart Assurance.

This failover solution works only with a combination of SAM 9.4 with Notification Cache Publishing Enabled and VMware M&R 6.5u1 or later versions of both.

This UI Services failover solution will not work for VMware M&R 6.4.x versions or earlier.

Example: If SAM 9.4 with Notification Cache Publishing Enabled is configured to work with VMware M&R 6.4u2, the UI services failover solution is not supported.

Configure the Broker for failover

Use the following steps to configure the Broker for failover:

1. Configure the Broker service in Active and Standby locations
2. Start the service for the Broker
3. Add the Broker to the Failover Manager
4. Display the Failover Manager status of the Broker

Configure the Broker service in Active and Standby locations

Install the service for the Active Broker on an Active server (host A) and install the service for the Standby Broker on the Standby server (host B) using the command below:
Example:

```bash
./sm_service install --force --unmanaged --startmode=runonce
    '---name=ic-broker' \
    '---description=EMC Smarts Broker' \
    '---env=SM_CLIENTCONNECT=brokerConnect.conf' \
    '/opt/InCharge/SAM/smarts/bin/brstart' \ 
    '---port=1751' \ 
    '---restore=/opt/InCharge/SAM/smarts/local/repos/broker/broker.rps'
    '---output'
```

Start the service for the Broker

Start the service for the Broker in the Active and Standby locations.

**Linux**

To start the service on Linux:

1. Navigate to the `BASEDIR/smarts/bin` directory for the product.
2. Type: `./sm_service start ic-broker`
3. Press `Enter`.

**Windows**

To start the service from the Windows desktop:

2. Right-click `EMC Smarts Broker`.
3. Select `Start`.

Add the Broker to the Failover Manager

The Failover Manager registers with all Brokers specified in the failover.conf file.

You can add any number of Brokers to the BrokerSection of the failover.conf file.

When the Failover Manager starts, it assigns priorities to Brokers based on each Broker’s order of definition in failover.conf under the BrokerSection.

The Failover Manager assigns the first Broker entry a priority of 0. The first Broker entry is always the default Active Broker. If you want the Broker running on Location A to be the Active Broker, define it as the first entry under the BrokerSection. Then, define the Standby Broker and any other alternate Broker after the first Broker entry.
Use the following steps to configure monitoring for the Broker on the Failover Manager:

1. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

   ```
   ./sm_edit conf/failover/failover.conf
   ```

2. Under the Broker section, uncomment the Broker entries and modify them as needed (for example, change the default port 426 to a value greater than 1024). The first entry for Host A is treated as the Active Broker.

   ```
   BrokerSection
   {
    # Broker
    # {
    #    HostName   = "broker-host-A";
    #    PortNumber = 426;
    #    Basedir    = "/opt/InCharge/SAM/smarts";
    #    InstalledServiceName = "ic-broker";
    # }
    # Broker
    # {
    #    HostName   = "broker-host-B";
    #    PortNumber = 426;
    #    Basedir    = "/opt/InCharge/SAM/smarts";
    #    InstalledServiceName = "ic-broker";
    # }
    # Any URLs listed in OnChangePOST will receive a POST
    # with a form parameter of "broker" whenever the active
    # broker changes. CAS-protected URLs are supported.
    #
    # OnChangePOST = "http://smarts-tomcat-host-B:8080/smarts-edaa/setBroker";
   ```

3. Save the `failover.conf` file and exit.

   **Note** If you configure the Broker for failover while the Failover Manager is already running, use the ic-failover-server script reload option to reload the failover.conf file and use the Reconfigure button in the Domain Manager Administration Console to reconfigure the Failover Manager.

## Display the Failover Manager status of the Broker

Navigate to the `<BASEDIR>/smarts/script` directory and type the following command to view the status of the Broker:

```
ic-failover-server status
```
Optional additional configuration tasks for Broker failover

The following additional configuration tasks are available for manually configuring a Broker failover solution.

**Note**  The following configurations of the Load Balancer, the DNS system, or the High Availability solution are the responsibility of your system administrators as these configurations are external to the VMware Smart Assurance applications.

**Load Balancer**

You can choose to configure a Load Balancer in a failover scenario, where if the Active Broker fails, the Load Balancer will forward all traffic to the Standby Broker. The switchover is transparent to both you as well as the VMware Smart Assurance applications, because the same hostname or IP address is used to access the Broker.

**DNS**

If the Active host on which the Broker is running fails and cannot be restarted, edit the `/etc/hosts` file so that the DNS of the Active host that has failed, points to the IP address of the Standby host. The Failover Manager will recognize the DNS of the failed host and identify the IP address of the Standby host as running and start the Broker on the Standby host. The Failover Manager then synchronizes all the Active SAM and Domain Managers to the Broker.

The `/etc/hosts` file of each server (host) must be edited to avoid a downtime in Broker communication. You must ensure that any cache in the DNS is cleared so that all SAM and Domain Managers point to the Standby host.

Example:

An example of a `/etc/hosts` file is provided below:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1 localhost.loca!domain localhost
::1 localhost6.loca!domain6 localhost6
xx.x.xx.230 itops-tco-230.lss.emc.com itops-tco-230
xx.x.xx.227 itops-tco-227.lss.emc.com itops-tco-227
```

If the Broker running at itops-tco-227.lss.emc.com fails, edit the `etc/hosts` file as shown below:

```plaintext
# Do not remove the following line, or various programs # that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
xx.x.xx.230 itops-tco-230.lss.emc.com itops-tco-230
xx.x.xx.228 itops-tco-227.lss.emc.com itops-tco-227
```

After making the configuration changes, you must restart your network for the changes to take effect. Type the following command to restart your network:

```
/etc/rc.d/init.d/network restart
```

The following messages are displayed:

