



CHAPTER 14

Managing the Event Collector (AVM 100)

These topics describe the Prime Network Event Collector, the fault management tasks it performs, and how to configure multiple Event Collectors:

- [Overview of the Event Collector and Event Processing, page 14-1](#)
- [Configuring the Event Collector: Examples, page 14-6](#)
- [Enabling a Single Event Collector on a Gateway or a Unit, page 14-11](#)
- [Configuring and Enabling Multiple Event Collectors, page 14-12](#)
- [Registering VNEs with a Non-Default Event Collector, page 14-15](#)
- [Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15](#)
- [Disabling and Re-Enabling Event Archiving, page 14-16](#)

Overview of the Event Collector and Event Processing

When a trap or syslog is sent from a device to Prime Network, it is received by the Event Collector, which runs on AVM 100. [Figure 14-1](#) illustrates how Prime Network responds to incoming notifications from devices. The exact flow depends on how Prime Network is configured in your network.



Note

[Figure 14-1](#) illustrates the *logical* flow of events through Prime Network. The actual network communication is subject to the transport configuration between the gateway server and units.

Figure 14-1 How Prime Network Responds to Incoming Notifications from Devices

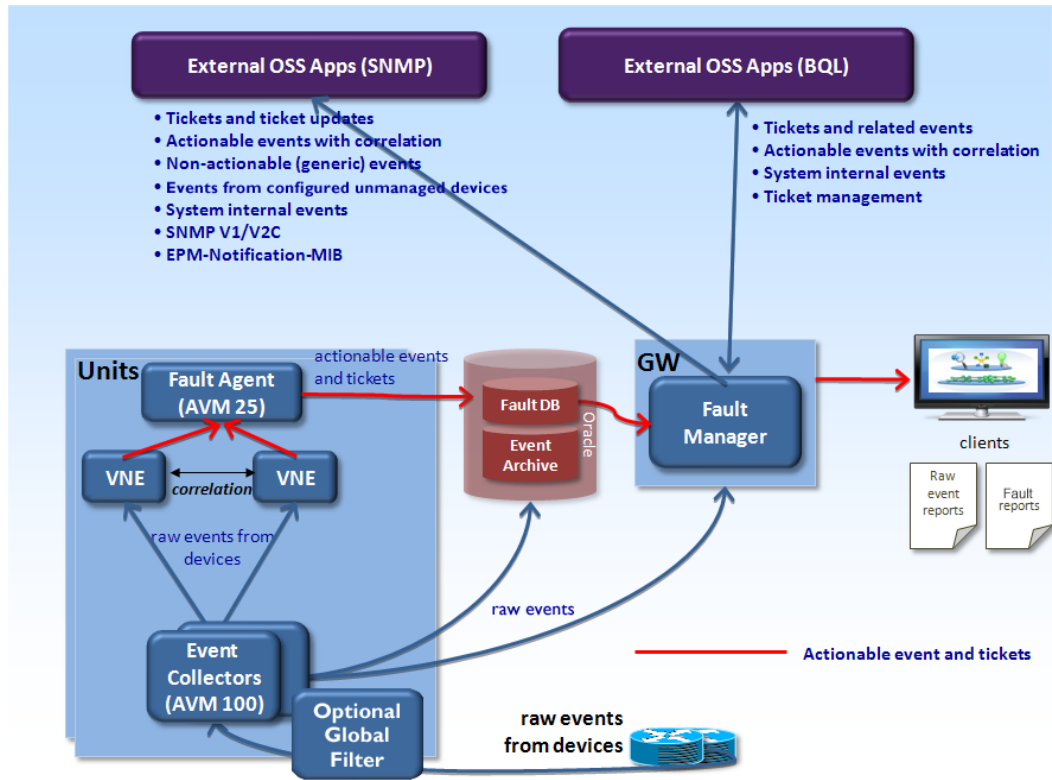


Figure 14-1 also illustrates the two entities that store fault information, both of which reside in the Prime Network database:

- **Event Archive**—Contains all raw events (traps, and syslogs) received from devices. The Event Archive also stores information from unmanaged devices (if notification from unmanaged devices is enabled; see the [Cisco Prime Network Integration Developer Guide](#)). The database schema name is `network user_ep`, where `network user` is the operating system user account for the Prime Network application. (This account is created when Prime Network is installed.) For example, if `network user` is named **network39**, the Event Archive schema is called **network39_ep**. You can only view information in the Event Archive using the reports mechanism. Event archiving is enabled by default, but you can disable it using the procedure in [Disabling and Re-Enabling Event Archiving](#), page 14-16.
- **Fault Database**—Contains all the actionable events (events that Prime Network knows how to parse and can therefore participate in correlation). The Fault Database also contains information such as tickets, alarms, and severity information. The Fault Database schema name is `network user`. For example, if `network user` is named **network39**, the main schema is called **network39**. You can view information in the Fault Database using the Prime Network Events and using Prime Network Vision GUI clients.

