RealSecure Server Sensor

Installation and User Guide for RealSecure Server Sensor, Expansion Pack Version

July 16, 2008

Overview

Introduction

The AIX 5.3 Expansion Pack and the AIX 6.1 Expansion Pack contain a purpose-built version of RealSecure Server Sensor (Server Sensor Lite). Server Sensor Lite is a real-time intrusion detection system that unobtrusively analyzes activity across your computer system and network.

Latest version of this document

For the latest version of this document, go to the documentation Website:

http://www.iss.net/support/documentation/all.php

In this document

This document contains the following topics:

About Server Sensor Lite

Introduction

Server Sensor Lite monitors activity on an individual host, using information in the log files of the operating system to determine whether an intruder has gained access to that host and to identify unauthorized activity on the system. Server Sensor Lite also monitors inbound and outbound network traffic for malicious content.

The sensor only identifies attacks destined for active services. Attacks destined for services that do not exist will not be caught because the system does not pass the attack traffic up the stack. This specific monitoring reduces the number of false positives on the system.

Sensor attributes

Server Sensor Lite has the following attributes:

- detects both network and system events
- detects events at the application layer
- detects events before they reach the IP stack
- monitors traffic to and from the host it is installed on

Event detection for network and system activity

The sensor monitors both network and operating system (OS) activity.

Event detection at the application layer

The sensor monitors traffic before it reaches a running application. The sensor detects sophisticated, high-level protocol-specific attacks at this level. Exploits found at this level are typically multi-packet attacks, such as the HTTP PHF attacks.

Monitoring at the application layer provides the following benefits:

- The sensor can analyze streams of data in addition to analyzing individual packets.
- The sensor is not susceptible to packet fragmentation because TCP packets are reassembled above the stack.

Event detection before reaching the IP stack

The sensor monitors network traffic as it moves through the server's kernel. The sensor watches for protocol violations, such as header violations, and other single packet events. Watching packets at this level allows the sensor to detect simple events before the packet can even enter the TCP/IP stack.

Monitoring traffic to and from one host

The sensor monitors traffic to and from one computer to determine if an intruder has gained access to that computer. Advantages to monitoring traffic to and from one computer include the following:

- The coverage is not adversely affected by switched networks because traffic is monitored at the host instead of on a network segment.
- High-traffic networks do not adversely affect the performance of the sensor because the traffic workload is distributed at the host level.

Before you install

Introduction

This topic provides information you should consider before you install Server Sensor Lite.

System requirements

For installations in non-workload partitions, global partitions, and workload partitions where the sensor was **not** installed using the sync command:

Component	Requirement
Minimum Memory	128 MB in addition to memory required by other applications
Disk Space Minimum	80 MB for the ServerSensor.pkg

Table 1: *Requirements for non-workload partitions, global partitions, and non-synchronized workload partitions*

For installations in workload partitions where the sensor was installed using a sync command:

Component	Requirement
Minimum Memory	100 MB in addition to memory required by other applications
Minimum Disk Space	22 MB for the ServerSensor.pkg

Table 2: *Requirements for synchronized workload partitions*

Detection settings

The sensor monitors the following:

- syslog (in the global and workload partitions)
- C2 audit log (in the global and workload partitions)
- network monitoring (in the global partition). As the global partition sees all system traffic, traffic in the workload partition is monitored.

Perl requirement

You must have Perl installed on the system where you will install Server Sensor Lite.

Note: Both the AIX 5.3 and the AIX 6.1 base installations include Perl 5.8.2 by default.

Installations in the trusted computing base

When installing the sensor to the trusted computing base, you cannot use a non-default installation path. This means that, for trusted computing base installations, you cannot use the installp -R installation method.

C2 audit subsystem

You must enable the C2 auditing subsystem if you want Server Sensor Lite to detect C2 audit events.

1. Log on using a superuser account, such as **`root`**.
2. Type the following command:

   ```
   audit start
   ```

Monitoring local syslog events

Before the sensor can monitor for local syslog events, you must configure the syslog.conf file to indicate the location of the syslog file you want the sensor to monitor.

1. Open the syslog configuration file, `/etc/syslog.conf`, using a text editor.

   Example: `vi /etc/syslog.conf`

2. Add the following line:

   `*.info  /path/messages_file`

   This identifies the path to your syslog file. The default path is `/var/adm/messages`.