```
Shutting down interface eth0: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
```

**High Availability server**

As another possible solution, the Broker can be located on a server that has a High Availability (HA) hardware configuration to provide a more robust solution, whereby if the physical server where the Broker is located should go down, the HA server would become enabled. The switch-over would be transparent to both you as well as the VMware Smart Assurance applications as the same hostname and IP address of the server that has gone down would be used by the HA server.
Site Failover

This chapter includes the following topics:

- Overview
- Limitations

Overview

The Failover Manager supports a Site Failover or disaster-recovery (DR) scenario. In a site failover, components (all Domain Managers or all server hosts) on the active location or Location A fail. In this case, the Failover Manager switches the Domain Managers, including the Broker, to the standby location or Location B.

The Failover Manager performs the following operations when all Domain Managers or hosts on Location A fail:

- Switches the Broker to Location B.
- Updates the Broker to Location B on all Domain Managers at Location B.
- Switches all Domain Managers from Location A to Location B.

Following a failover for all components on Location A, the Failover Manager marks their roles as Standby and status as Down. If you restart the components on Location A, Failover Manager will determine their status as Up and continue to mark them as Standby. Synchronizations between the Domain Manager pairs will run from Location B to Location A. If you wish to failback to Location A, it is a manual task.
Figure 12-1. Site failover

Limitations

A Site Failover scenario can have the following limitations:

- If you had consoles attached to any of the Domain Managers on Location A while they were active, you have to reattach to the consoles via the Broker on Location B after the failover finishes.

- To change the BROKER parameter and point it to the current active Broker, you must modify the ic-failover-server script.

- For the SAM server with Notification Cache Publishing, if the Active site fails, user intervention is required to reconfigure the SolutionPack for VMware Smart Assurance to point to the Broker on the Standby site. In the SolutionPack, the Failover Manager updates the new EDAA details in the Report Section automatically. In the Data Collection and Events sections, you need to manually update the new Broker details.

This may depend on the version of VMware M&R as described in Failover of UI services is supported with Service Assurance Manager (SAM) 9.4 and VMware M&R 6.5u1.
Failover Manager

This chapter includes the following topics:
- Failover Manager
- Validation
- Broker registration
- Polling monitored Domain Managers
- Periodic Backup
- Configure the Failover Manager
- Other administrator tasks

**Failover Manager**

The Failover Manager monitors the operational state of the various VMware Smart Assurance components such as Broker, Trap Adapters, Trap Exploder, and the Active and Standby SAM, IP Manager, MPLS, Server Manager, NPM, VoIP Availability Manager, BIM, and Adapter Platform. When the Failover Manager detects that a failure of an Active component has occurred, it initiates a failover. The Failover Manager periodically takes a backup of the repository (RPS) and local files from the Active component to the Standby component.

If the Failover Manager monitoring process exits for some reason, you must restart Failover Manager manually. If the Failover Manager fails, you are notified as follows:

- If the Failover Manager is connected to a Global Console when the Failover Manager fails, you are notified by a pop-up message stating that Failover Manager is disconnected.

- If the Failover Manager is not connected to a console, the Failover Manager will be underlying to a Service Assurance Manager and the Domain Disconnected notification appears in the Notification Log Console.
Validation

The Failover Manager validates the product software versions and the command-line string used to start the component.

- **Version validation:** The Failover Manager checks the version of each of the products you have specified. If any component is found to be below version 9.1, it will be unmanaged and the component will not be monitored. If versions of either of the peers do not match both the Location A and Location B, the components specified in the failover.conf file for the Failover Manager will be unmanaged.

- **Command-line string validation:** The Failover Manager expects the EMC Smarts services for components that participate in a failover deployment to be started by specifying some options explicitly, which include the following:
  - For all components except the Broker: --noregister and --port (-p) option
  - For Trap Adapter and Trap Exploder (TRAPE/TRAPD): --sport (-P) option along with the ones needed for all components

  If the components are not started by specifying these options, the components for both locations will be unmanaged on the Failover Manager.

  For more information, consult Manage and Unmanage topology objects.

Broker registration

All components (SAM and Domain Managers) are started using the --noregister option. This ensures that the components are not registered with the Broker until the Failover Manager assigns the Active and Standby roles to the components. The Failover Manager then registers all the Active components with the Broker.

Polling monitored Domain Managers

The Failover Manager polls all configured SAM and Domain Managers and the systems on which they are running to determine their status.

Accept the default polling settings. If you modify default polling settings, you need to consider the size of your topology. For example, if the topology of the IP Manager or the Server Manager is large, you need to set the polling interval to a higher value. This is because the Managers can be unresponsive for a short duration while repository restore or reconfigure is in progress.

Monitored entities include the following:

- **Hosts:** The systems on which the services are configured. Hosts are monitored using ICMP pings
- **Broker s:** Broker services
- **Services:** All Domain Managers
Default polling groups

Use the Polling and Thresholds Console attached to the Failover Manager to view the default polling groups. The Failover Manager provides the following default polling groups:

- Broker Groups
  - Brokers
- Host Groups
  - Hosts
- Service Groups
  - IP Manager Domains
  - SAM Domains
  - MPLS Domains
  - ESM Domains
  - NPM Domains
  - VoIP Domains
  - Other Domains

Polling group target class and matching criteria lists the default polling groups and the associated target class and matching criterion and default setting for each group.

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Default settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brokers</td>
<td>InChargeBroker with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name = Broker*</td>
<td></td>
</tr>
<tr>
<td>Hosts</td>
<td>Host with attributes</td>
<td>Host Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td>IP Manager Domains</td>
<td>InChargeService with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServerType = AM</td>
<td>PM</td>
</tr>
<tr>
<td>SAM Domains</td>
<td>InChargeService with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServerType = SAM</td>
<td>OI</td>
</tr>
<tr>
<td>MPLS Domains</td>
<td>InChargeService with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServerType = MPLS</td>
<td></td>
</tr>
<tr>
<td>ESM Domains</td>
<td>InChargeService with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td>IsManaged = TRUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServerType = ESM</td>
<td></td>
</tr>
</tbody>
</table>
### Table 13-1. Polling group target class and matching criteria (Continued)

<table>
<thead>
<tr>
<th>Polling group</th>
<th>Target class and matching criteria</th>
<th>Default settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPM Domains</td>
<td><code>InChargeService</code> with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td><code>IsManaged = TRUE</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ServerType = NPM</code></td>
<td></td>
</tr>
<tr>
<td>VoIP Domains</td>
<td><code>InChargeService</code> with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td><code>IsManaged = TRUE</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ServerType = VoIP</code></td>
<td></td>
</tr>
<tr>
<td>Other Domains</td>
<td><code>InChargeService</code> with attributes</td>
<td>Service Connectivity Polling</td>
</tr>
<tr>
<td></td>
<td><code>IsManaged = TRUE</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**  The Other Domains polling group has the lowest priority. Managed services that do not match the criteria for the other groups become members of the Other Domains polling group. Only configured services in `failover.conf` that match the type and attribute values in the “target class and matching criteria” column for a particular group can become members of that group.

### Polling settings

**Polling settings and type** lists the polling settings and type.

#### Table 13-2. Polling settings and type

<table>
<thead>
<tr>
<th>Polling setting</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Connectivity Polling</td>
<td>Availability monitoring for Hosts</td>
</tr>
<tr>
<td>Service Connectivity Polling</td>
<td>Availability monitoring for Services</td>
</tr>
</tbody>
</table>

**Note**  Host connectivity polling is applicable to the Hosts group only and Service connectivity polling is applicable to the Brokers and Services groups.

### Host Connectivity Polling Parameters

**Host connectivity polling parameters** provides a description of the host connectivity polling parameters.

#### Table 13-3. Host connectivity polling parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>Enable or disable analysis. Instrumentation is not created and no polling is performed if analysis is disabled.</td>
<td>ENABLED, DISABLED Default: ENABLED</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>Time interval between successive polls.</td>
<td>30 to 3600 seconds Default: 120 seconds</td>
</tr>
</tbody>
</table>
Table 13-3. Host connectivity polling parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
</table>
| Retries   | Number of retry polls to perform when the initial poll fails. | 0 to 10 retries  
Default: 3 |
| Timeout   | Amount of time to wait for the poll response before the first poll request times out. | 10 to 10000 milliseconds  
Default: 700 milliseconds |

Service Connectivity Polling Parameters

Service connectivity polling parameters provides a description of the service connectivity polling parameters.

Table 13-4. Service connectivity polling parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible values</th>
</tr>
</thead>
</table>
| AnalysisMode  | Enable or disable analysis. Instrumentation is not created and no polling is performed if analysis is disabled. | ENABLED, DISABLED                  
Default: ENABLED |
| PollingInterval | Time interval between successive polls. | 30 to 3600 seconds                  
Default: 120 seconds |
| Retries       | Number of retry polls to perform when the initial poll fails. | 0 to 10 retries  
Default: 3 |
| Timeout       | Amount of time to wait for the poll response before the first poll request times out. | 10 to 10000 milliseconds  
Default: 700 milliseconds |

Periodic Backup

The Failover Manager performs the backup of repository (RPS) and local files periodically from Active host to Standby host based on the value specified for the **BackupInterval** parameter in the failover.conf file.
Also, you can perform a manual backup action as described in **Initiate manual backup, failback, and reload**.

**Note** If you are running the Failover Manager from your Standby SAM installation, and you customize any files in the following directories for use by Failover Manager, the changes should be present on both the Active and Standby SAM hosts. The affected directories are local/actions, local/model, local/rules, and local/script. Placing copies of Failover Manager files in both Active and Standby locations ensures that the Standby files will not be overwritten when Failover Manager performs backups.

The brokerConnect.conf, clientConnect.conf, serverConnect.conf, runcmd_env.sh, and imk.dat files do not get copied between locations as part of the backup. These special files should not be copied between Active and Standby hosts. If any maintenance is needed for these files, you need manually modify the file on both hosts as described in **Update special installation files manually**.

The Failover Manager copies the following directories from the SM_SITEMOD location of the Active host to the SM_SITEMOD location of the Standby host:

- The /rules, /actions, /script, and /model directories under the /local directory
- The conf/icf, conf/trapd, conf/beacon, conf/asm-ntier, conf/audit-parse, conf/serverhealth, conf/icim-core, conf/maps, conf/notifier, conf/alcatel-sam, conf/discovery, conf/devstat, conf/health
- The conf/mpls-tma, conf/mpls-a, conf/mpls-m, conf/mpls-t, conf/vpn-tagging

Repository files are not copied for SAM and Adapter Platform, but the repository files for BIM, IP Manager, NPM, MPLS, Server Manager, and VoIP Availability Manager are copied. The name of the copied repository file is `<domain-name>.latest.rps` in the Standby host.

If the directory is not present in the Active host, Failover Manager writes an error in the action log file and continues to do further backup. If the directory is not present in the Standby host, it creates that directory before copying the content.

Backup actions will be suspended during discovery in the Active host and also during the saving of the repository file in the Active host.

The StrictSitemod parameter mentioned in the failover.conf file controls strict validation of the paths of SM_SITEMOD and SM_WRITEABLE directories on the Active and Standby hosts. The default value of this parameter is `TRUE`.

When `StrictSitemod` is set to `TRUE`,

- The paths of SM_SITEMOD directories and SM_WRITEABLE directory on the Active host are verified with the paths on the Standby host.
- If the path of a directory matches, files from the directory location on the Active host are copied to the same location on the Standby host.
- If the path of a directory does not match, the directory is ignored and files from the other directories whose path matches are copied from Active to Standby host.
- If there are multiple SM_SITEMOD directories and none of the paths match, the backup action fails.
- If the path of the SM_WRITEABLE directory does not match, the backup action fails.
  
  When StrictSitemod is set to FALSE,

- The paths of SM_SITEMOD directories and SM_WRITEABLE directory are not verified.

- Files from the default SM_SITEMOD directory at <BASEDIR>/local on the Active host are copied to the same location on the Standby host.

  **Note**  The SM_SITEMOD directories that you have defined are not copied from Active to Standby host.

- The RPS files from the SM_WRITEABLE directory on the Active host are copied to the SM_WRITEABLE directory located anywhere on the Standby host.

  In general, when a new device is discovered in the topology, it is automatically saved to the topology. In this case, you need not manually save the topology. However, you need to manually save the topology in the following scenarios:

- You make some changes in Polling and Thresholds, and then do a manual reconfigure.

- You have managed or unmanaged a device or carried out some other changes.

  Manually saving the topology enables the backup script in failover to transfer the updated topology with minimum or no delta. The backup script is invoked after the specified time interval is exceeded (BackupInterval parameter value) and after every topology save.

  **Note**  If the topology is empty or you have started a new component, then during the backup action for failover, an error message is displayed in the log. However, this message will not be displayed during the next backup action as soon as you discover the topology.

### Configure the Failover Manager

This section describes how to configure the Failover Manager.

1. Configure the ic-failover-server script
2. Configure Domain Managers 9.3 or earlier for the failover backup if necessary
3. Configure the failover.conf file
4. Configure authentication credentials for Failover Manager if you are using SAM with Notification Cache Publishing Enabled
5. Install the Failover Manager service
6. Copy Failover Manager-specific files
7. Start the Failover Manager
8. Display failover status
9. Configure the Failover Manager as a source for SAM
Configure the ic-failover-server script

The ic-failover-server script is located in the /script directory. The Failover Manager uses the values specified in this script when it copies files from the Active component to the Standby component. Also, this script is used for failback actions (manual failover) and manual backups.

A copy of the ic-failover-server script must reside in both the Active and Standby locations:

- For Failover Manager running on a separate dedicated host with an EMC Smarts product installed, modify the ic-failover-server script.
- For Failover Manager running on a Standby host, modify the ic-failover-server script and copy it to the corresponding Active <BASEDIR>/smarts/local/script directory (for example, <BASEDIR>/SAM/smarts/script).

A modified script in both Active and Standby locations ensures that the Standby copy of the script will not be overwritten when Failover Manager synchronizes files.

To configure the ic-failover-server script:

a. From the FAILOVER_BASEDIR/smarts/bin directory, type the following command:

   ```bash
   ./sm_edit script/ic-failover-server
   ```

b. Press Enter.

c. Update the parameters as necessary based on the values you selected at system installation. Ignore the comment in the script about moving it to the /etc/init.d directory. ic-failover-server parameters describes the ic-failover-server parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SM_HOME** | Is the directory where Failover Manager resides. For example on Linux: /opt/InCharge/SAM/smarts  
For Windows, the SM_HOME default value can be: C:/InCharge/SAM/smarts |
| **DMNAME** | Is the name of the Failover Manager. The default: INCHARGE-FAILOVER  
For example:  
DMNAME=FAILOVER |
### Table 13-5. ic-failover-server parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMPORT</td>
<td>Is the TCP port on which Failover Manager is listening.</td>
</tr>
</tbody>
</table>
| BROKER    | Is the host where the Broker resides and the host port. The default: localhost:426 For Linux, specify a port value greater than 1024. The Failover Manager uses a non-root user account when restarting the Broker, so privileged ports (below 1024) cannot be used. For Windows, this restriction is not applicable. Failover Manager on Windows cannot be configured with a non-administrator user account to perform failover actions. For multiple Brokers, list those Brokers that are defined in the failover.conf file. For example: 

```
BROKER=--broker=smartslin02:1426,smartslin04:1426
```

1. Save and close the file. The modified version of the ic-failover-server script is saved to the FAILOVER_BASEDIR/smarts/local/script directory.

2. If the Failover Manager is running on a Standby host (and not a dedicated host), copy the modified ic-failover-server script from the Standby location to the corresponding Active <BASEDIR>/smarts/local/script directory.

### Syntax for the ic-failover-server script

The ic-failover-server script is located in the `<BASEDIR>/smarts/local/script directory. The syntax is:

```
ic-failover-server [options... ]
```

Options are provided in Syntax options for the ic-failover-server script.

### Table 13-6. Syntax options for the ic-failover-server script

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reloads the failover.conf file on the Failover Manager.</td>
</tr>
<tr>
<td>activate &lt;domain_name&gt;&lt;A</td>
<td>B&gt;</td>
</tr>
<tr>
<td>activate &lt;broker_name&gt;</td>
<td>The Broker will be activated to take the primary role.</td>
</tr>
<tr>
<td>status</td>
<td>Shows the status output of monitored services and hosts.</td>
</tr>
<tr>
<td>backup -s &lt;domain_name&gt;&lt;A</td>
<td>B&gt;</td>
</tr>
<tr>
<td>backup -h &lt;host_name&gt;</td>
<td>All active VMware Smart Assurance Managers running on this host will be scheduled for backup.</td>
</tr>
<tr>
<td>backup -all</td>
<td>All active components managed by the Failover Manager will be scheduled for backup.</td>
</tr>
</tbody>
</table>
Configure Domain Managers 9.3 or earlier for the failover backup

If your deployment includes Domain Managers Version 9.3 or earlier, you need to perform an extra task to configure the failover backup process.

Both backup methods, periodic (automatic) backup and manual backup that uses the ic-failover-server script, do not work if the failover is started from the 9.4 installation directory and the Domain Managers are Version 9.3 or earlier.

Also, for the backup process to work properly, the Failover Manager and Domain Managers need to run on the same platform. For example, Failover Manager on Linux and Domain Managers on Windows is not supported.

The extra task involves copying the recursive.pm Perl module from the 9.4 SAM installation where Failover Manager resides to the 9.3 installations for Active and Standby Domain Managers.

1. In the 9.3 installations for Active and Standby Domain Managers, create a Copy folder:

```
<BASEDIR>/smarts/toolbox/perl/lib/5.16.2/File/Copy
```

2. Locate the recursive.pm module in the 9.4 SAM installation where Failover Manager resides. The directory is:

```
<BASEDIR>/smarts/toolbox/perl/lib/5.16.2/File/Copy
```

3. Copy the recursive.pm module from the 9.4 location into the 9.3 location.

   For example, on Linux, copy the module to the 9.3 IP Manager location:

```
/opt/InCharge/IP/smarts/toolbox/perl/lib/5.16.2/File/Copy
```

```
C:\InCharge\IP\smarts\toolbox\perl\lib\5.16.2\File\Copy
```

Configure the failover.conf file

The failover.conf file implements Failover Manager configuration. The file is located in the BASEDIR/smarts/conf/failover directory.

Add entries for your deployment to the failover.conf file before starting the Failover Manager. Also, the sm_configureFailover.pl script uses the entries from this file to create subscriptions for Service Assurance Manager, Adapter Platform, and BIM.

If you modify the failover.conf file while the Failover Manager is already running, you must reload it in the Failover Manager. Initiate Failover Manager reload describes how to reload the Failover Manager.

The failover.conf file contains these sections:

- Root and non-root user sections (Linux)
- SettingSection
- BrokerSection
To configure the Failover Manager for your failover solution:

a. From the installation directory of Failover Manager (BASEDIR/smarts/bin), open the failover.conf file. Type:

```bash
./sm_edit conf/failover/failover.conf
```

b. Press **Enter**.

Configure the failover.conf file lists the specific product sections that provide examples of entries for the failover.conf file.

### Root and non-root user sections (Linux)

The Root and Non-Root User sections contain parameters for a non-root user. This ensures that the root process executes commands for non-root user. Also, it specifies the location of the security key.

Remove the pound sign (#) character to enable TransferCmd and RemoteLogin parameters for the non-root user and revise them as follows:

```bash
## If User is root:
#    TransferCmd = "/usr/bin/scp";
#    RemoteLogin = "/usr/bin/ssh";
## If User is non-root:
#    TransferCmd = "/usr/bin/scp -i /home/smartsusr/.ssh/id_rsa";
#    RemoteLogin = "/usr/bin/ssh -i /home/smartsusr/.ssh/id_rsa";
```

By Default the root and non-root user section is commented. It needs to be uncommented to use Failover as a non-root user.

