



CHAPTER 10

Configuring Generic, Solaris, Linux, and Windows Application Hosts

Revised: June 19, 2007, 78-17020-01

Application hosts are simply hosts on your network that are running important applications. Many of the supported reporting devices and mitigation devices cannot be represented in MARS until the base host on which they are running is defined. Examples of such applications include CheckPoint Firewalls and all forms of web servers.

MARS provides for the definition of the following host types:

- **Generic.** Identifies no specific operating system, as well as any that are not directly supported.
- **Windows.** Identifies one of the Microsoft operating systems.
- **Solaris.** Identifies any of the Solaris family of operating systems.
- **Linux.** Identifies any of the Linux family of operating systems.

You should strive to define the application host as exactly as possible. This guideline applies to the vulnerability assessment information as well as the general settings. This detailed information helps MARS determine whether the host is susceptible to known attacks, such as those that specifically target on operating system or application/service running on the host.

This chapter contains the following sections:

- [Adding Generic Devices, page 10-1](#)
- [Sun Solaris and Linux Hosts, page 10-2](#)
- [Microsoft Windows Hosts, page 10-4](#)
- [Define Vulnerability Assessment Information, page 10-12](#)

Adding Generic Devices

The MARS can support any syslog or SNMP devices, even if they do not appear on the list of devices supported by the MARS. You can enter any syslog or SNMP device into the network topology, configure it to report data to the MARS, and query it using a free-form query. For more information on free form queries, see [To Run a Free-form Query, page 20-2](#).

Sun Solaris and Linux Hosts

To configure MARS to receive and process Solaris or Linux host log information, you must perform three tasks:

- [Configure the Solaris or Linux Host to Generate Events, page 10-2](#)
- [Configure Syslogd to Publish to the MARS Appliance, page 10-2](#)
- [Configure MARS to Receive the Solaris or Linux Host Logs, page 10-3](#)

Configure the Solaris or Linux Host to Generate Events

MARS Appliance can receive syslog information from a Linux/Solaris host. To configure the Linux/Solaris applications, you must configure the following applications to write to syslog:

- xferlog
- inetd

To configure these applications to write to the system log, follow these steps:

Step 1 xferlog (which provides transfer logging information from the FTP server)

For ftpd, add the following to `/etc/ftpd/ftppass`:

```
log transfers real,guest,anonymous inbound,outbound log syslog+xferlog
```

Step 2 inetd trace messages (which provide the authentication information for services provided using inetd)

For inetd, the line in `/etc/rc2.d/S72inetsvc` that reads:

```
/usr/sbin/inetd -s
```

needs to be changed to:

```
/usr/sbin/inetd -t -s
```

Other messages will automatically appear in the syslog and do not need to be specifically configured.

Step 3 Once you have enabled the message generation, you must configure the syslogd daemon to publish messages to the MARS Appliance. For more information, see [Configure Syslogd to Publish to the MARS Appliance, page 10-2](#).

Configure Syslogd to Publish to the MARS Appliance

Once you have enabled the correct applications to write to the system log, you must configure the syslog daemon on the Solaris or Linux host to publish syslog messages to the MARS Appliance.

To configure the Solaris or Linux host to publish syslogs to the MARS Appliance, follow these steps:

Step 1 Edit `/etc/syslog.conf` file and add the line below:

```
*.debug @MARS_hostname
```

where `MARS_hostname` is the hostname or IP address of the MARS Appliance.