Event Archive and Fault Database data is archived and saved according to the settings in the **Global Settings > Event Management Settings** window in the Prime Network Administration GUI client. (See [Customizing Archive and Purge Settings for the Fault Database and Event Archive](#), page 10-6.)

The following topics describe how the Event Collector, VNEs, and the Fault Agent (AVM 25) work together to process incoming notifications from devices. For more details about the event flow illustrated in Figure 14-1, see the [Cisco Prime Network Integration Developer Guide](#).

Event Collector (AVM 100)

The Event Collector is the first receiver for incoming event notifications from devices. It is an internal service that is part of AVM 100. During installation, Event Collectors are created on the gateway and all units, but a single Event Collector AVM is started only on the gateway. By default, all new VNEs will register with the Event Collector on the gateway server. This Event Collector has the internal address 0.0.0.0 (this address is not related to the device IP address).



Note If desired, you can figure a filter that will drop “pure noise” at the Event Collector level. In other words, this filter will drop all raw events before any processing or archiving is done; the events are not processed by VNEs or forwarded using the Event Notification Service. Complete instructions for configuring this type of filter is provided on the Cisco Developer Network at <http://developer.cisco.com/web/prime-network/home>. (This is different from the global event filter that drops events at the VNE level when the system moves into safe mode; see [Automatic Overload Prevention \(AOP/Safe Mode\)](#), page 9-17.)

When an event, trap, or syslog is received by the Event Collector, the Event Collector does the following:

1. Performs initial parsing to obtain basic information about each event.
2. (If a global filter is implemented) Filters out (drops) any events that match the filter. By default, no filters are implemented. To configure a filter, see [Configuring the Event Collector: Examples](#), page 14-6.
3. Stores all events, traps, and syslogs in the Event Archive (if event archiving is enabled, which it is by default). Events are saved in the Event Archive only if the device has corresponding VNE which is registered to the Event Collector. This can also include information from unmanaged devices if notification from unmanaged devices is enabled (see the [Cisco Prime Network Integration Developer Guide](#)). If a syslogs is sent as an SNMP trap by way of the CISCO-SYSLOG-MIB, the Event Collector interprets it to be a syslog.
4. If enabled, forwards events from unmanaged devices to the Event Notification Service. (See [Configuring Event Notifications](#), page 6-1.)
5. Distributes each event to its corresponding VNE (if the VNE is registered with the Event Collector).

The Event Collector AVM requires a database connection when event archiving is enabled. If event archiving is disabled, a connection to the database is *not* required. To disable or reenable event archiving, see [Disabling and Re-Enabling Event Archiving](#), page 14-16.

Event Collector and Unit Server High Availability

You can configure the Event Collector to run on a unit instead of the gateway. If the unit is also configured with unit server high availability, the Event Collector on the standby unit will drop all events because the Event Collector is disabled. This is by design; it should not start until a switchover occurs.

The standby unit contains a port watchdog script that listens for events on the unit’s Syslog and SNMP ports. The script prevents unnecessary ICMP unreachable messages being sent back to the network. If a switchover occurs, the standby unit and Event Collector AVM will start, and the watchdog script releases the ports.

When the original unit comes back up, the standby Event Collector AVM goes back down, and the watchdog script recommences listening on the standby unit’s Syslog and SNMP ports.

**Note**

If the Cisco Prime Performance Manager application is also installed (with Prime Central), the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and do the following:

- Save TCA events in the Event Archive.
- Forward TCA events to appropriate VNEs. The events are currently not parsed by the VNE. They will be identified as generic traps and will be dropped. If desired, you can forward them to an Event Notification Service (see [Configuring an Event Notification Service, page 6-3](#)).

No special configuration is required.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at <http://developer.cisco.com/web/prime-network/home>.

VNEs

When a VNE receives an event from the Event Collector, the VNE does the following:

- Attempts to match the event with a predefined pattern. Events that are successfully matched are designated as *actionable events*. The VNE attempts to extract information from the raw event (the source, the problem, and the severity).

Events that are not matched can still be forwarded to configured recipients. This is done by an enabling an Event Notification Service to forward generic syslogs/enterprise trap syslogs. See [Figure 6-3 on page 6-6](#) for an example of how this is done from the Event Notification Service in the Prime Network Administration GUI client.

- If the event is actionable, correlates the event and, if possible, identifies a root cause.

Sends the parsed event and correlation information to AVM 25 to be saved to the Fault Database. The Fault Database also contains information such as tickets, alarms, and severity information.