   Example: `*.info  /var/adm/messages`

3. Type the following command to restart the syslog daemon:

   `refresh -s syslogd`

LPAR and WPAR support

Server Sensor Lite is supported in both logical partition environments and in system workload partition environments.

Workload partitions created after sensor installation

If you install Server Sensor Lite in the global partition and then, at a later time, create a new workload partition, the system will automatically synchronize Server Sensor Lite to the new workload partition.

Previewing the license agreement

The sensor installation includes a license agreement that you may want to preview before you install the sensor. You can preview the license agreement by selecting the **Preview new LICENSE agreements** option in the System Management Interface Tool (SMIT).

Installation options for Server Sensor Lite

Introduction

There are several installation options available. Use the tables in this topic to identify your installation environment, and then use the procedure listed in the Reference column to complete the installation process.

Note: You can only install one sensor on each instance of an AIX operating system.

Installation options for non-workload partition environments

If installing to an instance of the AIX operating system that is not using workload partitions, use one of the following options:

Option	Description	Reference
Preferred	Use SMIT to install the sensor. This installs the sensor to the /opt/ISS directory.	"Preferred method" on page 8
Alternate	Use the relocatable installation (installp -R) option. **Note:** This method is not supported on AIX 5.3 systems **or** on installations to the trusted computing base. This installs the sensor to an /opt/ISS subdirectory of the user-specified directory.	"Alternate method" on page 8

Table 3: *Installation options for non-workload partition environments*

Installation options for global and workload partition environments

If installing to an instance of the AIX operating system that is using workload partitions, use one of the following options

Option	Description	Reference
Preferred	Use SMIT to install the sensor to the global environment, and then use a sync command to install the sensor to the system workload partitions. This option does the following: • places the sensor files in the /opt /ISS directory of the global environment • installs the network monitoring component of the sensor in the global partition where it monitors all network traffic to and from the workload partitions • installs any writable files in the /var/ISS directory in the workload partition and symlinks read-only files from the global environment to the workload partition Because this method allows the workload partition to share files from the global partition, it reduces the installation footprint in the workload partition.	"Preferred method" on page 9

Table 4: *Installation options for global and workload partition environments*

Option	Description	Reference
Alternate	Use the relocatable installation (installp -R) option to install in both the global environment and the workload partition. **Note:** This method is not supported on AIX 5.3 systems **or** on installations to the trusted computing base. This option: • installs the sensor to an /opt/ISS subdirectory of the user-specified directory • does not allow the workload partition to share files from the global partition and, therefore, increases the installation footprint in the workload partition • allows you to specify custom installation directories	"Alternate method" on page 10

Table 4: *Installation options for global and workload partition environments (Continued)*

Installation options for installing in only a workload partition

If installing to a workload partition (but not to the global partition), use one of the following options:

Note: When you install the sensor in only the workload partition, the sensor cannot provide any network monitoring as all network monitoring is performed from the global partition.

Option	Description	Reference
Preferred	Use SMIT to install the sensor to the workload partition. **Note:** The workload partition must have a read-write /opt directory to use this option. This option places the sensor files in the /opt /ISS directory of the workload partition.	"Preferred method" on page 11
Alternate	Use the installp installation option to install the sensor in the workload partition. **Note:** The installp -R option is not supported on AIX 5.3 systems **or** on installations to the trusted computing base. This option: • places the sensor files in an /opt/ISS subdirectory of the user-specified directory • allows you to specify a custom installation directory	"Alternate method" on page 11

Table 5: *Installation options for workload partition-only environments*

Installing in non-workload partition environments

Introduction

Use one of the procedures in this topic to install the sensor if your environment does not include workload partitions.

Preferred method

1. Log in as a user with root authority.
2. Insert and mount the Expansion Pack CD-ROM.
3. Type **`smit`** to open SMIT.
4. Select **Software Installation and Maintenance→ Install and Update Software→ Install Software**.
5. Press F4 to list the available input devices or directories.
6. Select the mounted CD-ROM drive from the list.
7. Press ENTER.
8. Select **SOFTWARE to install**.
9. Press F4 to list the available software.
10. Select the ServerSensor.pkg file.
11. Press ENTER.
12. Select **ACCEPT new license agreement**.
13. Press TAB to toggle the entry field to **yes**.
14. Press ENTER. The installation program installs Server Sensor Lite in the /opt/iss/ directory.
15. Unmount the CD.

