Security Management System High Availability Troubleshooting and Best Practices

Version 5.0.0

October 2017

Legal and notice information

TippingPoint Best Practices: Security Management System High Availability

Contents

About this guide

This guide is intended for Security Management System (SMS) administrators and network specialists who monitor and manage the SMS. The information provided describes how to troubleshoot the SMS in a high availability (HA) cluster and provides best practice information.

This section covers the following topics:

Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at *https://tmc.tippingpoint.com*. The documentation generally includes installation and user guides, command line interface (CLI) references, safety and compliance information, and release notes.

Product support

Information for you to contact product support is available on the TMC at *https://tmc.tippingpoint.com*.

Overview

The SMS can be configured to operate in an active-passive, HA cluster, increasing the availability of the SMS in case an unexpected event causes the primary SMS to fail or become inaccessible.

This guide explains how to diagnose issues with an SMS HA cluster and provides best practice information.

For detailed installation and configuration information, see the *Security Management System User Guide* on the Threat Management Center (TMC) at *https://tmc.tippingpoint.com/*.

Best practices

The following sections provide best practice information and guidelines for SMS HA clusters.

Disable HA before you apply software updates to the SMS

Disable HA between the primary and secondary SMS server when applying the following:

- A database patch or hotfix
- SMS software upgrades

With SMS HA disabled, apply the software upgrade, patch, or hotfix to both SMS servers separately, and then configure HA and synchronize the cluster.

You do not need to disable HA when installing an patch or hotfix that does not contain database changes.

Do not power off SMS while HA is enabled

To avoid potentially unrecoverable file system and database corruption, do not power off the SMS while HA is enabled.

If an SMS node is inaccessible, SSH to it from its peer node and then manually restart the SMS database and server services. If necessary, perform a shutdown or restart of the cluster from the primary SMS cluster using a CLI command.

Avoid network-related failovers

Avoid a network-related SMS HA server failover by ensuring that the network has a reliable link between the SMS servers with a bandwidth delay of less than 300 ms. Monitor the primary SMS server to make sure it is not overloaded and has adequate resources including memory, file systems, and threads.

By default, each node sends a heartbeat signal to its peer node every minute. If network issues prevent both nodes from receiving three consecutive heartbeat signals, it is possible for both server nodes to

be functional. However, the passive node initiates automatic failover, which results in an active-active configuration.

If necessary, fail back the cluster to the primary node by performing a synchronization.

Investigate server-related SMS HA failovers

Before performing a synchronization, investigate and resolve any server-related issues on the primary SMS server that may have resulted in SMS HA automatic failover to the secondary node.

When investigating SMS server issues, consider the following:

- The number of managed devices
- The rate at which the SMS server receives device events
- Profile distribution
- DV distribution

Enable dual NICs on the SMS

We recommend configuring a primary and secondary network interface on the SMS HA servers.

If the SMS primary and secondary servers are in different geographic locations, and only the primary network interface is enabled, make sure the network provides enough bandwidth for the heartbeat signal and replication operations, described in the section *To configure SMS HA with the SMS servers located in different geographical locations* on page 3.

To configure SMS HA with the SMS servers located in different geographical locations

You can configure the SMS server for HA while the servers are located in different geographic locations. The main issue with this configuration is maintaining the link between both SMS servers and the database replication. But with sufficient bandwidth, link reliability, and an acceptable delay (less than 300 ms), the configuration works properly.

By default, each node sends a heartbeat signal to its peer node every minute. If network issues prevent both nodes from receiving three consecutive heartbeat signals, it is possible for both server nodes to be functional. However, the passive node initiates automatic failover, which results in an active-active configuration.

To avoid unnecessary SMS HA server failover, ensure that the network has a reliable link between the SMS servers with a bandwidth delay of less than 300 ms. Monitor the primary SMS server to make sure it is not overloaded and has adequate resources including memory, file systems, and threads.

To resolve this issue, fail the cluster back to the primary node by performing a synchronization.