These actions are performed by a process within the VNE called the *event manager*, which is responsible for handling all network events, whether they are syslogs or traps, discovered during normal polling, or threshold-crossing alarms.

VNEs must be registered with an Event Collector's internal address (this address is not related to the device IP address)). When a VNE is first initialized, the following occurs:

- The VNE reads this Event Collector's internal address from the registry. (By default, all new VNEs will register with the Event Collector on the gateway server. This Event Collector has the internal address 0.0.0.0.)
- The VNE registers its management IP address with this Event Collector.

If the Event Collector receives a trap or syslog, and the trap or syslog's source IP address matches the VNE's management IP address, the Event Collector will forward the syslogs or trap to that VNE.

A VNE may have more than one IP address registered with the Event Collector (for example, when the device is using other IP addresses as sources for syslogs or traps). These IP addresses can be discovered automatically from the device configuration but can also be manually configured using the VNE Event settings in Prime Network Administration (see [VNE Events Settings, page 19-42](#)).

AVM 25 (Fault Agent)

When a VNE forwards an event to AVM 25, the Fault Agent does the following:

1. Saves the information to the Fault Database.
2. If necessary, creates a new ticket based on the correlation information and event type. Some event types are configured as ticketable and others are not; this is controlled in the registry. Prime Network will create a ticket for ticketable events, even if they are non-correlated events.

AVM 25 requires a database connection to store information in the Fault Database so that it can be subsequently viewed in Prime Network Events. If a direct connection is not available, you can configure AVM 25 without connectivity to forward its events to another AVM 25 that does have a database connection. This is called using a *proxy AVM 25*. How to do so is described in [Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15](#).

Keep these items in mind when starting and stopping AVM 25:

- Avoid stopping AVM 25 to make sure that Prime Network does not drop events
- If you stop and restart AVM 25, you do not have to restart user-created AVMs.
- User-created AVMs will not start if AVM 25 is not running; they will be Unreachable.

Example of Full Event Flow

The following steps show the flow of events when Device A sends a Port Down notification to the Event Collector.

1. The Event Collector receives the notification and persists the Port Down event to the Event Archive. The Event Collector forwards the syslog to the corresponding VNE.
2. The VNE polls the device and issues a Link Down service event. The VNE correlates the Port Down event to the Link Down service event. The VNE sends all of this information to AVM 25.
3. AVM 25 saves all of this information to the Fault Database and opens a Link Down ticket with the Link Down event as the root cause. AVM 25 updates the severity aspect.

At this point, the Fault Database contains:

- A Link Down ticket with the Link Down event as its root cause.
- A Port Down event that has been correlated to the Link Down event.

At this point users can view the ticket in Prime Network Vision, but the Port Down event will not be in the ticket's correlation information.

4. When it queries the Fault Database, the Ticket Agent will pick up the Port Down event because it is correlated to a Link Down event, but not associated with any ticket. The Ticket Agent updates the Link Down service event, associates the Port Down event with the Link Down ticket, updates the ticket information and severity aspect.

Configuring the Event Collector: Examples

During installation, Event Collector AVMs are created on the gateway and all units, but a single Event Collector AVM is started only on the gateway. You can configure an Event Collector to run on a unit instead, or configure multiple Event Collectors. These topics describe the supported scenarios.



Note

Deploying multiple Event Collectors does *not* increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will *not* increase to 200.

When considering which scenario is best for you, consider the following points:

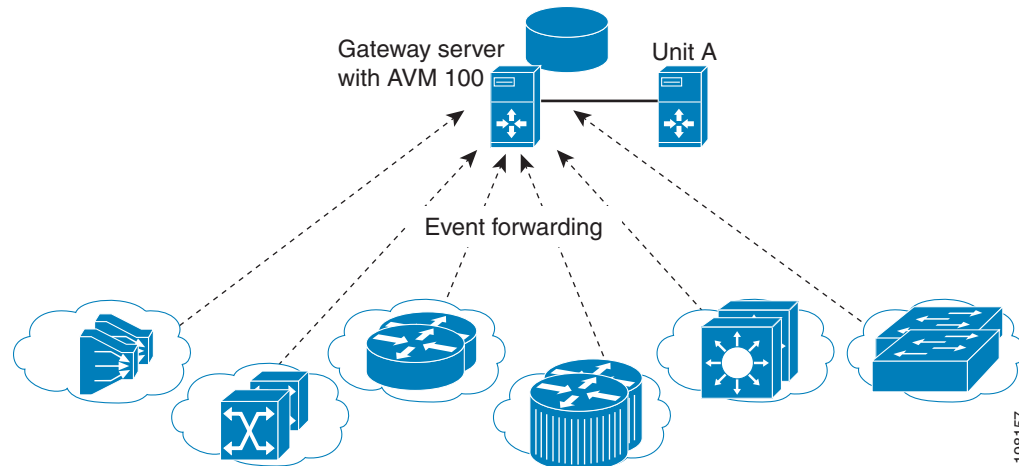
- If event archiving is disabled, the Event Collector AVM does *not* require database connectivity.
- The Event Collector on a unit in standby mode will not forward any events to the Event Archive; it will drop all events.
- AVM 25 *always* requires database connectivity. If a connection is not available, you can configure AVM 25 to use a proxy AVM 25. (See [Configuring Proxy AVM 25 for Units Not Connected to Database](#), page 14-15.)