```bash
## If a non-root user is specified, the RemoteLogin and TransferCmd options also need to be changed.
#    User = "root";
TransferCmd = "/usr/bin/scp -p -i /home/smartsusr/.ssh/id_rsa";
RemoteLogin = "/usr/bin/ssh -i /home/smartsusr/.ssh/id_rsa";
User = "smartsusr";
## ActionLogging = false;
```

### SettingSection

The SettingSection contains parameters that globally apply to all monitored components. Entries for email are mandatory since the Failover Manager is designed to send email to administrators when changes occur in the monitored systems.

The email parameters are:

- **MailSender**
- **MailRecipient**
- MailServer (the name of SMTP server to which email messages are sent)

- MailLevel—Controls the amount of email notifications that the Failover Manager sends. Possible values are:
  - ALL—All messages. This is the default value.
  - ERROR—Error messages only.
  - NONE—Disable all messages.

  The other parameters listed in this section are optional. If they are not specified, Failover Manager uses their default values.

- TransferCmd—Provides the path to the scp executable. For Linux, the default is "/usr/bin/scp" and for Windows, the default is "C:/Windows/System32/xcopy.exe".

- RemoteLogin—Provides the path to the ssh executable. For Linux, the default is "/usr/bin/ssh" and for Windows, the default is "C:/Windows/System32/WindowsPowerShell/v1.0/powershell".

- FailoverRetries—Is the maximum number of retries after an unsuccessfully attempt. The default is: 5

- FailoverRetryInterval—Is the time between a failed failover and the next attempt to retry. The default is: 300 seconds

- BackupInterval—Is the interval at which the current active configuration or data will be propagated to the Standby component. Some configuration changes may need additional steps (for example, restarting the Domain Manager, loading a configuration file through sm_tpmgr, and so on) to be fully picked up by the secondary component. The default is: 1800 seconds

  VMware recommends that VMware Smart Assurance administrators make every attempt to keep the Active and Standby components synchronized and, if necessary, apply manual commands to both components.

  If BackupInterval is set below 1800 seconds, the Failover Manager prints an error in the Domain Manager log file and uses a default value of 1800 seconds.

  **Note** If the component is running a discovery or saving the repository, the action of backing up the repository (RPS) file will be skipped.

- StrictSitemod—Indicates strict validation of the paths of SM_SITEMOD and SM_WRITEABLE directories for copying the failover files from the Active to Standby component. The default is: true

  For more information on StrictSitemod, refer to Periodic Backup.

- User—Defines the username that is used in remote access operations, such as scp, if different than the user that started the Failover Manager. The value is the non-root account to be used by Failover Manager for passwordless communication (for example, smartsusr ). The default is: " "
BrokerSection

The BrokerSection contains parameters that apply to the Broker.

- **ActionLogging**—If true, actions are logged to the `<failover_manager>.actions.log`. The default is: false
  The BASEDIR/smarts/local/logs/<failover_manager>.actions.log file is generated after you reload the failover.conf and if you reconfigure the Failover Manager using the Domain Manager Administration Console.
- **Debug**—If true, activates the debug mode in the Failover Manager. The default is: false
- **Verbose**—If true, prints changes in the Failover Manager. The default is: true
- **HostName**—Is the fully qualified hostname or IP address of the host where the Broker is running. For Windows, specify the Fully Qualified Domain Name (FQDN) for the host.
- **PortNumber**—Is the port where the host is running.

**Note** On Linux, the sm_service install --port value for the Broker must be changed to values greater than 1024. The Failover Manager uses a non-root user account when restarting these components, so privileged ports (below 1024) cannot be used. For Windows, this restriction is not applicable. Failover Manager on Windows cannot be configured with a non-administrator user account to perform failover actions.

- **Basedir**—Is the directory path where the Broker is installed.
- **InstalledServiceName**—Is the VMware Smart Assurance service name as specified in the sm_service install command for the Broker. The default is: ic-broker.
- **OnChangePOST**—Defines the URLs for the EMC Data Access API (smarts-edaa). For the SAM server with Notification Cache Publishing, when the Active Broker fails, the Failover Manager uses this value to set the new Broker location in the EMC Data Access API.

Here is an example of the parameters for multiple Brokers including OnChangePOST. The first entry for Host A is treated as the Active Broker:

```yaml
BrokerSection
{
  Broker
  {
    HostName   = "broker-host-A";
    PortNumber = 1751;
    Basedir    = "/opt/InCharge/SAM/smarts";
    InstalledServiceName = "ic-broker";
  }
  Broker
  {
    HostName   = "broker-host-B";
    PortNumber = 1751;
    Basedir    = "/opt/InCharge/SAM/smarts";
    InstalledServiceName = "ic-broker";
  }
}```
ServerSection

The ServerSection defines the components of the failover solution. The ServerSection contains mandatory parameters.

- **Name**—The VMware Smart Assurance product name (example: INCHARGE-SA). [Values for the Name parameter](#) provides a list of product names.

- **UIServices**—Required for a SAM with Notification Cache Publishing. Specify the services for VMware Smart Assurance Data Web Applications (smarts-tomcat), VMware Smart Assurance Notification Exchange (smarts-rabbitmq), and VMware Smart Assurance Notification Cache (smarts-elasticsearch).

  Configure Hostname, PortNumber, Basedir, and InstalledServiceName for each pair of Active and Standby components in the LocationA and LocationB entries, respectively:

  - **Hostname**—Is the fully qualified hostname or IP address of the host where the component is running. For Linux, the value must exactly match the name displayed when you run the Linux hostname command. For Windows, specify the Fully Qualified Domain Name (FQDN) for the host.

  - **PortNumber**—Is the port where the component is running. For Trap Exploder, the PortNumber value must match the --sport value in the sm_service install command.

  - **Basedir**—Is the directory path where the component is installed.

  - **InstalledServiceName**—Is the service name of the Trap Exploder (ic-trapd-exploder) or the VoIP Trap Adapter (ic-voip-notification-trapd-receiver). Failover Manager uses this value to start the component as a service. Trap Exploder, VoIP Trap Adapter, and the Broker (specified in the BrokerSection) are the only components that Failover Manager restarts. Specifying this parameter for other components has no effect since the Failover Manager does not restart them.

The following parameters are optional:

- **ServerType**—Is the type of component or Domain Manager. [ServerType](#) provides a list of ServerType values.

- **DetachInterval**—[DetachInterval](#) provides detailed information about when to specify this parameter.

In the entry, once you specify the value of the Name parameter, you need to provide specific information for Active and Standby (sibling) components within the two separate subsections: LocationA and LocationB.
LocationA and LocationB are two segments in a given network environment. Each contains a set of hosts on which Active and/or Standby VMware Smart Assurance products run.

An example is provided for defining the parameters for SAM:

```plaintext
ServerSection
{
 Server
 {
 DetachInterval = 300;
 Name= "INCHARGE-SA";
 ServerType= "SAM";
 # UIServices = "smarts-tomcat,smarts-rabbitmq, smarts-elasticsearch";
 DetachInterval=300;
 LocationA
 {
 HostName = "<host-A>";
 PortNumber= 2611;
 Basedir= "/opt/InCharge/SAM";
 }
 LocationB
 {
 HostName = "<host-B>";
 PortNumber = 2622;
 Basedir = /opt/InCharge/SAM
 }
 }
}
```

Configure ServerSection for each VMware Smart Assurance component lists the VMware Smart Assurance components and their entry examples for the ServerSection.

**Table 13-7. Configure ServerSection for each VMware Smart Assurance component**

<table>
<thead>
<tr>
<th>Component</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broker</td>
<td>Add the Broker to the Failover Manager</td>
</tr>
<tr>
<td>SAM, Adapter Platform, and BIM</td>
<td>Configure the failover.conf file for SAM, Adapter Platform, and BIM</td>
</tr>
<tr>
<td>IP Manager</td>
<td>Add IP Managers to the Failover Manager</td>
</tr>
<tr>
<td>MPLS Manager</td>
<td>Add the MPLS Manager to the Failover Manager</td>
</tr>
<tr>
<td>Server Manager (ESM)</td>
<td>Add the Server Manager to the Failover Manager</td>
</tr>
<tr>
<td>NPM</td>
<td>Add Network Protocol Manager to the Failover Manager</td>
</tr>
<tr>
<td>VoIP Availability Manager</td>
<td>Add VoIP Availability Manager and VoIP Trap Adapter to the Failover Manager</td>
</tr>
<tr>
<td>Trap Adapter</td>
<td>Add the Trap Adapter to the Failover Manager</td>
</tr>
<tr>
<td>Trap Exploder</td>
<td>Add the Trap Exploder to the Failover Manager</td>
</tr>
</tbody>
</table>

Values for the Name parameter

The Name parameter must match the name of the Global Manager, the Domain Manager, Trap Adapter, or Trap Exploder. The value of the Name parameter is not limited to the following default values:
SAM: INCHARGE-SA, INCHARGE-SA-PRES, or INCHARGE-SA-AGG

Adapter Platform: INCHARGE-OI

Business Impact Manager: INCHARGE-MBIM

IP: INCHARGE-AM

ESM: INCHARGE-ESM

MPLS: INCHARGE-MPLS-TOPOLOGY, INCHARGE-MPLS-MONITORING or INCHARGE-MPLS-ANALYSIS

NPM: INCHARGE-BGP, INCHARGE-EIGRP, INCHARGE-ISIS, or INCHARGE-OSPF

Trap Adapter: TRAP-INCHARGE-OI

Trap Exploder: TRAP-INCHARGE-Exploder

VoIP: VoIP-AM or TRAP-INCHARGE-VOIP

ServerType

The ServerType parameter is optional and defines the type of component being monitored. The default for this parameter is OTHER. The values supported for this parameter include:

- AM
- AMPM
- PM
- ESM
- MPLS
- NPM
- VoIP
- OI
- OTHER
- SAM
- BIM
- TRAPD
- TRAPE

DetachInterval

DetachInterval is an optional parameter that is applicable to SAM, Adapter Platform, BIM, and all Domain Managers.