Step 2 Run following commands to restart syslogd so that the changes are process:

```
/etc/init.d/syslog stop
```

`/etc/init.d/syslog start`

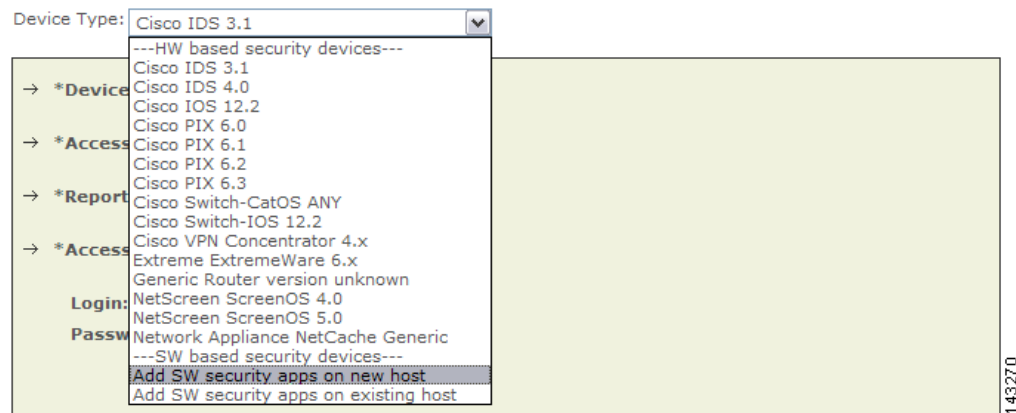
Once this line is added to the `syslog.conf` file and you have restarted `syslogd`, any messages sent to console are also sent to the MARS Appliance.

Configure MARS to Receive the Solaris or Linux Host Logs

To add a Solaris or Linux device to MARS, follow these steps:

- Step 1** Click **Admin > Security and Monitor Devices > Add**.

Figure 10-1 Adding a Solaris or Linux Device



- Step 2** From the **Device Type** list, select **Add SW Security apps on a new host**.

Figure 10-2 Identifying a Solaris or Linux Device From Which to Receive Logs

↓

General	Reporting Applications	Vulnerability Assessment Info						
<p>→ *Device Name: <input type="text"/></p> <p>→ Access IP: <input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></p> <p>→ Reporting IP: <input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></p> <p>→ Operating System: <input type="text" value="Generic"/> <input type="button" value="Logging Info"/></p> <p>→ NetBIOS Name: <input type="text"/></p> <p>→ Monitor Resource Usage: <input type="text" value="NO"/></p> <p>Enter interface information:</p> <table border="1"> <thead> <tr> <th>Name:</th> <th>IP Address:</th> <th>Network Mask:</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> ether0</td> <td><input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></td> <td><input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></td> </tr> </tbody> </table> <p><input type="button" value="Add IP/Network Mask"/></p>			Name:	IP Address:	Network Mask:	<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Name:	IP Address:	Network Mask:						
<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>						

143256

Step 3 Enter values for the following fields:

- **Device Name.** Enter the hostname for this device.
- **Reporting IP.** Enter the IP address from which the logs will be pulled.

Step 4 In the Operating System list, select either **Solaris** or **Linux** to match the operating system running on the host.

Step 5 Select **Logging Info** and select **Receive**, then click **Submit**.

Step 6 Click **Apply** to add the device.

Microsoft Windows Hosts

MARS processes data pulled from hosts running Microsoft Windows. This data includes the events found in the security event log as well as application event and system event logs. You can use one of two methods to retrieve the logs from a host running Microsoft Windows, whether it is a server or workstation version:

- You can configure MARS to pull the logs from the host.
- You can configure the host to send the log data to the MARS Appliance.

These two methods are mutually exclusive; in other words, you cannot configure both methods. Your decision in which method to use depends on how much time you can spend preparing the host, the desired load on the MARS Appliance, and how near real-time you want MARS to process the event data.

The *pull method* not only requires system resources for correlating, but also for contacting and pulling the event data from each host. It also operates in a single process, completing the pull from one device before moving to the next. As a result, the pull method may take much longer to cycle through all of the reporting devices as the number of devices grows.

The *push method* is more efficient in terms of resource utilization on the MARS Appliance and in terms of how quickly the MARS Appliance can be made aware of event data, but it requires that you install and configure the Snare Agent for Windows on the Microsoft Windows host. The Snare Agent pushes event data from the servers to MARS in near real time, when an audit event occurs, the agent sends a syslog message to MARS that details the event. It is also more efficient and timely in that each Snare Agent is able to act independently rather than being bound by a single process as with the pull method.