Before you contact TAC to request assistance

Before you contact TAC:

- Do not power off the SMS while under HA. Power cycling the SMS HA server causes file system and database corruption.
- Collect logs from both SMS nodes in the cluster. If the SMS client cannot collect the logs from the peer SMS server, SSH to the peer server node and use the CLI command to collect logs.
- Provide a description of the issue and the date it occurred.
- Collect the logs as soon as possible after the issue occurs to avoid losing log entries to logging rollover.

Troubleshooting

This section discusses common troubleshooting techniques.

How do I apply SMS software updates to a cluster?

Upgrades: Before applying software upgrades to an SMS HA cluster, be sure to disable the HA cluster. The process for upgrading an HA cluster is to disable clustering, upgrade each SMS server separately, and then reestablish the cluster. The passive SMS server cannot be upgraded while HA is enabled because:

1. The low-level services that are running on the passive node do not perform software upgrades or database updates.
2. Database updates on the passive node break database replication and as a result, data integrity.

Patches: Before applying a patch to an SMS HA cluster, determine whether the patch includes database updates:

- If the patch contains database changes, be sure to disable the SMS HA cluster, apply the patch to each SMS server separately, then reestablish the cluster. Applying a database patch while under SMS HA breaks database replication and as a result, data integrity. The patch process does not prevent you from applying a database patch while under SMS HA.
- If the patch does not contain database changes, initiate the patch process from the active SMS server. The active SMS server automatically propagates the patch to the passive SMS server. If the patch requires a restart of the SMS software, or a reboot of the SMS server, the action takes place on both the active and passive SMS servers.

Hotfixes: Before applying a hotfix to an SMS HA cluster, determine whether the patch includes database updates, and follow the same installation procedure for applying a patch.

Does SMS HA support IPv6?

SMS HA is not supported with IPv6. If the SMS is IPv6 only, the HA configuration button will display an error when selected.

Does SMS HA support external database replication?

External database replication and SMS HA features both leverage the same functionality in the underlying database. The SMS database does not support replication to multiple destinations; therefore, Trend Micro does not recommend using SMS HA and external database replication at the same time.

How do I configure SNMP or NAT on each SMS HA server?

SMS HA does not replicate the settings for *Simple Network Management Protocol (SNMP)* and *Network Address Translation (NAT)*. By default, only the active SMS can be configured to respond to SNMP queries. However, the passive SMS can be configured to respond to SNMP queries if you configure the SNMP service on the passive SMS before you enable SMS HA clustering. If SNMP is enabled, the SMS will respond regardless of its HA state. SNMP settings are managed independently on each SMS in a SMS HA cluster.

Why are my IPS devices unmanaged after I disable SMS HA?

Under normal HA failover conditions, the certificate from the active SMS is copied to the passive SMS and used to manage the devices. If the cluster fails-over or is swapped, then the devices are still seamlessly managed with the same certificate.

If the original passive SMS server becomes the active SMS server and you disable HA, then the SMS displays a dialog with two list panels.

- The left panel identifies devices that will continue to be managed by the currently active (original secondary) SMS.
- The right panel identifies devices that will be unmanaged by the currently active SMS. The devices in this right panel will be managed by the currently passive (original primary) SMS unless you unmanage them and remanage them on the currently active SMS.

To determine the original primary SMS that manages a device, run the `show sms` CLI command on the device.

How do I collect logs?

Collect SMS logs from both the primary and secondary SMS HA servers by running the following commands from the primary SMS server.

- To collect logs from the primary SMS server, run this command:

```
set logs.create=yes
```

- To collect logs from the secondary SMS server, run the command below. If this command is unsuccessful, SSH to the secondary SMS server and run the command above:

```
set logs.create-peer=yes
```

How do I access a secondary SMS HA server without the SMS client?

After you enable SMS HA, the SMS client cannot log in to the secondary (passive) server. Use service mode to access an otherwise inaccessible SMS server. To access service mode, contact product support.