DetachInterval in a warm failover
In case of a warm failover (Business Impact Manager, IP Manager, MPLS Manager, Network Protocol Manager, Server Manager, and VoIP Availability Manager), the DetachInterval determines how long the Active SAM server will wait before starting topology synchronization with the newly-promoted Active Domain Manager. This way, the previously Standby Domain Manager is allowed to settle in after initiating network monitoring. Both initiating network monitoring and topology synchronization with SAM are resource intensive operations, so the DetachInterval ensures that they do not happen at the same time. The default DetachInterval for Domain Managers is 300 seconds, except for IP Managers, the value is 480.

DetachInterval in a hot failover

In case of a hot failover (SAM and Adapter Platform), use the DetachInterval parameter to avoid the creation of orphaned events. This parameter controls the number of minutes between the enabling of the underlying Domain Managers and detaching the peer component during a failover. The default DetachInterval for SAM and Adapter Platform is 300 seconds.

Orphaned events are discarded, which should be avoided since the events the peer knows about, came from the recently enabled underlying Domain Managers. EMC recommends waiting for the synchronization of the underlying Managers to complete so that when the peer is removed as a source, the events do not become orphans.

After the specified interval, the Standby component deletes its Active sibling from its repository after a failover occurs and the roles of the components switch. The Standby component no longer needs to obtain its data from the failed component, since it is itself connected to the underlying Domain Managers after the failover.

The interval should allow enough time for the Standby component to synchronize its topology and event data directly from the underlying Domain Manager before deleting the sibling component. Therefore, it does not allow any window where data may be missing in the newly Active component.

Although the newly Active component will stabilize its data eventually, as smooth a transition as possible is imperative. Especially, in case of a too short detach interval, clearing and re-notifying existing notification will result in re-occurrences of notifications and may cause opening new tickets.

For example, when a connection from the Standby SAM to Active SAM is disabled and the Standby SAM becomes Active, the topology that came from the old Active SAM will be removed from the new Active SAM. This is why it is important that the new Active SAM establishes connections and completes synchronization with underlying analysis Domain Managers so that:

- The old Active SAM is not the only source on notifications and topology in the new active SAM.
- There is no premature notifications clearing and topology removal.

  The notifications and topology will stay in the new Active SAM, but the notification source and topology domain management will no longer list the old Active SAM. Instead, it will only list the source analysis Domain Managers.

  The Active component is one that participates in the connection set within the current deployment. Connections may be established between:
The VMware Smart Assurance Managers (Service Assurance Manager to Service Assurance Manager, Service Assurance Manager to Adapter Platform, Service Assurance Manager to IP Availability Manager, so on).

Or, between clients and the server, mainly the Global Console and the top-level Service Assurance Manager.

A hot Standby component, on the other hand, synchronizes with the Active component and no other servers or clients are connected to it (unless required for some maintenance purpose).

**Note** Failover script files located in `<BASEDIR>/smarts/actions` and `<BASEDIR/smarts/rules` directories must not be modified.

### MNRSection

For SAM server with Notification Cache Publishing that is configured in the SolutionPack for VMware Smart Assurance for use with the VMware M&R UI, you need to uncomment the MNRSection and specify information for those parameters. The Failover Manager uses this information to set the Active EDAA and Active Broker in the SolutionPack for VMware Smart Assurance.

The parameters are:

- **MNRHost**—Is the VMware M&R Frontend server (tomcat) host.
- **MNRPor**—Is the VMware M&R Frontend server (tomcat) port.
- **MNRPor**—Is the VMware M&R Frontend server (tomcat) protocol.
- **GatewayHost**—Is the VMware M&R web-service gateway host.
- **GatewayPort**—Is the VMware M&R web-service gateway port.
- **GatewayProtocol**—Is the VMware M&R web-service gateway protocol.

In case you have multiple SolutionPack instances, specify the SolutionPack that contains the Reports SolutionPack block.

For each SolutionPack block (Reports, Events, Data collection) specify the values exactly how they appear in the Centralized Management page in the VMware M&R UI. To locate and copy the values, navigate to the SolutionPacks page. (Log in to the VMware UI and type `http://<Frontend IP address>:58080/centralized-management`. Click SolutionPacks and then click VMware Smart Assurance to locate the information.)

- **Component**—Is the component. For example: Reports, Events, Data collection.
- **ComponentVersion**—Is the component version.
- **SPInstance**—Is the SolutionPack instance. For example: emc-smarts
- **SPVersion**—Is the SolutionPack version.
- **SPServer**—Is the SolutionPack server distribution.

If you have upgraded VMware M&R, check the version information after the upgrade. You might need to update version information in the MNRSSection of the failover.conf file.

For example:

```plaintext
MNRSection
{
  MNRHost = "smartslin03.emc.com";
  MNRPort = 58080;
  MNRProtocol = "http";
  GatewayHost = "smartslin03.emc.com";
  GatewayPort = 48443;
  GatewayProtocol = "https";
}

SolutionPackBlock
{
  Component = "Reports";
    ComponentVersion = "2.1.1";
    SPInstance = "emc-smarts";
    SPVersion = "2.1.1";
    SPServer = "smartslin02.emc.com";
}

SolutionPackBlock
{
  Component = "Events";
    ComponentVersion = "2.1.1";
    SPInstance = "emc-smarts";
    SPVersion = "2.1.1";
    SPServer = "smartslin02.emc.com";
}

SolutionPackBlock
{
  Component = "Data collection";
    ComponentVersion = "2.1.1";
    SPInstance = "emc-smarts";
    SPVersion = "2.1.1";
    SPServer = "smartslin02.emc.com";
}
}
```

**Configure authentication credentials for Failover Manager**

If you are using SAM with Notification Cache Publishing Enabled, you need to configure credentials to access VMware M&R in the clientConnect.conf file for Failover Manager.

1. Use `sm_edit` to open the `<BASEDIR>/smarts/conf/local/clientConnect.conf` file.
2 In the Webservices Access section, specify the credentials for the VMware M&R frontend (Tomcat) and VMware M&R Webservice Gateway.

```
#### Webservices Access ####
# Credentials to access MNR.
# This is used by Failover Manager.
# You should change the password!
*:http://*:58080/*:admin:<E-1.0>94441BB01A289C5DE162B2DF494915A8CDD0B0D64001066FD26CA40987554FCF

# Credentials to access MNR webservice-gateway.
# This is used by Failover Manager.
# You should change the password!
*:https://*:48443/*:admin:<E-1.0>94699AAE806A687113B3086DFE9B68CC438844A814F7846E5DA54D62ADA
```

3 In the Smarts EDAA Access section, specify the credentials for the EMC Data Access API (smarts-edaa). Replace the default password (changeme) with the Broker password.

```
#### SMARTS EDAA Access ####
# Credentials to access the smarts-edaa.
# This is used by the Failover Manager to update
# the broker location when the broker fails over.
# You should change the password!
*:http://*/smarts-edaa/*:admin:<E-1.0>94F1EEFCD82DA82E9838EE0B269334940F6F54CE3AC9FC49DA8AC723B4FA8E3

*:https://*/smarts-edaa/*:admin:<E-1.0>94080CD2DAE1065974DAC098DEEC2E37EFF267AF8A285C82ED98ACCAE84273B
```

4 Save the file and exit.

**Install the Failover Manager service**

After installing the VMware Smart Assurance products for the Failover solution, use the sm_service install command to create a Failover Manager service. The host system will automatically start the Failover Manager as a process running in the background each time that the system boots.

An example of a sm_service install command used to create a Failover Manager service is:

```
./sm_service install --force --unmanaged --startmode=runonce 
'--name=ic-failover-manager' 
'--InCharge/SAM/smarts/bin/sm_server' 
'--name=INCHARGE-FAILOVER' 
'--config=failover' 
'--norestore' 
'--output'
```

The *VMware Smart Assurance System Administration Guide* provides complete information about the sm_service command options.
Copy Failover Manager-specific files

If you are running the Failover Manager from your Standby SAM installation, and you customize any files in the following directories for use by Failover Manager, the changes should be present on both the Active and Standby SAM hosts. The affected directories are local/actions, local/model, local/rules, and local/script.

Before you start the Failover Manager, copy the ic-failover-server script described in Configure the ic-failover-server script and any other customized Failover Manager files to the corresponding directories in the Active and Standby locations.

Placing copies of Failover Manager files in both Active and Standby locations ensures that the Standby files will not be overwritten when Failover Manager synchronizes files.

Start the Failover Manager

Review the following prerequisites before starting the Failover Manager.

- The Failover Manager must be started with root privileges since the Failover Manager must be able to execute ICMP pings on the hosts that are monitored.
  
  For Windows, the failover service (ic-failover) needs to be started as an administrator service for PowerShell remoting to work. Normally, all EMC Smarts services start up with the Local System account which does not have PowerShell remoting access and this causes the failover service remote execution to fail in Windows. Setting up Administrator service for PowerShell remoting (Windows only) provides instructions.

- File permissions must be set to allow the copying of files from one host to another.

- The Failover solution uses secure copy and remote login programs. Appropriate network and host configurations must be in place for the solution to function. The requirement also includes non-prompting authentication settings whenever applicable, either with SCP or SSH commands or with VMware Smart Assurance programs, such as dmctl, sm_config, or others.

  For more information on setting up non-prompting authentication, refer to Set up passwordless communication between Active and Standby hosts.

  Start the Failover Manager only after all the components to be monitored are started and configured.

  After creating the Failover Manager service and assuming that you have yet to reboot the host machine, you can use the sm_service start command to start or stop the Failover Manager.

Setting up Administrator service for PowerShell remoting (Windows only)

For Windows only, the failover service (ic-failover) needs to be started as an administrator service for PowerShell remoting to work. Perform these additional steps before starting the failover service:

1. After configuring the Failover Manager service using the sm_service install command (Install the Failover Manager service), go to the Windows Services Management Console.

2. Click Start.
3 Type `services.msc` in the Search box and press **Enter**.

4 Right-click **EMC Smarts Failover Manager** and select **Properties**.

5 Click the **Log On** tab.

6 Select **This account**.

7 Fill in the account name to read: `<Machine-Name>\Administrator`  
   Where `<Machine-Name>` is the actual name of the machine.  
   Or, type: `.\Administrator` in the field.

8 Fill in the Administrator Password and Confirm Password fields.

9 Click **OK**.

**Starting the Failover Manager service**

For the purpose of this example, the name of the Failover Manager service is `ic-failover`.

**Linux**

To start the service on Linux:

1 Navigate to the FAILOVER_BASEDIR/smarts/bin directory.

2 Type the following command:

   ```
   ./sm_service start ic-failover
   ```

3 Press **Enter**.

**Windows**

To start the service from the Windows desktop:

1 Select **Start > Settings > Control Panel > Administrative Tools > Services**.

2 Right-click **EMC Smarts Failover**.

3 Select **Start**.

**Stopping the Failover Manager service**

**Linux**

1 Navigate to the FAILOVER_BASEDIR/smarts/bin directory.

2 Type the following command:

   ```
   ./sm_service stop ic-failover
   ```

3 Press **Enter**.
Windows

To start the service from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Right-click **EMC Smarts Failover**.
3. Select **Stop**.

Display failover status

To display the current failover status, use the `ic-failover-server` script:

1. From the `FAILOVER_BASEDIR/smarts/local/script` directory, type:

   ```bash
   ic-failover-server status
   ```

2. Press **Enter**.

A sample of the Failover status is:

```
[root@wpl-019-093 bin]# ./sm_adapter -s INCHARGE-FAILOVER ../rules/failover/failover-status.asl
Status of Monitored Entities on: INCHARGE-FAILOVER

|------- Process -------| P-Status |-|---- Role -----|----------- Host -----------|- H-Status -|
| INCHARGE-ESM-A ....... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-ESM-B ....... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| Broker0 .............. UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| TRAP-EXPLODER-A ...... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| TRAP-EXPLODER-B ...... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-SA-A ........ UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-SA-B ........ UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-PM-A ........ UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-PM-B ........ UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-OI-A ........ UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-OI-B ........ UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-AM-A ........ UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-AM-B ........ UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-AM-PM-A ..... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-AM-PM-B ..... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-EIGRP-A ..... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-EIGRP-B ..... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-OSPF-A ..... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-OSPF-B ..... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| Broker1 .............. UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-MPLS-TOPOLOGY-A UP......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-MPLS-TOPOLOGY-B UP......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-BGP-A ....... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-BGP-B ....... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| INCHARGE-ISIS-A ....... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| INCHARGE-ISIS-B ....... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| TRAP-INCHARGE-OI-A ... UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
| TRAP-INCHARGE-OI-B ... UP.......... ACTIVE......... wpl-019-093.lss.emc.com..... UP.......... |
| VoIP-AM-A ............ UP.......... STANDBY........ wpl-019-092.lss.emc.com..... UP.......... |
```
Configure the Failover Manager as a source for SAM

Configure the Failover Manager as a source for SAM and enable the viewing of the failover notifications in the Notification Log Console.