The following sections describe these two methods:

- [Push Method: Configure Generic Microsoft Windows Hosts, page 10-5](#)
- [Pull Method: Configure the Microsoft Windows Host, page 10-6](#)

Push Method: Configure Generic Microsoft Windows Hosts

MARS can treat hosts running Microsoft Windows as reporting devices, monitoring the event log data generated by the host. The host needs to run InterSect Alliance SNARE Agent for Windows, which captures event log data and sends it to MARS. The push method requires four steps:

1. Install the SNARE agent on the Microsoft Windows host. For more information, see [Install the SNARE Agent on the Microsoft Windows Host, page 10-5](#).
2. Configure the SNARE agent to forward event data to the MARS Appliance. For more information, see [Enable SNARE on the Microsoft Windows Host, page 10-6](#)
3. Ensure that UDP 514 traffic can pass between the hosts and the MARS Appliance.
4. Identify that host in MARS so that it can correctly parse and correlate the event data. For more information, see [Configure the MARS to Pull or Receive Windows Host Logs, page 10-9](#).

Install the SNARE Agent on the Microsoft Windows Host

To install the SNARE agent, follow these steps:

-
- Step 1** Log in to the target host using a username with proper administrative privileges.
The username must have the permission to publish audit data as well as to install new programs.
 - Step 2** Download the SNARE Agent for Windows from the following URL that corresponds to the operating system type installed on the target host:
<http://www.intersectalliance.com/projects/SnareWindows/index.html#Download>
 - Step 3** Double-click the **SnareSetup<version>.exe** file to start the install program.
 - Step 4** Click **Next**.
 - Step 5** Select the target install folder and click **Next**.
 - Step 6** Select **Normal Installation** in the Components list and click **Next**.
 - Step 7** Select the target Start menu location and click **Next**.
 - Step 8** Verify the selection options and click **Install**.

- Step 9** SNARE is installed and started on the local host. A dialog box appears, prompting you to specify whether to allow SNARE to control the EventLog configuration for the Microsoft Windows host.
- Step 10** Select **Yes** to enable SNARE to control the EventLog configuration for this Microsoft Windows host. The SNARE - Remote Event Logging for Windows user interface appears.
- Step 11** To configure the Snare agent, continue with [Enable SNARE on the Microsoft Windows Host, page 10-6](#).
-

Enable SNARE on the Microsoft Windows Host

Once you have downloaded and installed the SNARE agent on the target Microsoft Windows host, you must configure the agent to forward the correct event data in the correct format to the MARS Appliance.

To configure the SNARE agent, follow these steps:

-
- Step 1** Click **All Programs > InterSect Alliance > Snare for Windows** to run the SNARE - Remote Event Logging for Windows user interface.
- Step 2** Click **Setup > Network Configuration...**
The Network Configuration page appears.
- Step 3** Specify values for the following fields:
- **Override detected DNS Name with.** Specify the IP address or DNS name of the local host in the field.
 - **Destination Snare Server address.** Specify the IP address or the DNS name of the MARS Appliance.
- Step 4** Verify that the following options are selected:
- **Allow SNARE to automatically set audit configuration**
 - **Allow SNARE to automatically set file audit configuration**
 - **Enable SYSLOG Header**



Note Verify the syslog port is 514.

- Step 5** Click **Apply the Latest Audit Configuration** on the Network Configuration page.
- Step 6** Click **File > Close** to close SNARE - Remote Event Logging for Windows user interface.
The SNARE agent is stopped and restarted to pick up the configuration changes.
-

Pull Method: Configure the Microsoft Windows Host

As an alternative to the push method, you can configure MARS to pull event log data (security, application, and system event logs) from Microsoft Windows hosts. The pull method requires the following steps:

1. Ensure that the Windows host and MARS Appliance clocks are synchronized. It is recommend that you configure a NTP server for this purpose. For more information, see [Specify the Time Settings, page 5-10](#).