Scenario	Appropriate for:	For an example, see:
Single Event Collector on gateway	Systems with exceptional reliability (where gateway is never expected to go down).	Figure 14-2 on page 14-7
Single Event Collector on unit	Systems where you want to localize Event Collector functionality to one unit (if the unit goes down, the system will operate but will lose the unit's functionality).	Figure 14-3 on page 14-8
Single Event Collector on unit with high availability	Systems where you want to localize Event Collector functionality to one unit (if unit goes down, the system will operate with no loss of unit functionality).	Figure 14-4 on page 14-9
Multiple Event Collectors on units	<p>Systems with either or both of the following characteristics:</p> <ul style="list-style-type: none"> • Systems with devices that have connectivity issues with the configured single Event Collector; or • Systems with a relatively high events-per-second rate that are using SNMPv3, and find it desirable to spread network event decryption and initial parsing across several machines <p>Deploying multiple Event Collectors does <i>not</i> increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database.</p> <p>For information on increasing SNMPv3 decryption capabilities and other deployment information and recommendations, contact your Cisco representative.</p>	Figure 14-5 on page 14-10

Example: Single Event Collector on Gateway Server

Figure 14-2 illustrates how events should be forwarded in a configuration where a single Event Collector is enabled on the gateway server.

Figure 14-2 Single Event Collector On Gateway Server



For this scenario, because the Event Collector AVM is enabled on the gateway server by default, all you must do is:

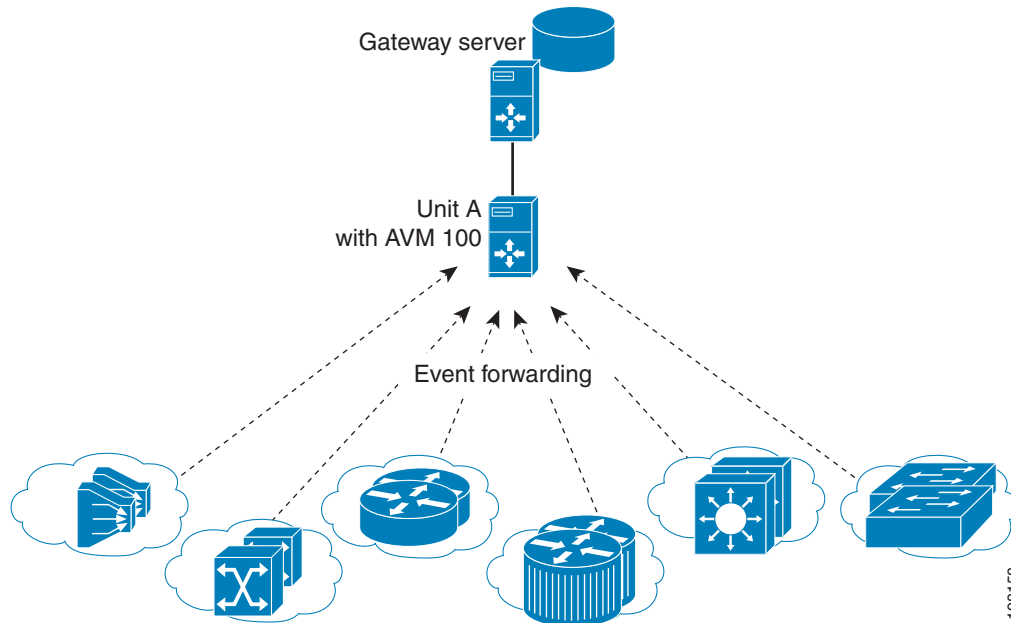
1. Configure the network elements to forward events to the gateway server.
2. Make sure all other Event Collectors are disabled. The Event Collector AVM is enabled on the gateway server by default. If you have to manually enable it, see [Enabling the Event Collector on the Gateway Server](#), page 14-11.

No other configuration changes are required. New VNEs will automatically register to this Event Collector.

Example: Single Event Collector on Unit Server (No High Availability)

Figure 14-3 illustrates how events should be forwarded in a configuration where one Event Collector is enabled on a unit server.