If your deployment includes a hierarchical SAM architecture, configure the Failover Manager as a source for the top-most SAM server.

Perform these steps:

1. In your Active SAM server, go to Global Manager Administration Console > ICS Configuration > IC Domain Configuration > Domains and select INCHARGE-FAILOVER. Enable this connection by clicking on the Enabled checkbox as displayed in Enabling INCHARGE-FAILOVER in SAM.

   ![Enabling INCHARGE-FAILOVER in SAM](image)

2. In your Standby SAM, ensure that INCHARGE-FAILOVER domain is disabled.

3. Go to Global Manager Administration Console > ICS Configuration > IC Domain Configuration > Domains and select the Standby INCHARGE-FAILOVER domain.
4 Select the Enabled checkbox to clear it and click Apply.

**Other administrator tasks**

This section describes other administrator tasks that you can perform on an as-needed basis.

- Display failover status
- Update special installation files manually
- Initiate manual backup, failback, and reload
- Connect the console to a Standby Domain Manager
- Manage and Unmanage topology objects
- Manual cleanup of unused files
- *Additional customizations with hook scripts on page 59*

**Update special installation files manually**

The brokerConnect.conf, clientConnect.conf, serverConnect.conf, runcmd_env.sh, and imk.dat files do not get copied between locations as part of the periodic (automatic) backup or the manual backup that uses the ic-failover-server script. These special files are generated as part of the installation process and should not be copied between Active and Standby hosts.

If any maintenance or modifications are needed for these files, you need manually modify each file on the Active and Standby hosts.

**Initiate manual backup, failback, and reload**

You can perform a manual backup, a failback, or a reload action using the ic-failover-server script.

- By setting **Manualbackup** to **TRUE** in the ic-failover-server script of an Active component, a manual backup of RPS and local files is taken from the Active host to the corresponding Standby host.

- A failback (or a manual failover) will switch the roles of Active and Standby hosts. You can perform a failback by setting the **TakeOver** parameter to **TRUE** in the ic-failover-server script.

- A manual reload will reload a modified failover.conf file.

  **Manualbackup** and **TakeOver** can also be set through the Global Console.

  Before you use the ic-failover-server script, modify it with the settings appropriate for your deployment in **Configure the ic-failover-server script**.

**Initiate manual backup**

Performing a manual backup does not affect the periodic backups. Periodic backups continue to happen as per their original scheduled interval, including for the component that is manually backed up.
The performance of Failover Manager will deteriorate while backing up a bigger topology. You may also see a delay in the polling suspension activity if the backup is happening while the component is coming up.

Use the ic-failover-server script to perform three different types of backup actions.

- To run an on-demand backup for a specific component, type the following command from the FAILOVER_BASEDIR/smarts/local/script directory and press Enter. Specify -A or -B depending on which side is active. This command sets the ManualBackup parameter to TRUE if the Active component is up and running.

  ```shell
  ic-failover-server backup -s <domain_name>-<A|-B>>
  Server INCHARGE-SA-B has been successfully scheduled for backup.
  ```

- To run an on-demand backup for all Active components on a specific host that Failover Manager monitors, type the following command from the FAILOVER_BASEDIR/smarts/local/script directory and press Enter.

  ```shell
  ic-failover-server backup -h <host_name>
  ```

- To run an on-demand backup for all Active components that Failover Manager monitors, type the following command from the FAILOVER_BASEDIR/smarts/local/script directory and press Enter.

  ```shell
  ic-failover-server backup -all
  ```

### Initiate failback (or manual failover) of SAM or a Domain Manager

You can use a failback action for the following situations:

- Consider that an Active component at Location A fails. The Failover Manager performs a failover and the Standby component at Location B is promoted as the Active component. When the component at Location A is running again, it is assigned the role of a Standby component. You can change the Standby role of the component at Location A to Active by performing a failback.

- Consider that maintenance is scheduled for the Active components at Location A. Use the ic-failover-server script to execute manual failover to promote the Standby components at Location B to be Active components for the maintenance period. After maintenance is completed, initiate a failback again to promote components in Location A as Active.

Use the ic-failover-server script to perform a failback action:

a  From the FAILOVER_BASEDIR/smarts/local/script directory, type the following command. Specify -A or -B depending on which side is active.

  ```shell
  ic-failover-server activate <domain_name>-<A|-B>>
  "Server INCHARGE-SA-B has been successfully scheduled for activation."
  ```
b Press Enter.

The Failover Manager executes the failover action to the specified EMC Smarts Manager and, as a result, that Manager will become Active.

c Stop and start the service of the previously Active Manager which is now a Standby Manager.

Initiate failback (or manual failover) of the Broker

You can switch the role of a Broker manually at any time using the failover utility script ic-failover-server. You can switch the Broker after the Failover Manager restarts a failed Broker or if the Broker needs to be manually switched to perform maintenance operations.

You can invoke a failback for a Broker as follows:

1 From the FAILOVER_BASEDIR/smarts/local/script directory, type:

```
ic-failover-server activate <broker>
[root@itops-tco-213 bin]# ../script/ic-failover-server activate Broker1
Server FAILOVER User: admin
admin's Password: XXXXXXXXXX
ic-failover-server: Server/Broker 'Broker1' has been successfully scheduled for activation.
```

2 Then, determine the status and roles of Domain Managers and Brokers as follows:

```
ic-failover-server status
[root@itops-tco-213 bin]# ../script/ic-failover-server status
Server FAILOVER User: admin
admin's Password: XXXXXXXXXX
Status of Monitored Entities on: FAILOVER
|------- Process ------|- P-Status -|---- Role -----|----------- Host -----------|- H-Status -|
Broker0 .............. UP.......... STANDBY........ itops-tco-212.lss.emc.com... UP........
Broker1 .............. UP.......... ACTIVE......... itops-tco-213.lss.emc.com... UP........
INCHARGE-AM-PM-A ..... UP.......... ACTIVE......... itops-tco-212.lss.emc.com... UP........
INCHARGE-AM-PM-B ..... UP.......... STANDBY........ itops-tco-213.lss.emc.com... UP........
INCHARGE-SA-A ........ UP.......... ACTIVE......... itops-tco-212.lss.emc.com... UP........
INCHARGE-SA-B ........ UP.......... STANDBY........ itops-tco-213.lss.emc.com... UP........
|---------------------|------------|---------------|----------------------------|----------|
P-Status: Process Status
H-Status: Host Status
```

Initiate Failover Manager reload

If you need to make a change to the failover.conf file, you do not need to restart the Failover Manager. The changes can be loaded in using ic-failover-server script.

1 From the FAILOVER_BASEDIR/smarts/local/script directory, type the following command:

```
ic-failover-server reload
```

2 Attach the Domain Manager Administration Console to the Failover Manager and select Reconfigure to reconfigure the Failover Manager.
Connect the console to a Standby Domain Manager

If necessary, you can attach the console to a Standby Domain Manager. Use the direct connection approach which does not require the Broker. Specify the following in the Manager Name field of the Attach Manager Dialog Box:

\[ \text{<FQDN_hostA>:<portA>/ServerName} \]

For example, specify: itops-tco-217.lss.emc.com:1751/INCHARGE-SA

Manage and Unmanage topology objects

The Failover Manager monitors managed InChargeService and Host objects, but not unmanaged objects. InChargeServices are the sm_server processes like SAM, IP, MPLS, ESM, NPM and VoIP domains, and Host objects are the servers on which these processes are running. The InChargeService and Host objects can be managed and unmanaged through the Domain Manager Administration Console.

The Failover Manager monitors a managed object for the purpose of determining the object’s status. An unmanaged object is not polled by the Failover Manager, but remains present in the modeled topology.

A managed object is an object whose IsManaged attribute has a value of TRUE. IsManaged is a Boolean attribute: TRUE when an object is managed and FALSE when an object is unmanaged.

The Manage and Unmanage options enable you to control whether an object is managed. Unmanaging a service or host might be useful when, for example, services or hosts need to be taken offline for maintenance.

Management state can be set for the following types of objects:

- Hosts
- Brokers
- InChargeServices

The function of Manage and Unmanage options is recursive. When you unmanage an object, all the other objects that are functionally dependent on that object become unmanaged. When you unmanage a Host, all the services (Brokers and InChargeServices) that belong to that Host will be unmanaged.

If you unmanage an InChargeService object, then that service will not be monitored. No scheduled backups will be performed and no failover will be performed when the domain fails. The status of the service will be marked as UNKNOWN.

The Failover Manager maintains the management state of objects even after it is restarted.

When you manage back an unmanaged object, a reconfiguration is required so that the polling settings can be applied back.
Setting the management state of individual objects

The management state of individual objects can be set by attaching the Domain Manager Administration Console to the Failover Manager and using the Manage and Unmanage options. To set the management state of an object:

1. Attach the Failover Manager to the Domain Manager Administration Console.
2. Select the InChargeServices or InChargeBrokers whose objects you want to manage or unmanage.
3. Right-click on a service or Broker and select:
   - Manage to poll the service so the Failover Manager will start monitoring this service.
   - Unmanage to stop polling the service so the Failover Manager stops monitoring the service.

Manual cleanup of unused files

The Failover Manager copies the contents of certain directories from the Active location to the Standby location. If a file is no longer needed, and it is deleted from the Active location, it will remain in the Standby installation area. Furthermore, if the component roles are switched, the file will show up on the original area again because of backup action by the failover. Although harmless, in time, the number of unused files may grow. Therefore, you must manually remove the unused files from both locations as needed.
Advanced techniques: Hook scripts and VMware M&R collectors

This chapter includes the following topics:

- Overview
- Additional customizations with hook scripts
- VMware M&R collector scenarios used with hook scripts
- Configure VMware M&R collectors for an VMware Smart Assurance failover

Overview

Failover Manager supports customer-defined hook scripts written in Perl. You can create hook scripts that perform actions at the beginning or the end of a failover process. You need to save them in the installation where Failover Manager resides. Conventions for creating hook scripts are described in Additional customizations with hook scripts.

One special use for a hook script is that it can starts another VMware M&R collector during a Domain Manager failover. For reports, graphics, and metrics visible in the VMware M&R User Interface, the hook script starts the collector near the Standby location to continue collecting data from the newly-promoted Domain Manager. Not all scenarios require multiple VMware M&R collectors.

VMware M&R collector scenarios used with hook scripts describes scenarios and Configure VMware M&R collectors for an VMware Smart Assurance failover describes how to configure the sample hook script that is provided for VMware M&R collectors.

Additional customizations with hook scripts

In addition to the tasks that Failover Manager performs automatically during a failover, you can use hook scripts to specify additional actions to occur at the beginning or the end of the failover process. For example, you can create a hook script to start or stop a smarts-collector associated with the Active Domain Manager.

Failover Manager supports customer-defined hook scripts written in Perl. The hook scripts run from the smarts/local/actions directory in the installation where Failover Manager resides. The hook scripts can connect to Active and Standby Service Assurance Managers and Domain Managers that are registered with the Broker.
Use Perl to create the scripts to run in the beginning or in the end of a failover. Save them in the FAILOVER_BASEDIR/smarts/local/actions directory. You can also associate the script with a server type or with a server name. The naming conventions are as follows:

- `failover_pre.pl`—Runs at the beginning of a failover of any component.
- `failover_post.pl`—Runs at the end of a failover of any component.
- `failover_pre_<SERVER_TYPE>.pl`—Runs at the beginning of a failover of any component with the specified type described in `ServerType`.
- `failover_post_<SERVER_TYPE>.pl`—Runs at the end of a failover of any component with the specified type.
- `failover_pre_<SERVER_NAME>.pl`—Runs at the beginning of a failover of the component with the specified name. Values for the Name parameter provides a list of default names.
- `failover_post_<SERVER_NAME>.pl`—Runs at the end of a failover of any component with the specified name.