2. Select an existing or define a new user account on the Windows host that the MARS Appliance can use to pull event log records.
3. Ensure that the user account has the correct credentials. Verify that the user account belongs to the Administrator group and verify that it includes the privilege for managing and auditing security logs. For more information, see the procedure that corresponds to the operating system running on the host:
 - [Enable Windows Pulling Using a Domain User, page 10-7](#)
 - [Enable Windows Pulling from Windows NT, page 10-7](#)
 - [Enable Windows Pulling from a Windows 2000 Server, page 10-7](#)
 - [Windows Pulling from a Windows Server 2003 or Windows XP Host, page 10-8](#)
4. Configure the Windows host to generate the correct event data.
5. Identify that host in MARS so that it can correctly parse and correlate the event data. For more information, see [Configure the MARS to Pull or Receive Windows Host Logs, page 10-9](#).
6. Specify the time interval at which the event log data should be pulled from all identified host running Microsoft. For more information, see [Windows Event Log Pulling Time Interval, page 10-11](#).

Enable Windows Pulling Using a Domain User

To enable Windows pulling using a domain user (`domain\username`), for example, `CORP\syslog`, do the following on the domain controller *before* you enable Windows pulling on your client:

-
- Step 1** On the domain controller, click **Administrative Tools > Default Domain Security Policy > Security Settings > Local Policies > User Rights Management**.
 - Step 2** Grant the permission **Manage auditing and security log** to the domain user (`domain\username`).
-

Enable Windows Pulling from Windows NT

To enable MARS to pull event log data from a Windows NT host, follow these steps:

-
- Step 1** From **Start > Programs > Administrative Tools > User Manager**, in the menu bar, choose **Policies**.
 - Step 2** In the submenu, choose **User Rights**, make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.
 - Step 3** In the submenu, choose **Audit**. Configure the audit policy according to your site's security auditing policy.
-

Enable Windows Pulling from a Windows 2000 Server

When there is no Active Directory Service (ADS) server sending domain information to your Windows 2000 server, you must set this property to *Disabled* on each host from which you want the MARS Appliance to pull syslogs.

To enable MARS to pull event log data from a Windows 2000 host, follow these steps:

Step 1 Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

The Local Security Settings applet appears.

Step 2 Configure the settings under the following Local Policy groups as specified:

- Security Settings > Local Security Policy > User Rights Management

Make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.

- Security Settings > Local Security Policy > Audit Policy

Configure the audit policy according to your site's security auditing policy and ensure that all entries under Effective Setting are set to **Success, Failure**.

Windows Pulling from a Windows Server 2003 or Windows XP Host



Note

If you are selecting Microsoft Windows XP Home Edition, you must enable the Remote Procedure Call services under All Programs > Control Panel > Administrative Tools > Services. This service is enabled by default on Windows XP Professional.

To enable MARS to pull event log data from a Windows Server 2003 or Windows XP host, follow these steps:

Step 1 Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.

The Local Security Settings applet appears.

Step 2 Configure the settings under the following Local Policy groups as specified:

- Security Settings > Local Security Policy > User Rights Management

Make sure the right of **Manage auditing and security log** is granted to the user account used for pulling event log records.

- Security Settings > Local Security Policy > Audit Policy

Configure the audit policy according to your site's security auditing policy.

Step 3 To grant the pulling account the privileges to read security, application and system event logs, use the method described in the Microsoft Knowledge Base Article Q323076, at the following URL:

<http://support.microsoft.com/kb/323076/en-us>



Note

The pulling of an event log itself generates security event logs if certain events, such as **Log on/off**, are audited. We recommend you either set a default domain policy, or set the retention method for security event logs on your Windows system to be **Overwrite as needed**. Otherwise, when the log is full no new event log can be generated on the Windows system.