Figure 14-3 Single Event Collector On Unit Server



For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway server (it is enabled on the gateway server by default).
2. Configure the network elements to forward events to the unit server that will host the enabled Event Collector.
3. Start the Event Collector AVM on the unit server and make sure all other Event Collectors are disabled. See [Enabling a New Event Collector on a Unit](#), page 14-12.
4. If the unit with the running Event Collector does not have connectivity to the database, disable event archiving on the unit as described in [Disabling and Re-Enabling Event Archiving](#), page 14-16. (In addition, you should configure a proxy AVM 25 on this unit. See [Configuring Proxy AVM 25 for Units Not Connected to Database](#), page 14-15.)

No other configuration changes are required. New VNEs will automatically register to this Event Collector.

If the unit with the enabled Event Collector fails and is not operational, you must do the following:

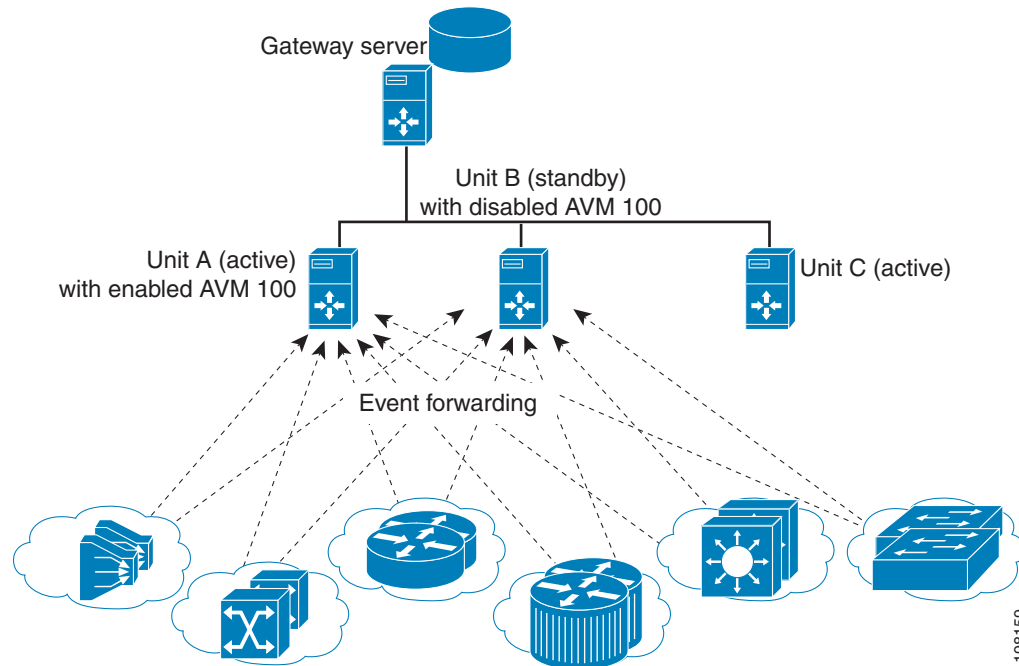
1. Repeat the previous steps on the new machine.
2. Move all AVMs to the new machine (see [Moving and Deleting AVMs](#), page 4-13). When the moved VNEs start, they will automatically register to the new Event Collector.

Example: Single Event Collector on Unit Server with High Availability

Figure 14-4 illustrates how events should be forwarded in a configuration where one Event Collector is enabled on a unit server, and the unit server is part of a protection group that contains Unit A (an active unit with an enabled Event Collector), Unit B (standby unit with disabled Event Collector), and Unit C (active unit). See [AVM 100 and Unit Server High Availability, page 16-3](#), for details about how the Event Collector operates in a unit server high availability scenario.

In Figure 14-4, devices are managed by Unit A.

Figure 14-4 Event Collector On Unit Server with High Availability



For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway (it is enabled on the gateway by default).
2. Configure and start the Event Collector AVM on the active unit as explained in [Enabling a New Event Collector on a Unit, page 14-12](#). (The Event Collector AVM on the standby unit should *not* be enabled.)
3. Configure the network elements to forward events to *both* the active and standby units.
4. If any of the units with a running Event Collector do not have connectivity to the database, disable event archiving on them as described in [Disabling and Re-Enabling Event Archiving, page 14-16](#). (In addition, you should configure a proxy AVM 25 on this unit. See [Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15](#).)

If the unit with the enabled Event Collector fails, the Event Collector on the standby unit is automatically started and the VNEs are automatically reregistered with the Event Collector on the standby unit. See [AVM 100 and Unit Server High Availability, page 16-3](#) for information on what happens if the failed unit comes back up.

Example: Multiple Event Collectors on Unit Servers (No High Availability)

Prime Network supports multiple enabled Event Collectors. The Event Collectors can be on the gateway and units, or just the units.