Follow these steps:

1. Log in to the primary SMS server using service mode.
2. SSH to the secondary SMS server from the primary SMS server, for example, by running the following command:

```
ssh -i /root/.ssh/sms-ha.rsa root@<secondary_SMS_IP>
```

How do I identify the state of the SMS HA server?

Follow these steps:

- From service mode, run either of the following commands:
  - `cat /etc/ha.state`
  - `grep "Local state:" ha.log | more`
- From the CLI, run the following command:

  `get HA`

What are the HA state transitions?

When you enable SMS HA, the nodes transition through the states below. If a transition failure occurs, the node reverts to the previous state.

1. Un-configured
2. Configured
3. Primary: synchronization-source, Secondary: synchronization-target (synchronization state is transitional state).
4. Restart
5. Primary node is active and the secondary node is passive.

How do I isolate HA problems in service mode?

See the following sections for information about isolating HA problems in service mode.

HA Failed

- Review the ha.log files to determine when the failure first occurred by running the following command:
  - `grep "Local state: Failed" ha.log* | more`
- Review the sms-info.log for errors that occurred before the time and date of interest.
  - If the HA was shut down improperly, it is normal for the HA to initiate a Failed state.
  - If the passive node performed a takeover, and the active node detects an active peer, sometimes the peer asks the node to put itself in a Failed state to avoid an active/active cluster. By design, it needs to put itself in a Failed state.
  - Sometimes the peer asks the node to put itself in a failed state to avoid an active/active cluster.
  - See if there is a local health check failure, like a database check, for example.

Passive Takeover

Perform the following investigations:

- From passive node:
  - Run the following command:
    - `grep "considering cluster takeover" ha.log*`
  - Look at sms-info.log in the same time frame for any peer health check failures such as:
    - Heartbeat
    - Interface/network
    - Database
    - JBoss
  - `grep "attempting to restart active system" ha.log*`
- From the active node:
  - In the same timeframe, look for SMS failure of a local health check such as:
    - Heartbeat
    - Interface/network
    - Database

- JBoss

HA Degraded

- On SMS 4.0 (and later), check the ha.log files by running the following command:
  - `grep "DEGRADED HA" ha.log.*`
- On all SMS versions, check the sms-info.log* files for exceptions. Review the log entries that precede each exception to identify potential issues.

How do I determine whether the SMS is out of Java Heap memory?

A Java Heap memory error occurs when there is not enough Heap memory left for the application to operate correctly.

Run one of the following commands to check for out-of-memory errors:

- grep "java.lang.OutOfMemoryError" tpt_sms.txt
- `grep "java.lang.OutOfMemoryError" sms-info.log*`

How do I check for database errors?

Check the following log file for database corruption or crash entries:

- `/var/lib/mysql/dbdatadir/mysqld.err`

SMS HA terminology

Use the following terms and concepts to better understand SMS HA clustering.

Cluster heartbeat

A *cluster heartbeat* is an intra-cluster communication with which the two nodes in the cluster communicate their operating status. When the cluster is operating in a normal state, the passive server periodically sends a heartbeat signal to the active server. The active server responds, letting the passive server know that there are no issues and that there is no need for the passive server to initiate a failover process.

When the passive server sends a heartbeat request and the active server does not respond, the passive server makes a few more attempts, and even attempts alternate communication paths if available. If the passive server is unable to obtain a response from the active server, the passive server assumes the active server is unavailable and that it must initiate a failover process.

The heartbeat signal travels across an Ethernet network. You can instruct SMS HA to send the heartbeat over one of two possible network configurations. You can instruct SMS HA to send the heartbeat over the

same, public network that the SMS uses to communicate to its clients and managed devices. Alternatively, you can instruct the SMS to send the heartbeat over a private, intra-cluster Ethernet network.