Example Configuration of Event Log Security Privileges on a Microsoft Windows 2003 Server

The following procedure is an example of the *Microsoft Configure Event Log Security Locally* procedure. Complete this procedure to give the pulling account the following event log privileges:

- Read security event log
- Read application event log
- Read system event log



Warning

If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft Corporation or Cisco Systems, Inc. cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

-
- Step 1** Launch the Microsoft Windows regedit program. (Enter **regedit** from the **Start > Run** menu)
- Step 2** Append `(A;;0x1;;;sid-of-the-pulling-account)` to the end of the following registry keys:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\CustomSD
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\CustomSD
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\CustomSD
- Use the Security Identifier [SID] of the pulling account to replace the variable *sid-of-the-pulling-account*. For example, if the pulling account's SID is `S-1-5-21-1801671234-2025421234-839521234-123456` and the original value of CustomSD is as follows:
- ```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)
```
- Change the CustomSD registry key as follows:
- ```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x1;;;S-1-5-21-1801671234-2025421234-839521234-123456)
```
- Step 3** Save changes and exit regedit.
-

Configure the MARS to Pull or Receive Windows Host Logs

Once you've prepared the Microsoft Windows host, you must identify that host in MARS and identify whether the push or pull method is being used on that host.

To configure the MARS Appliance to either pull or receive logs, follow these steps:

-
- Step 1** Select **Admin > Security and Monitor Devices > Add**
- Step 2** From the **Device Type** list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.
- Step 3** Enter the **Device Name** and **IP addresses** if adding a new host.
- Step 4** Select the **Operating System > Windows** from the list.

Step 5 (Optional) Enter **NetBIOS name**.

Figure 10-3 Window Log Configuration

The screenshot shows the 'Reporting Applications' tab of a configuration window. It contains several input fields and a table for interface configuration. The fields are: *Device Name (Softie III), Access IP (192.168.2.5), Reporting IP (192.168.2.5), Operating System (Windows), NetBIOS Name (netBIOS_Name), and Monitor Resource Usage (NO). A 'Logging Info' button is located next to the Operating System dropdown. Below these fields is a section titled 'Enter interface information:' which includes 'Add Interface' and 'Remove Interface/IP' buttons. A table lists the interface 'ether0' with IP Address 192.168.2.5 and Network Mask 255.255.255.255. An 'Add IP/Network Mask' button is also present.

Step 6 Click on **Logging Info** to configure OS Logging Information. New pop-up window will appear.

Step 7 From the Windows Operating System, select the correct option for either the server or workstation version:

- Microsoft Windows 2000
- Microsoft Windows 2003 (Also used for Microsoft Windows XP platforms.)
- Microsoft Windows Generic
- Microsoft Windows NT



Note

If you are selecting Microsoft Windows XP Home Edition, you must enable the Remote Procedure Call services under All Programs > Control Panel > Administrative Tools > Services.

Step 8 Select either the **Pull** or the **Receive** checkbox, based on the host configuration that you have performed.



Caution

Do not select both checkboxes. Doing so generates unpredictable results.

Step 9 If you selected the Pull method, enter values for the following fields:

- **Domain name**—Identifies the domain name to which the host belongs.
- **Host login**—Identifies the username with security audit and log permissions.
- **Host password**—Identifies that password that authenticates the username provided in the Host login field.

Step 10 Click **Submit**.

Figure 10-4 Windows Logging

OS Logging Information

Windows Operating System:	Microsoft Windows 2003
Logging mechanism:	<input checked="" type="checkbox"/> Pull <input type="checkbox"/> Receive
Domain Name:	my_domain
Host login:	username
Host password:

Step 11 Click **Submit** to save your changes.

Step 12 Add Interface IP Address and Network Mask.

Step 13 Click **Apply**.

Step 14 Click the **Vulnerability Assessment Info** link to define the host information that MARS uses to determine false positive attacks against this host. Continue with [Define Vulnerability Assessment Information](#), page 10-12.

Step 15 Click **Done** to save the changes.

Step 16 To activate the device, click **Activate**.

If you selected the pull check box in [Step 8](#), verify that a value has been specified for the interval at which which MARS pulls an event log from the host. For more information, see [Windows Event Log Pulling Time Interval](#), page 10-11.