Figure 14-5 illustrates how events should be forwarded in a configuration with two Event Collectors enabled on different unit servers. This configuration is appropriate to a network in which devices have connectivity issues with the configured single Event Collector.

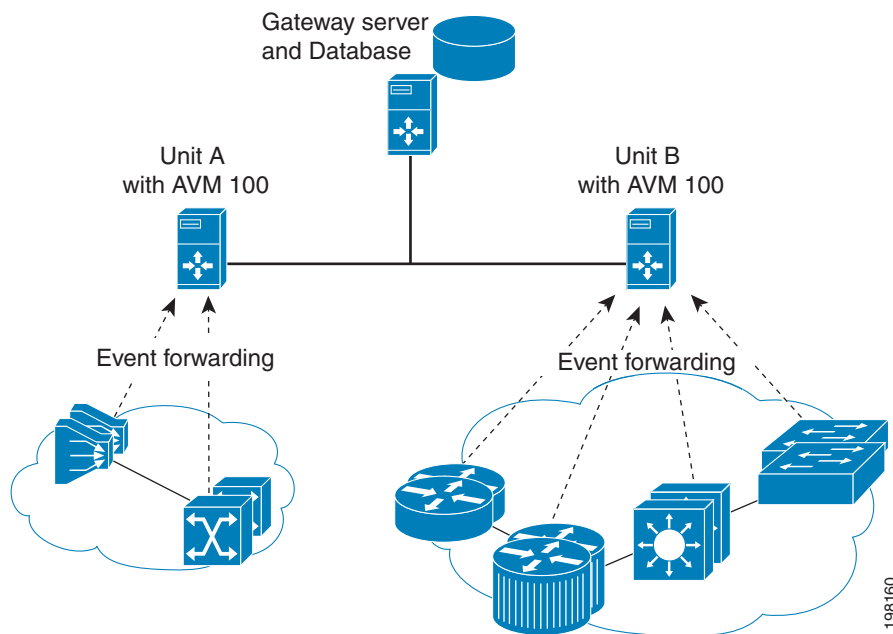
Deploying multiple Event Collectors does *not* increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will *not* increase to 200.



Note

This scenario can also increase SNMPv3 decryption capabilities. For information on this and other deployment information and recommendations, contact your Cisco representative.

Figure 14-5 Event Collector On Two Unit Servers with No Unit Server High Availability



For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway (it is enabled on the gateway by default).
2. Configure and start the Event Collectors as explained in [Enabling a New Event Collector on a Unit](#), page 14-12.
3. Configure the network elements to forward events to *one* of the units with an enabled Event Collectors.

4. If any units do not have connectivity to the database, disable event archiving and configure a proxy AVM 25 on those units. See [Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15](#).
5. For the group of VNEs you want to use the newly defined Event Collector, you must manually register the VNEs with the new Event Collector. See [Registering VNEs with a Non-Default Event Collector, page 14-15](#).

Enabling a Single Event Collector on a Gateway or a Unit

During installation, an Event Collector AVM is created on the gateway and all units, but it is started only on the gateway. By default, the enabled Event Collector has the internal address 0.0.0.0 (this address is not related to the device IP address). All new VNEs will register with the Event Collector on the gateway server.

Enabling the Event Collector on the Gateway Server

Although the Event Collector runs on the gateway by default, there may be instances where it has been stopped. If so and you need to restart it, use the following procedure.

Before You Begin

- Configure the network elements to forward traps and syslogs to the gateway server that will contain the enabled Event Collector.
- Make sure all other Event Collectors are disabled.

If no other Event Collector was enabled *after* the gateway Event Collector was stopped, do the following to restart the Event Collector:

-
- Step 1** In the All Servers branch, open the gateway branch.
 - Step 2** Right-click the Event Collector AVM and choose **Actions > Start**.
-

If an Event Collector was enabled on another unit, do the following:

-
- Step 1** Stop the Event Collector AVM on the unit.
 - Step 2** Stop the unit on which the Event Collector was enabled.
 - Step 3** Restart the gateway.
 - Step 4** Start the Event Collector AVM on the gateway.
 - Step 5** Start the unit.
-

The Event Collector will begin processing events when they are received. By default, any new VNEs will register with the Event Collector on the gateway server.

Enabling a New Event Collector on a Unit

Follow this procedure to start a single Event Collector on a unit.



Note

If an Event Collector was previously enabled and is now disabled, the new Event Collector will automatically take the internal address 0.0.0.0. (This address is not related to the device IP address.)

Before You Begin

- Configure the network elements to forward traps and syslogs to the unit that will contain the enabled Event Collector.
- If you are using unit server high availability, you must also configure the network elements to forward traps and syslogs to the standby unit.
- Make sure all other Event Collectors are disabled.