If you configure SMS HA to use the private network, your configuration has built-in redundancy. If the heartbeat signal doesn't make it through the private network, the SMS attempts to communicate the heartbeat through the public network. If the heartbeat makes it through the public network, then the SMS will continue to operate without change, but if the heartbeat does not make it through the public network, then the SMS initiates a failover.

Failover

The SMS HA cluster configuration contains one SMS cluster node acting as the active SMS server and another SMS cluster node acting as a passive SMS server. Active and passive are roles that may be adopted by either physical cluster node. The process of promoting a passive SMS server to an active SMS server is called *failover*. A failover occurs when the primary SMS server experiences a fault or is taken offline for maintenance. You can also manually failover the cluster swap roles between the active and passive SMS servers.

Database replication

Critical SMS data, including the database and SMS configuration information, must be kept current on the passive SMS server, even as the active SMS server gathers and administers data generated by managed devices or its own activities. The active SMS server replicates the data to the passive SMS server. During initial configuration, the SMS cluster performs a synchronization of the database from the active SMS server to the passive SMS server.

The synchronization and replication can take place over the same network that is used by the SMS clients to connect to the active SMS server, or it can take place over a private, intra-cluster, network. If an intra-cluster network is used, the replication activity occurs over this private network, removing the traffic from the public network over which clients connect to SMS and through which SMS manages devices. To make use of an intra-cluster network, you need to connect an Ethernet crossover cable between the two cluster nodes and configure SMS HA to use a primary and secondary network configuration.

Data synchronization

When you first configure an SMS HA cluster, the cluster synchronizes files from the active SMS server to the passive SMS server. The synchronization is a complete replication of the SMS database and any SMS configuration files. The synchronization process also replicates some required security certificates from the active to the passive SMS server. When a failover occurs, and the surviving SMS server notifies its managed devices that it is the new active SMS server, it will have the correct security certificates to validate communications between itself and the devices.

To ensure that the important communications to and from the SMS server continue without disruption, as part of the failover process, SMS HA moves the network identity of the active SMS server to the passive SMS server. Continuity of network traffic is assured between:

- The SMS server and its managed devices
- The SMS server and the Threat Management Center (TMC)
- The active and passive SMS servers

Client connections

SMS clients use an IP address or a hostname to connect to an SMS server. When an SMS client first connects to an SMS HA cluster, it obtains and caches the IP addresses of each SMS HA cluster node. From that point on, whenever the SMS client attempts to log on to the SMS HA cluster, the client performs a round robin connection process with the IP addresses of the SMS HA cluster nodes, eventually connecting to the active node. Regardless of which SMS server is active, the round robin approach ensures that the SMS client connects to the active SMS server.

Managed device connections

The devices that the SMS manages do not maintain a continuous connection with an SMS server. Instead, the SMS server periodically creates a connection with each device, initiates a transfer of data, such as event data or operational statistics, obtains the data and stores it in the SMS database, and then disconnects from the device.

Unlike client connections, which are initiated by an SMS client and therefore require the client to know which SMS server is active, managed device connections are initiated by the SMS server. This means the managed device connections do not follow the same round robin process used by SMS clients.

One exception exists. When a managed device experiences an event that triggers an SNMP trap, the device sends the trap information to the active SMS server. The trap destination is configured in the managed device. When the SMS fails-over, the failover process includes a task to update the trap destination in each of the managed devices so that the trap destination always points to the active SMS server. If SMS HA is ever disabled, essentially breaking apart the cluster, then the SMS server that was designated as active when the cluster was formed now manages the devices.

Primary and secondary SMS server

The primary SMS server is the SMS server that was used to configure the SMS HA cluster. Under normal operation, the state of the primary SMS server is active, and the state of the secondary SMS server is passive, unless the primary server becomes unavailable. When the primary SMS is unavailable, the state of the secondary SMS changes to active.

During initial HA configuration, the SMS cluster performs a synchronization of the database from the active SMS to the passive SMS. To keep the passive SMS current, the active SMS replicates critical SMS data to the passive SMS, including database and SMS configuration.