Windows Event Log Pulling Time Interval

You can now set the interval at which MARS pulls an event log from all Microsoft Windows host that are defined as reporting devices. This feature determines how often MARS requests logs from the Windows hosts that are configured a reporting devices.



Note

If you are using SNARE to push the log data to MARS, then you do not need to enable this setting.

To configure the Windows event log pulling time interval, follow these steps:

Step 1 Click **Admin > System Parameters > Windows Event Log Pulling Time Interval**.

Windows Event Log Pulling Time Interval

Windows Event Log Pulling Time Interval: (secs)

Step 2 Enter the new time interval in seconds. The default value is 300 seconds (five minutes).

Step 3 Click **Submit**.

Define Vulnerability Assessment Information

For each host that you define in MARS, you can specify information about that host that assists MARS in assessing whether that host is vulnerable to the attacks that MARS detects. For example, you can identify the operating system running on the host, even providing the latest or nearest patch level. When an attack is detected that is targeted toward a specific operating system, then MARS can quickly determine whether the host is running the operating system that is targeted.

For hosts that are defined as the base platform of a reporting device, you should define this information as part of that device definition.

However, as MARS, it begins to add discovered hosts to the list of hosts under Management > IP Management. You should periodically review these hosts to update their information if you do not have a vulnerability assessment software device or service, such as Qualys QualysGuard, running on your network.

To specify the vulnerability assessment information for a host, follow these steps:

Step 1 To select the desired host, do one of the following:

- Select **Management > IP Management**, select the check box next to the desired host, and click **Edit**.
- Select **Admin > Security and Monitor Devices**, select the check box next to the desired host, and click **Edit**.

Step 2 Click the **Vulnerability Assessment Info** tab.

Figure 10-5 Vulnerability Assessment Info for a Host

- Step 3** Under Specify OS and patch Information, do one of the following:
- Select **Select operating system from**, and then select the operating system that matches the one running on this host from the list. Continue with [Step 4](#).
 - Select **Define new operating system**, and continue with Step [a.](#)
 - a. Enter the name of the operating system in the Name field.
 - b. Enter the version number for this operating system in the Version field.
 - c. Enter the patch level associated with the version number the Patch field.
 - d. Enter the name of manufacturer of the operating system in the Vendor field.
 - e. Click **Apply** to save the operating system definition.

Result: The new operating system definition is added to the Select operating system from list, and it is the selected option.

If you define a custom operating system, you must select **Generic** in the Operating System list on the General page of the host and click **Apply**. Otherwise, you cannot select the new operating system in the Select operating system from list.
- Step 4** To allow the information that you provided to be overridden by a vulnerability assessment service running on your network, select the **Allow Overwrite with VA** checkbox.
- Step 5** To add more detailed information about the host, continue with [Identify Network Services Running on the Host, page 10-14](#).
- Step 6** Click **Apply** to save the changes made to this host.
- Step 7** Click **Done** to close the Host page

Identify Network Services Running on the Host

By identifying the network services that are running on a host, you are specifying the types of network activities that you expect for this host. This data is helpful in eliminating expected activities that might otherwise be flagged as suspicious by MARS; for example, if you have administrative servers that run network discovery applications or perform vulnerability assessment probes at scheduled times.

To identify the network services running on a host, follow these steps:

-
- Step 1** To select the desired host, do one of the following:
- Select **Management > IP Management**, select the check box next to the desired host, and click **Edit**.
 - Select **Admin > Security and Monitor Devices**, select the check box next to the desired host, and click **Edit**.

- Step 2** Click **Add New Service** under Current running services.



Note

It may take five minutes or more for this dialog box to load. You can place the cursor over the title bar of the window that opens. This allows you to see if the window is still loading.

- Step 3** Enter as much detail on the service and its applications as you can.
- You can choose between selecting a service and defining a new service.
 - You can also choose between select an application or defining a new application.
- Step 4** Click **Submit**.
- Step 5** You can enter more services here by clicking **Add New Service**, or you can click **Submit** to continue.
- Step 6** Click **Submit** to complete the addition of the host.
-