To enable the Event Collector on a unit:

Step 1 If an Event Collector was enabled at any time since the last boot, stop and restart the gateway server:

```
# cd $ANAHOME/Main
# networkctl restart
```

Step 2 In the Servers branch, open the unit branch.

Step 3 Right-click the Event Collector AVM and choose **Actions > Start**. The new Event Collector will automatically take the internal address 0.0.0.0.

By default, any new VNEs will register with the Event Collector on the unit.

Configuring and Enabling Multiple Event Collectors

Configuring a network to have two Event Collectors enabled on different unit servers is appropriate to a network in which devices have connectivity issues with the configured single Event Collector. However, deploying multiple Event Collectors does *not* increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will *not* increase to 200.

An illustration of this configuration is provided in [Example: Multiple Event Collectors on Unit Servers \(No High Availability\)](#), page 14-10.



Note

This scenario can also increase SNMPv3 decryption capabilities. For information on this and other deployment information and recommendations, contact your Cisco representative.

To configure multiple Event Collectors you must edit the registry using the **runRegTool.sh** script.

The **runRegTool.sh** script is in the directory *NETWORKHOME/Main* and uses the following format:

```
runRegTool.sh -gs 127.0.0.1 set unit-IP "vne-avm/agents/da/vne-name/trap/xidip"
event-collector-address
```

The **runRegTool.sh** script accepts the following arguments:

Argument	Description
<i>unit-IP</i>	The IP address of the machine on which the AVM resides (if the AVM resides on the gateway, this should be 127.0.0.1). This IP address is defined during installation and configuration.
<i>vne-avm</i>	The AVM on which the VNE is configured.
<i>vne-name</i>	The name of the VNE in Prime Network.
<i>event-collector-address</i>	The internal IP address of the Event Collector (internally, this is called the XIDIP of the Event Collector). This address is used for communication between the VNEs and the Event Collector and is unrelated to the device IP address. <i>event-collector-address</i> can have the following values based on how many Event Collectors are running in the system.
0.0.0.0	The default <i>event-collector-address</i> . Used when only <i>one</i> Event Collector is running on a system.
<i>unit-IP</i>	Used when configuring <i>additional</i> Event Collectors.

How To Configure Multiple Event Collectors

Complete the following procedure for each additional Event Collector that needs to be configured. Because this is a completely new Event Collector, you do not have to stop or restart any AVMs.

Before You Begin

Configure the network elements to forward traps and syslogs to the appropriate Event Collector. If you are using unit server high availability, traps and syslogs should be forwarded to both the active and standby units.

To configure multiple Event Collectors:

-
- Step 1** From the gateway, issue the following **runRegTool.sh** script to add an additional Event Collector to Prime Network:

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avm100/agents/trap/xidip" unit-IP
```

The update is automatically propagated from the gateway to the relevant units.

- Step 2** Start the Event Collector AVM on the unit with Prime Network Administration by right-clicking the AVM and choosing **Actions > Start**.

- Step 3** If you want any existing VNEs to register with an Event Collector other than the default (at 0.0.0.0), perform the instructions in [Registering VNEs with a Non-Default Event Collector, page 14-15](#).

When you add new VNEs, you must register the VNEs to the appropriate Event Collector as described in [Registering VNEs with a Non-Default Event Collector, page 14-15](#).

Example Procedure for Configuring Two Event Collectors on Two Units

This example illustrates how to configure an Event Collector to run on one unit, and a second Event Collector to run on a second unit. The configuration is as follows:

- Gateway IP address: 192.168.10.1
- Unit 1 IP address: 192.168.10.2
 - Contains AVM 100, which is an Event Collector with the address 192.168.10.2.
 - Contains AVM 200, which is an AVM that contains user-created VNEs.
- Unit 2 IP address: 192.168.10.3
 - Contains AVM 100, which is an Event Collector with the address 192.168.10.3.
 - Contains AVM 300, which is an AVM that contains user-created VNEs.

In this example, two Event Collectors are configured, one on each unit. Each Event Collector handles the events (SNMP traps and syslogs) sent from the network elements that correspond to the VNEs it manages.

After installing the gateway and the two units, configure the Event Collectors and the VNEs:

-
- Step 1** Log into the gateway as *network user* (where *network user* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of *network user* is **network39**), and change to the Main directory by entering the following command:
- ```
cd $ANAHOME/Main
```
- Step 2** Issue the following commands to configure the Event Collector addresses:
- ```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2 "avm100/agents/trap/xidip" 192.168.10.2
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.3 "avm100/agents/trap/xidip" 192.168.10.3
```
- Step 3** Issue the following commands to configure the VNEs to register to their Event Collector:
- a. For each VNE configured to receive traps and syslogs from the Event Collector (AVM 100) on Unit 1, use the following command:


```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2
"avm200/agents/da/vne-name/trap/xidip" 192.168.10.2
```
 - b. For each VNE configured to receive traps and syslogs from the Event Collector (AVM 100) on Unit 2, use the following command:


```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.3
"avm300/agents/da/vne-name/trap/xidip" 192.168.10.3
```
 - c. Restart the reconfigured VNEs.
- Step 4** Start each new Event Collector with Prime Network Administration by right-clicking the Event Collector AVM and choosing **Actions > Start**.
-

Registering VNEs with a Non-Default Event Collector

If you do not want a VNE to be registered with the default Event Collector—that is, the Event Collector that uses the internal address 0.0.0.0—you must manually change the VNE registration. (This internal address is not related to the device IP address.)



Note

Before performing the following procedure, verify that all VNEs are configured in the relevant units.

Complete the following procedure to register VNEs to an enabled Event Collector:

-
- Step 1** Choose the Event Collector that is to receive the traps and syslogs for the VNE.
- Step 2** Locate the AVM on which the VNE resides.
- Step 3** Log into the gateway as *network user* (where *network user* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of *network user* is **network39**), and change to the Main directory by entering the following command:
- ```
cd $ANAHOME/Main
```
- Step 4** Issue the following **runRegTool.sh** script (*vne-key* is the VNE name):
- ```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agents/da/vne-key/trap/ip" unit-IP
```
- The update is automatically propagated to the relevant units. For details on the command syntax, see [Example Procedure for Configuring Two Event Collectors on Two Units, page 14-14](#).
- Step 5** Reload the VNE with Prime Network Administration by right-clicking the VNE and choosing **Actions > Start**.
-

Configuring Proxy AVM 25 for Units Not Connected to Database

If a unit server does not have a direct connection to the database, you can configure another unit to be its proxy and persist event information to the Fault Database. However, because there is no proxy support for the Event Collector (AVM 100), raw events will not be saved to the Event Archive. Therefore, you should disable raw event archiving as described in [Disabling and Re-Enabling Event Archiving, page 14-16](#). If you do not disable event archiving, the log will contain errors because events are not being forwarded to VNEs nor are system events being generated.

To configure a proxy AVM 25, you must edit the registry (the *avm25.xml* file) for the unit that does not have database connectivity. The proxy unit will process the events as part of its normal event flow.

-
- Step 1** Disable event archiving on the unit that does not have a database connection. See [Disabling and Re-Enabling Event Archiving, page 14-16](#).
- Step 2** On the unit that has no database connection, edit the registry to add the proxy instructions using the following **runRegTool.sh** scripts:
- ```
runRegTool.sh -gs 127.0.0.1 add unit-IP "avm25/services/management/proxy"
runRegTool.sh -gs 127.0.0.1 set unit-IP "avm25/services/management/proxy/IP" proxy-unit-IP
```

This `runRegTool.sh` script requires the following arguments:

| Argument                   | Description                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <code>unit-IP</code>       | The IP address of the unit server that does not have a database connection.                                                            |
| <code>proxy-unit-IP</code> | The IP address of the unit server that has a database connection and will act as a proxy for the unit server at <code>unit-IP</code> . |

The following is an example:

- Unit 1 (192.168.10.2) does not have a database connection.
- Unit 2 (192.162.11.1) has a database connection and will act as a proxy for Unit 1.

To configure Unit 1 to use Unit 2 as a proxy for AVM 25, enter these commands:

```
cd $ANAHOME/Main
./runRegTool.sh -gs 127.0.0.1 add 192.168.10.2 "avm25/services/management/proxy"
./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2 "avm25/services/management/proxy/IP"
192.162.11.1
```

**Step 3** Restart the unit that has no database connectivity (in the example this would be Unit 1):

```
networkctl restart
```

(This will also restart any VNEs on Unit 1 that are using a non-default Event Collector, which is also required.)

## Disabling and Re-Enabling Event Archiving

By default, Prime Network archives all event notifications it receives from devices and saves them in the Event Archive. Events are saved according to the settings that are configured in the **Global Settings > Event Management Settings** window in the Prime Network Administration GUI client (see [Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6](#)). If you do not want to save any raw events to the Event Archive, you can disable it by using the following procedure.



### Note

If you disable this feature, the data will not be available for event-related reports.

**Step 1** Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; an example of `network user` is `network39`), and change to the Main directory by entering the following command:

```
cd $ANAHOME/Main
```

**Step 2** Issue the following command to disable event archiving:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/trap/agents/trap/netEventPersistencyEnabled" false
```



To reenable event archiving, use this command:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/trap/agents/trap/netEventPersistencyEnabled" true
```

- Step 3** Restart the Event Collector AVM from Prime Network Administration by right-clicking the AVM and choosing **Actions > Stop** and (when it is down) **Actions > Start**.
-