Examples:

- `failover_post_<SERVER_TYPE>.pl` is `failover_post_SAM.pl` which will run at the end of any Service Assurance Manager failover.
- `failover_post_<SERVER_NAME>.pl` is `failover_post_INCHARGE-SA-PRES.pl` which will run at the end of a failover for the Service Assurance Manager named INCHARGE-SA-PRES.

The sample hook script `failover_post-AMPM-sample.pl` for VMware M&R collectors

The sample customer script `failover_post-AMPM-sample.pl` is provided in the smarts/local/actions directory in the installation where Failover Manager resides.

The script is the mechanism that starts another VMware M&R collector to communicate with the Standby Domain Manager that is promoted to Active.

Unlike other `failover_pre` and `failover_post` hook scripts, the `failover_post-AMPM-sample.pl` script is designed to work with only Domain Managers. It is named for the combined IP Availability and Performance Manager, but you rename and modify it in “Configure VMware M&R collectors for an VMware Smart Assurance failover” on page 59.

The `failover_post-AMPM-sample.pl` script does not work with Service Assurance Manager, Business Impact Manager, Adapter Platform, Trap Exploder or Trap Adapter, because the VMware M&R smarts-collector does not collect data from these components.
VMware M&R collector scenarios used with hook scripts

For SAM with Notification Cache Publishing Enabled which interacts with VMware M&R UI, several failover scenarios exist and not all of them require hook scripts for VMware M&R collectors. In the VMware M&R platform, the smarts-collector typically resides on a separate host and performs event and performance collecting from one or more Domain Managers.

The Failover Manager monitors the Domain Managers and does not monitor the collectors. You can configure the failover_post-AMPM-sample.pl hook script so that the script can stop the smarts-collector on a separate host and start another one near the newly-promoted Domain Manager.

Table 14-1. Scenarios for hook scripts for collectors

<table>
<thead>
<tr>
<th>Scenario or situation</th>
<th>Is configuring a hook script needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>If SAM with Notification Cache Publishing Enabled or any one of its services (Tomcat, Rabbit MQ, and Elasticsearch) fail, the Failover Manager performs the actions described in Active SAM failure scenario</td>
<td>Not applicable. Configuring a hook script to start VMware M&amp;R collectors is not applicable, because the collectors gather data from Domain Managers and not from Global Managers like Service Assurance Managers or Adapter Platform.</td>
</tr>
<tr>
<td>For a Site failover which includes the failure of VMware M&amp;R UI</td>
<td>VMware M&amp;R failover is not covered in this guide and it is a custom solution.</td>
</tr>
<tr>
<td>For a Site failover where VMware M&amp;R UI is still running, the Failover Manager performs the actions described in Chapter 12 Site Failover for the failed VMware Smart Assurance components.</td>
<td>It depends on your VMware Smart Assurance deployment:</td>
</tr>
<tr>
<td>■ A hook script is not needed if the VMware M&amp;R collector is located near the Domain Manager at both Active (Site A) and Standby (Site B) locations in the same geographical area. In this case, delays due to high latency are not a concern and the same collector can get information from Domain Managers regardless of the site from which they are running.</td>
<td></td>
</tr>
<tr>
<td>■ A hook script is needed if the Domain Managers at both Active (Site A) and Standby (Site B) locations are geographically dispersed and the VMware M&amp;R collector is not located near the Domain Managers. Delays due to high latency are a concern when an Active Domain Manager associated with a collector fails. Also, for latency reasons, you should consider installing a second collector near the Standby location (Site B). Typically, you need at least one collector per site.</td>
<td></td>
</tr>
</tbody>
</table>

“Example of smarts-collector messages that indicate high latency” on page 69 provides additional information about high latency.

Configure VMware M&R collectors for an VMware Smart Assurance failover

When the VMware M&R smarts-collector cannot collect performance data from newly-promoted Active Domain Managers due to high latency, you can configure a hook script which starts another VMware M&R collector to communicate with the newly-promoted Active Domain Manager.

Perform the following tasks:

1. Modify the sample hook script
2. Set the web-service gateway credentials in the clientConnect.conf file
3 **Import the web-service gateway certificate into the Failover Manager jre keystore** which includes restarting the Failover Manager.

You can customize the sample hook script named `failover_post_AMPM-sample.pl` for the following configurations:

- A group of Domain Managers defined by a ServerType communicating with one collector.
- A specific Domain Manager communicating with one collector.
- Different Domain Managers communicating with different collectors.

Copy the sample script multiple times and rename it as `failover_post_<ServerName>.pl` for each Domain Manager.

The Failover Manager runs the hook script each time a failover of a Domain Manager with the type `<ServerType>` or the name `<ServerName>` occurs.

You might have a collector set up for each Domain Manager (IP Manager, MPLS Manager, NPM, and so on). If so, then you configure a hook script for each collector. Or, you might have one collector set up to collect from three IP Managers and another collector set up to collect from three Server Managers. Then, you configure a hook script with the AM type and another hook script with the ESM type.

The hook script assumes that:

- A collector near Site A is collecting from one or more Domain Managers. The hook script can be of same server type like AM-PM or AM, ESM.
- Two web-service gateway services exist. One manages Collector A and the other manages Collector B. Or, there may be one web-service gateway that manages both collectors.

By default, the hook script will not stop an VMware M&R collector for the failed Domain Manager, but the script will only start the collector near the new Active site. You can change this default behavior by modifying the `stopNeeded` parameter.

The hook script uses the VMware M&R web-service gateway to send service requests. By default, the gateway uses https protocol.

**Modify the sample hook script**

Configure one or more hook scripts according to your environment:

1. Copy the sample customer script `failover_post-AMPM-sample.pl` from the `FAILOVER_BASEDIR/smarts/local/actions/samples` directory to the `FAILOVER_BASEDIR/smarts/local/actions` directory.

2. Rename the `failover_post-AMPM-sample.pl` script.

This script works only with Domain Managers. It does not work with Service Assurance Manager, Business Impact Manager, Adapter Platform, Trap Exploder, or Trap Adapter, because the VMware M&R smarts-collector does not collect data from these components.

Use one of the following file naming conventions:
Table 14-2. File naming conventions for the hook script used for collectors

<table>
<thead>
<tr>
<th>Rename the sample script as one of the following:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failover_post_&lt;ServerType&gt;.pl</td>
<td>Where &lt;ServerType&gt; is one of the following: AM, AMPM, PM, ESM, MPLS, NPM, or VoIP. A hook script with this naming convention will run after the Failover Manager performs a failover for any Domain Manager of the specified type. For example: failover_post_AMPM.pl</td>
</tr>
<tr>
<td>failover_post_&lt;ServerName&gt;.pl</td>
<td>Where &lt;ServerName&gt; is the specific Domain Manager name. Values for the Name parameter for a complete list of default names. A hook script with this naming convention will run after the Failover Manager performs a failover for the specified Domain Manager. For example: failover_post_INCHARGE-AM.pl</td>
</tr>
</tbody>
</table>

1. Modify the settings in the Configuration Section of the script according to your environment. In addition to the settings described in the script, review the following:

2. Set both web-service URLs to the same value if one web-service gateway manages the collector in Location-A and the collector in Location-B.

3. For a failover_post_<ServerType>.pl script, set the serverNames parameter to an empty list in order to run the script for all Domain Managers of the specified type. To limit the script to a few Domain Managers of the same type, list the Domain Managers in the serverNames parameter. For a failover_post_<ServerName>.pl script, setting the serverNames parameter is not necessary, because the name of the script identifies the Domain Manager.

4. Set the stopNeeded parameter to True according to your deployment. When the parameter is set to True, the script attempts to stop the collector only if the peer collector has started successfully.
By default (False), the hook script will not stop an VMware M&R collector for the failed Domain Manager, but the script will only start the collector near the new Active site.

- Set the stopNeeded parameter to True if you have only one Domain Manager that communicates with the collector and you want to stop the collector when the Active Domain Manager is failing over.
- Set the stopNeeded parameter to False if you have a single collector communicating with multiple Domain Managers like IP Availability Manager, NPM, and MPLS Manager. The hook script should not stop the collector when a single Domain Manager in the group fails over.
- Set the stopNeeded parameter to False if you have two collectors associated with two sites communicating with multiple Domain Managers like IP Availability Manager, NPM, and MPLS Manager. The hook script should not stop the collector when a single Domain Manager in the group fails over. The collector associated with Site-A should continue running and communicating with the rest of the Domain Managers running on Site-A and the collector associated with Site-B should be started.

**Note**  The stopNeeded parameter should be set to False when the primary smarts-collector is collecting data from multiple Domain Managers. In this case where both primary and secondary smarts-collectors are running, both collectors will collect data from Domain Managers and duplicate data entries can appear in the VMware M&R database. The duplicate entries should not impact any VMware M&R reports, but the size of the database will increase due to duplicate database entries. In this case, if you stop the smarts-collector by setting the parameter to True, the VMware M&R reports will not display data from the other running Domain Managers that did not failover.

If you have multiple Domain Managers communicating with the collector, the script may run multiple times if multiple Domain Managers are failing over.

It is safe for the hook script to request the starting of an already running collector. The request just returns the status of the collector.

5  Save the script.

**Set the web-service gateway credentials in the clientConnect.conf file**

In the clientConnect.conf file, the host value needs to match the host in the web-service URL that you specified in the failover_post hook script.

- For Linux, the host value must exactly match the name displayed when you run the Linux hostname command on the host where the webservice gateway is running.
- For Windows, specify the Fully Qualified Domain Name (FQDN) for the host.

To set the credentials for web-service gateway:

a  Use sm_edit to open the /opt/InCharge/SAM/smarts/conf/local/clientConnect.conf file in the SAM installation where Failover Manager resides.
b Locate the Web services Access section and specify the credentials for the M&R FrontEnd and the web-service gateways of the smarts-collector hosts. Replace the string starting with <E-1.0> and going to the end of the line with your actual password. sm_edit will encrypt the password when you save the file.

If the Web services Access section is missing from the file, copy from here and paste it before the User Access section in the file.

```
#################### Webservices Access ###################
# Credentials to access MNR.  
# This is used by Failover Manager.  
# You should change the password!
*:http://*:58080/*:admin:<E-1.0>94441BB01A289C5DE16282DF494915A8CCD0DBD64001866FD26CA40987554FCF  
# Credentials to access MNR webservice-gateway.  
# This is used by Failover Manager.  
# You should change the password!
*:https://*:48443/*:admin:<E-1.0>94699AAE806A6871183086D6E9B668CC438844AB14F846E5DA5407DE4D62ADA
```

c Save the file and exit.

Import the web-service gateway certificate into the Failover Manager jre keystore

To import the web-service gateway certificate from M&R collector hosts into the Failover Manager jre keystore:

1 On the VMware M&R web-service gateway host, for each of the gateway services (A and B), perform Steps 2a-b.

2 Export web-service gateway certificate:

```
```

3 Copy the W4Ngateway-<A|B>.cert file to the machine where the Failover Manager is installed.

4 In the SAM installation where Failover Manager resides, back up the existing jre cacerts file. Type:

```
# cp /opt/InCharge/SAM/smarts/jre/lib/security/cacerts /opt/InCharge/SAM/smarts/jre/lib/security/cacerts-BACKUP
```

5 In the SAM installation where Failover Manager resides, import the W4Ngateway-<A|B>.cert to JVM cacerts file:

```
# /opt/InCharge/SAM/smarts/jre/bin/keytool -import -file W4Ngateway.cert -alias W4Ngateway-<A|B> -keystore /opt/InCharge/SAM/smarts/jre/lib/security/cacerts
```
6 After importing both certificates, stop and start the Failover Manager. Start the Failover Manager provides start and stop commands for the Failover Manager.
Test and Verify the Failover System

This chapter includes the following topics:

- Failover system components
- Failover directories
- Verify failover status
- Log files
- Failover system tests
- Failover notifications

Failover system components

Verify that the components are set up, connected, and configured as described in the product documentation.

The components include the:

- Failover Manager
- Broker
- Active and Standby Service Assurance Managers
- Active and Standby Adapter Platforms (OI)
- Active and Standby BIM servers
- Active and Standby IP Availability Managers
- Active and Standby MPLS Managers
- Active and Standby Server Managers (ESM)
- Active and Standby Network Protocol Managers
- Active and Standby VoIP Availability Managers
- Active and Standby Trap adapters
Failover directories

The common directories for all products (SAM, Adapter Platform, BIM, AM, PM, AMPM, ESM, MPLS, NPM, and VoIP) include the following:

Under the BASEDIR/smarts/local folder:

- rules
- actions
- script
- model
- conf/trapd
- conf/beacon
- conf/asm-ntier
- conf/audit-parse
- conf/serverhealth
- conf/icim-core
- conf/maps
- conf/notifier
- conf/alcatel-sam

IP Manager-specific directories

These include the following:

Under the BASEDIR/smarts/local folder:

- conf/discovery
- conf/devstat
- conf/icf
- conf/health

SAM, Adapter Platform, and BIM-specific directories

These include the following:

Under the BASEDIR/smarts/local folder:

- consoles
- conf/infovista2
MPLS-specific directories

These include the following:

Under the BASEDIR/smarts/local folder:

- conf/mpls-tma
- conf/vpn-tagging
- conf/mpls-t
- conf/mpls-m
- conf/mpls-a

MPLS Topology Server, MPLS Analysis Server and MPLS Monitoring Server will copy conf/mpls-t, conf/mpls-a and conf/mpls-m directory, respectively.

If the directory is not present in the Active component, it will log an error in the action log file and continue to do further backup.

If the directory is not present in the Standby component, it will create that directory before copying the content.

The RPS gets copied from the Active to the Standby component after a specific interval (based on the value specified for the BackupInterval parameter in the failover.conf) with the name <server-name>.latest.rps in the Standby component.

ESM-specific file directories

These include the following:

Under the BASEDIR/smarts/local folder:

- conf/esm
- conf/trapd
- conf/beacon
- conf/asm-ntier
- conf/audit-parse
- conf/serverhealth
- conf/icim-core
- conf/maps
These directories will be copied after a specific interval (based on the value specified for the BackupInterval parameter in the failover.conf file) from the Active Server Manager (ESM) to the Standby Server Manager.

If the directory is not present in the Active component, it will log an error in the action log file and continue to do further backup.

If the directory is not present in the Standby component, it will create that directory before copying the content.

The rps will be getting copied from Active to Standby component after a specific interval (BackupInterval, mentioned in failover.conf file) with the name <server-name>.latest.rps in the Standby component.

### NPM-specific directories

These include the following:

Under the BASEDIR/smarts/local folder:

- conf/bgp
- conf/eigrp
- conf/fnd
- conf/icf
- conf/isis
- conf/msi
- conf/ospf

### VoIP-specific directories

These include the following:

Under the BASEDIR/smarts/local folder:

- conf/fnd
- conf/icf
- conf/mshm
- conf/voip
Verify failover status

To check the failover configuration and status, type the following command from the FAILOVER_BASEDIR/smarts/local/script directory:

```
ic-failover-server status```

Log files

All log files related to failover are available under BASEDIR/smarts/local/logs directory.

The INCHARGE-FAILOVER.actions.log file contains the details of the actions that Failover Manager performed. This file is generated only if ActionLogging is set to TRUE in the failover.conf file.

Failover system tests

A comprehensive set of scenarios must be developed and used to test the Failover System in various situations. The scenarios should include, for example:

- Active component is Up; Standby component is Up, Down, Unresponsive, Unreachable
- Active component is Down; Standby component is Up, Down, Unresponsive, Unreachable
- Active component is Unresponsive; Standby component is Up, Down, Unresponsive, Unreachable
- Host on which the Active component resides is Unresponsive; Standby component is Up, Down, Unresponsive, Unreachable
- Location of the Active component is Unreachable; Standby component is Up, Down, Unresponsive, Unreachable

During the tests, email should be sent to the specified personnel. Type of email include:

- Informational email — Failure on Standby server, host, or location. This is to inform administrators of a failed Standby component although the Active component is functioning as expected and the whole system is unaffected. It provides an opportunity for administrators to fix the problem before the Active component fails and a smooth failover can be achieved when required.
- Warning email — Error during backup actions of component <serviceName>.... Sometimes, a launched action may fail because of timing where the resources may be abruptly unavailable, such as a location that becomes unreachable, or an Active or Standby component that goes Down.
- Failover email — A failover has occurred.
- Failover Error email — There is a failure on an Active component or host, but the system cannot failover because of one or more failed Standby components.
Failover notifications

To view failover notifications, ensure that SAM is configured as described in Configure the Failover Manager as a source for SAM.

Failover Manager generated notifications lists the impacted classes and possible events generated by the Failover Manager in the Notification Log Console. Failover Manager generated notifications provides a sample of the notifications displayed in the Notification Log Console.

When primary SAM failover happens, notifications are displayed in secondary SAM when it becomes the primary.

Table 15-1. Failover Manager generated notifications

<table>
<thead>
<tr>
<th>Class</th>
<th>Event</th>
<th>Description</th>
<th>Severity</th>
<th>Subscribed to by the Global Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>InChargeService</td>
<td>Down</td>
<td>Service is dead or the host is unresponsive while the location is accessible. Dead service or all the active services in an unresponsive host will be failed over to secondary service.</td>
<td>Severity 1</td>
<td>Yes</td>
</tr>
<tr>
<td>InChargeBroker</td>
<td>Down</td>
<td>Service is dead or the host is unresponsive while the location is accessible. Dead service or all the active services in an unresponsive host will be failed over to secondary service.</td>
<td>Severity 1</td>
<td>Yes</td>
</tr>
<tr>
<td>InChargeService</td>
<td>PrimaryUnregistered</td>
<td>The service is not registered. Failover Manager will try to register the service to brokers.</td>
<td>Severity 3</td>
<td>Yes</td>
</tr>
<tr>
<td>InChargeService</td>
<td>Unresponsive</td>
<td>Either the service or the host is unresponsive. A consistent unresponsive state may lead to the server going down.</td>
<td>Severity 2</td>
<td>Yes</td>
</tr>
<tr>
<td>Host</td>
<td>Unresponsive</td>
<td>This system is not responding to ICMP ping requests (timing out). It does not necessarily mean the system is down. Timeout may have occurred due to some network connectivity issues.</td>
<td>Severity 1</td>
<td>Yes</td>
</tr>
<tr>
<td>InChargeBroker</td>
<td>Unresponsive</td>
<td>Either the service or the host is unresponsive. A consistent unresponsive state may lead to the server going down.</td>
<td>Severity 2</td>
<td>Yes</td>
</tr>
<tr>
<td>Location</td>
<td>Unreachable</td>
<td>Indicates that this location cannot be accessed before timing out.</td>
<td>Severity 1</td>
<td>Yes</td>
</tr>
<tr>
<td>UnitaryComputerSystem</td>
<td>Timedout</td>
<td>This system did not respond to ICMP ping request before timing out.</td>
<td>Severity 1</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Figure 15-1. Failover Manager generated notifications

<table>
<thead>
<tr>
<th>No</th>
<th>Owner</th>
<th>Class</th>
<th>Name</th>
<th>Event</th>
<th>Source</th>
<th>Impact</th>
<th>Count</th>
<th>Last Notify</th>
<th>Post Notify</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18.12.13 07:02:35</td>
<td>03.14.16:27</td>
<td>03.14.16:27</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18.12.13 07:02:35</td>
<td>03.14.16:27</td>
<td>03.14.16:27</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18.12.13 07:02:35</td>
<td>03.14.16:27</td>
<td>03.14.16:27</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18.12.13 07:02:35</td>
<td>03.14.16:27</td>
<td>03.14.16:27</td>
</tr>
</tbody>
</table>
Failover Performance Statistics

This chapter includes the following topics:

- Environment
- Scenario
- Results
- Recommendations

Environment

The performance statistics obtained for a failover system had multiple domain managers and Failover Managers set up on the Active and Standby sites. The set up consisted of the following:

Table 16-1. Failover performance statistics example

<table>
<thead>
<tr>
<th>Active site</th>
<th>Standby site</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-1 running on port 2002</td>
<td>IP-1 running on port 2000</td>
</tr>
<tr>
<td>SAM running on port 1600</td>
<td>SAM, Broker, and Failover1(monitoring IP-1,broker and SAM) running on port 1600</td>
</tr>
<tr>
<td>IP-2 running on port 2001</td>
<td>IP-2 running on port 2001</td>
</tr>
<tr>
<td>ESM and MPLS running on ports 1660-1650-1651-1652</td>
<td>MPLS, ESM, and Failover2(monitoring IP-2, MPLS and ESM) running on ports 1660-1650-1651-1652</td>
</tr>
<tr>
<td>Total number of systems in the topology is 1197</td>
<td>Total number of systems in the topology is 1176</td>
</tr>
<tr>
<td>Total number of managed ports is 50304</td>
<td>Total number of managed ports is 7818</td>
</tr>
<tr>
<td>Total number of managed interfaces is 48205</td>
<td>Total number of managed interfaces is 144287</td>
</tr>
</tbody>
</table>

Scenario

The performance scenario included calculating the time taken by each process that runs in the background during backup of files from Active to Standby server. The values of the following parameters were monitored on Active and Standby servers before discovery, and after discovery of topology.

- RPS copy time
- File copy time
- Restore time
- Suspend time
- Reconfigure time
- Regroup time
- Codebook time

The time taken for a failover from Active to Standby server was also monitored using the default settings –

polling interval(120), retry(3), timeout(700 ms), DetachInterval(300)

Monitoring and polling is reactivated after a failover in under 2 polling cycles irrespective of the size of topology.

Results

The time taken by the Failover System for RPS copy, file copy, restore, reconfigure, and Codebook computation varied with varying topology sizes. Time taken for IP Manager provides information on the time taken for the IP Manager with approximately 50,000 managed ports and interfaces.

Table 16-2. Time taken for IP Manager

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Active Server</th>
<th>Standby Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup time</td>
<td>388 seconds</td>
<td>438 seconds</td>
</tr>
<tr>
<td>Repos Copy time</td>
<td>15 seconds</td>
<td>35 seconds</td>
</tr>
<tr>
<td>Restore repos time</td>
<td>126 seconds</td>
<td>104 seconds</td>
</tr>
<tr>
<td>Reconfiguration</td>
<td>225 seconds</td>
<td>510 seconds</td>
</tr>
</tbody>
</table>

Time taken for Service Assurance Manager provides information on the time taken for Service Assurance Manager.

Table 16-3. Time taken for Service Assurance Manager

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Active Server</th>
<th>Standby Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup time</td>
<td>18 to 30 seconds</td>
<td>18 to 30 seconds</td>
</tr>
</tbody>
</table>

When the topology was increased by approximately 30 devices, the time taken by the Failover System to copy the RPS and other files, restore, and reconfigure the IP Manager also increased. Time taken for IP Manager after increasing topology provides more information.

Table 16-4. Time taken for IP Manager after increasing topology

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Active Server</th>
<th>Standby Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup time</td>
<td>438 seconds</td>
<td>Not tested</td>
</tr>
<tr>
<td>Repos Copy time</td>
<td>17 seconds</td>
<td>Not tested</td>
</tr>
<tr>
<td>Restore repos time</td>
<td>135 seconds</td>
<td>Not tested</td>
</tr>
<tr>
<td>Reconfiguration</td>
<td>263 seconds</td>
<td>Not tested</td>
</tr>
</tbody>
</table>
Failover time on the Active and Standby servers provides information on the actions during a failover and, the time taken to complete the failover and bring up the new Active server.

Table 16-5. Failover time on the Active and Standby servers

<table>
<thead>
<tr>
<th>Failover action</th>
<th>Time taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time taken to detect that the Active server is down and trigger a failover</td>
<td>Approximately 3 minutes</td>
</tr>
<tr>
<td>Time taken by the Failover System to assign the Standby role to the Active server which is down</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Expected time which includes DetachInterval(300) and failover detection time from polling interval(120), retry(3), timeout(700 ms)</td>
<td>8 minutes</td>
</tr>
<tr>
<td>Total number of polling cycles to set up monitoring and polling on the new Active server</td>
<td>3 polling cycles</td>
</tr>
<tr>
<td>Total time taken to complete the failover action and bring up the new Active server</td>
<td>Approximately 11 minutes</td>
</tr>
</tbody>
</table>

Note  The performance of the Failover System was tested in the VMware lab environment. There are external factors outside of VMware Smart Assurance software control, such as customer topology size, server machine resource allocation, LAN configuration, and others, that may introduce variances in the statistics.

Recommendations

The Failover Detection time can be reduced by changing the values of the parameters, polling interval, retry, and timeout for that server.

DetachInterval time can also be reduced by setting a lower value for DetachInterval which is 300 seconds (5 minutes) by default.

EMC recommends using the default values for polling interval, retry, timeout, DetachInterval in a typical deployment.
BASEDIR Information

BASEDIR installation directory

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed:

- For UNIX, this location is: /opt/InCharge/<product>.
- For Windows, this location is: C:\InCharge\<product>.

For example, on UNIX operating systems, VMware Smart Assurance Service Assurance Manager is, by default, installed to /opt/InCharge/SAM/smarts. On Windows operating systems, this product is, by default, installed to: C:\InCharge\SAM\smarts. This location is referred to as BASEDIR/smarts.

Optionally, you can specify the root of BASEDIR to be something other than /opt/InCharge (on UNIX) or C:\InCharge (on Windows), but you cannot change the <product> location under the root directory.

The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.
EDAA mode for 9.3 IP Managers

Configuring EDAA mode for 9.3 IP Managers

If you are using 9.3 IP Managers in a deployment scenario with both the Failover Manager and Configuration Manager in the VMware M&R UI, the 9.3 IP Manager service command --edaa=ip/2.0 option does not have the features to support the Failover Manager. As a result, you have to manually configure the EDAA mode for 9.3 IP Managers for only this scenario.

Skip this section if you are only using Failover Manager and not Configuration Manager, because the 9.3 IP Managers do not need to be exposed using EDAA. Or, if you are only using Configuration Manager, because the 9.3 IP Managers service --edaa=ip/2.0 option that lacks Failover Manager support is not an issue.

Procedure: EDAA mode for 9.3 IP Managers

1. Edit the msa-sources.xml file located in the SAM installation in <SAMBASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes to add entries for your IP Managers.

2. For example, add the entry key information:

   `<entry key="INCHARGE-AM-93" value-ref="MsaDMTDataSource__INCHARGE-AM-93" />`

3. Add the corresponding bean id information.

   `<bean id="MsaDMTDataSource__INCHARGE-AM-93" class="com.emc.msa.dmt.dmpool.MSADMTContext">
   <property name="brokerContext" ref="MsaDMTDataSource__Broker" />
   <property name="dmtName" value="INCHARGE-AM-93" />
   <property name="dataSourceName" value="INCHARGE-AM-93" />
   <property name="modelName" value="ip" />
   <property name="modelVersion" value="2.0" />
   <property name="useTLS" value="true" />
   <property name="disableKeepalives" value="true" />
   </bean>`
4 Open the `msa-model-defaults.xml` file in the `<SAM-BASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes/` directory. If not commented, comment the `MR_MetaObject` value in the XML node with id="IPExcludeClassesDefault". For example:

```xml
<util:list id="IP-ExcludeClassesDefault">
  <value>GA.*</value>
  <value>ICIM_Test</value>
  <value>NasManager</value>
  <value>Topo.*</value>
  <value>Hierarchical.*</value>
  <value>VOIP.*</value>
</util:list>
```

5 Use `sm_edit` to open the `<SAM-BASEDIR>/smarts/conf/edaaClientConnect.conf` file.

6 Add an entry for the IP Manager using the format `*:<DOMAINNAME>:admin:changeme`.

```text
*:INCHARGE-AM-92:admin:changeme
::_edaa:changeme
```

7 Save the file.

8 Stop and start the smarts-tomcat, smarts-rabbit-mq, and smarts-elasticsearch services.
Troubleshooting

This chapter includes the following topics:

- Log files
- Troubleshooting the Invalid drive specification message
- Troubleshooting OTM when the Rabbit MQ service fails over
- Troubleshooting IP Configuration Manager when the Tomcat service fails over
- After failover Server Manager does not synchronize with IP Manager
- After failover Business Impact Manager sometimes does not list SAM as a source
- Example of smarts-collector messages that indicate high latency
- Windows PowerShell and Server Message Block additional information
- Where to get help

Log files

All log files related to failover are available under BASEDIR/smarts/local/logs directory.

- The <failover_manager>.actions.log file contains the details of the actions that Failover Manager performed. This file is generated only if the ActionLogging parameter is set to TRUE in the failover.conf file.

  The <failover_manager>.actions.log file is generated after you reload the failover.conf and if you reconfigure the Failover Manager using the Domain Manager Administration Console.


- sm_configureFailover<timestamp>.log contains the subscriptions made and the entries added to the failover.conf file.

Generating detailed debugging information in log files

If the Failover Manager’s log and actions log do not contain enough information to solve the problem you are observing, set the ActionLogging and Debug parameters to True in the failover.conf file and restart the Failover Manager.
Troubleshooting the Invalid drive specification message

On Windows, in the Failover Manager log, the message:

```
Invalid drive specification
```

does not always mean that the wrong drive was configured for the VMware Smart Assurance installation on the remote host. It can mean a permissions issue or other issue that prevents the Failover Manager from accessing the shared drive on the remote host.

Check that:

- The drive is shared with the correct permissions.
- The Failover Manager service is configured to run as ".\Administrator".

Setting up Administrator service for PowerShell remoting (Windows only) provides instructions about setting up the Failover Manager service.

Troubleshooting OTM when the Rabbit MQ service fails over

SND-1758

VMware Smart Assurance Optical Transport Manager (OTM) is not supported for failover.

OTM communicates with the VMware Smart Assurance Notification Exchange (Rabbit MQ) which is one of the components of the SAM server with Notification Cache Publishing Enabled.

If the Rabbit MQ service (smarts-rabbitmq) goes down, the Failover Manager considers the Active SAM to be down and performs a failover. Also, the AMQP_Consumer ConnectionError notification appears in the VMware M&R UI.

If you receive the AMQP_Consumer ConnectionError notification, restart the Rabbit MQ service (smarts-rabbitmq). Then, OTM will continue to process events.

Troubleshooting IP Configuration Manager when the Tomcat service fails over

SND-1757

VMware Smart Assurance IP Configuration Manager is not supported for failover.

If you are using the Configuration Manager in the VMware M&R UI to control discovery configuration settings, the Configuration Manager communicates with the VMware Smart Assurance Data Web Applications (Tomcat). Tomcat is one of the components of the SAM server with Notification Cache Publishing Enabled. The EMC Data Access API (EDAA) with service name smarts-edaa resides in Tomcat.
If the Tomcat service (smarts-tomcat) goes down, the Failover Manager considers the Active SAM to be down and performs a failover. The Failover Manager promotes the Standby SAM and its Standby services to Active. The Configuration Manager can continue to communicate with the newly-promoted Active Tomcat, because the Configuration Manager service indicates the primary and secondary EDAA in the Active and Standby Tomcats.

1. The Configuration Manager service must be installed to be registered with both primary EDAA and secondary EDAA. Type:

   ```
   sm_service install --force --unmanaged --startmode=runonce \
   '---name=ic-ip-configuration-edaa' \
   '---description=EMC Smarts IP Configuration Manager for EDAA' \
   '/opt/InCharge/IP/smarts/bin/sm_server' \
   '---name=INCHARGE-CM' \
   '---config=icf-c' \
   '---bootstrap=bootstrap.conf' \
   '---port=0' \
   '---edaa=ip/2.0@SMARTS-EDAA-A,SMARTS-EDAA-B' \
   '---ignore-restore-errors' \
   '---nodx' \
   '---output'
   ```

2. Start the Configuration Manager service from the BASEDIR/smarts/bin directory:

   ```
   ./sm_service start ic-ip-configuration-edaa
   ```

### After failover Server Manager does not synchronize with IP Manager

**SND-1279**

**Issue**

During a failover when the Active Server Manager goes down, the Failover Manager promotes the Standby Server Manager to Active. The newly-promoted Active Server Manager is not able to synchronize with IP Manager using discover-all. For example, the following error appears in the Server Manager log file:

```
SVIF-W-ESERVERCONNECT-While attempting to (re)connect to the remote server 'INCHARGE-AM-PM'
SM-ECONNECT-Attempt to connect failed; in file "g:/DMT-9.4.0.0/33/smarts/skclient/servif/SM_Broker.c" at line 423
```
Resolution

Two workarounds exist:

- For the newly-promoted Active Server Manager, type this command to force a topology synchronization:

  ```
  dmctl -s INCHARGE-AM-PM invoke ICF_TopologyManager::ICF-TopologyManager updateDiscoveryTimers
  ```

- Or, in the IP Manager, perform a discovery (Topology > Discover All) which results in the Server Manager synchronizing with the IP Manager.

After failover Business Impact Manager sometimes does not list SAM as a source

SND-1605

Issue

After a failover, the newly-promoted Active MBIM sometimes does not list SAM as a source. As a result, MBIM does not have topology from SAM.

Resolution

When MBIM failover happens, if the SAM server is not present, add the SAM as source to MBIM server. This enables newly-promoted Active MBIM to interface with SAM. Configure Active BIM provides steps for adding SAM as a source.

Example of smarts-collector messages that indicate high latency

The following messages in the smarts-collector indicate that the collector is not keeping up with domain polling. If a polling action exceeds 235 seconds, it is considered late.

```
collecting-0-0.log:INFO  -- [2014-03-27 07:20:36 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM2 (conf/smarts-pm.xml): polling completed in 235.674s, next polling will be late...
collecting-0-0.log:INFO  -- [2014-03-27 07:24:24 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM1 (conf/smarts-pm.xml): polling completed in 234.032s, next polling in 5.966s...
collecting-0-0.log:INFO  -- [2014-03-27 07:24:38 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM2 (conf/smarts-pm.xml): polling completed in 241.856s, next polling will be late...
collecting-0-0.log:INFO  -- [2014-03-27 07:28:25 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM1 (conf/smarts-pm.xml): polling completed in 244.88s, next polling in 5.118s...
collecting-0-0.log:INFO  -- [2014-03-27 07:28:47 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM2 (conf/smarts-pm.xml): polling completed in 248.549s, next polling will be late...
collecting-0-0.log:INFO  -- [2014-03-27 07:32:35 MDT] -- SmPollingData::updateNextPollingDelay(): emc-smarts : INCHARGE-PM1 (conf/smarts-pm.xml): polling completed in 244.762s, next polling will be late...
```
Windows PowerShell and Server Message Block
additional information

Additional information about configuring WinRM is available at:
Installation and Configuration for Windows Remote Management

Tips on PowerShell remote execution are available by running these commands:

```
powershell get-help about_remote
powershell get-help about_remote_troubleshooting
```

Information on security enhancements in Server Message Block (SMB) 3.0 is available at:
SMB Security Enhancements

Where to get help

VMware support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware products, go to VMware Online Support at:

docs.vmware.com

Technical support

Go to VMware Online Support. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.