Alternate method

Note: This method is not supported on AIX 5.3 systems **or** on installations to the trusted computing base.

1. Log in as a user with root authority.
2. Type the following command to add a User Specified Install Location (USIL) to the system database:

   `mkusil -R` *`relocation_path`*
3. Type the following command to install the sensor:

   `installp -R` *`relocation_path`* **`-Y -a -d`** *`path_to_package`* **`ISSXss`**

   Note: This installs the sensor in /*`relocation_path`*/opt/ISS.

Installing in global and workload partition environments

Introduction

Use one of the procedures in this topic to install the sensor if your environment includes workload partitions and you want to install the sensor in both the global environment and the workload partition.

Preferred method

1. Log in as a user with root authority.
2. Insert and mount the Expansion Pack CD-ROM.
3. Type **`smit`** to open SMIT.
4. Select **Software Installation and Maintenance→ Install and Update Software→ Install Software**.
5. Press F4 to list the available input devices or directories.
6. Select the mounted CD-ROM drive from the list.
7. Press ENTER.
8. Select **SOFTWARE to install**.
9. Press F4 to list the available software.
10. Select the ServerSensor.pkg file.
11. Press ENTER.
12. Select **ACCEPT new license agreement**.
13. Press TAB to toggle the entry field to **yes**.
14. Press ENTER. The installation program installs Server Sensor Lite in the /opt/iss/ directory.
15. Unmount the CD.
16. Use one of the following methods to install to the workload partition:

Method	Description
syncwpar *partition_name*[1]	Executed from the global environment, this command synchronizes a specific partition with the global environment.
syncwpar -A[1]	Executed from the global environment, this command synchronizes all of the available system workload partitions with the global environment.
syncroot[1]	Executed from a workload partition, this command synchronizes the partition with the global environment.

1. This installs any writable files in the /var/ISS directory on the workload partition and creates a symlink to any read-only components, which remain in the global environment. The network monitoring component is not enabled in the workload partition; the sensor performs all network monitoring from the global partition.

Alternate method

Note: This method is not supported on AIX 5.3 systems **or** on installations to the trusted computing base.

1. Log in as a user with root authority.
2. Type the following command to add a User Specified Install Location (USIL) to the system database:

   mkusil -R *relocation_path*
3. In the global environment, type the following command to install the sensor:

   installp -R *relocation_path* **-Y -a -d** *path_to_package* **ISSXss**

   Note: This installs the sensor in /*relocation_path*/opt/ISS.
4. In the workload partition, type the following command to install the sensor:

   installp -R *relocation_path* **-Y -a -d** *path_to_package* **ISSXss**

   Note: This installs the sensor in /*relocation_path*/opt/ISS.

Installing in only a workload partition

Introduction

Use one of the procedures in this topic to install the sensor if your environment includes workload partitions but you only want to install the sensor in the workload partition.

Important: When you install in only the workload partition, the sensor does not provide network monitoring.

Preferred method

Note: You can only use this method if the /opt directory in the workload partition is read-write.

1. Log in as a user with root authority.
2. Insert and mount the Expansion Pack CD-ROM.
3. Type **`smit`** to open SMIT.
4. Select **Software Installation and Maintenance→ Install and Update Software→ Install Software**.
5. Press F4 to list the available input devices or directories.
6. Select the mounted CD-ROM drive from the list.
7. Press ENTER.
8. Select **SOFTWARE to install**.
9. Press F4 to list the available software.
10. Select the ServerSensor.pkg file.
11. Press ENTER.
12. Select **ACCEPT new license agreement**.
13. Press TAB to toggle the entry field to **yes**.
14. Press ENTER. The installation program installs Server Sensor Lite in the /opt/iss/ directory.
15. Unmount the CD.

Alternate method

Note: The installp -R methods listed here are not supported on AIX 5.3 systems **or** on installations to the trusted computing base.

- Use one of the following methods to install to the partition:

If /opt is...	Then...
read-only	1. Type the following command to add a User Specified Install Location (USIL) to the system database: **`mkusil -R`** *`relocation_path`* 2. Type the following command to install the sensor: **`installp -R`** *`relocation_path`* **`-Y -a -d`** *`package_location`* **`ISSXss`** **Note:** This installs the sensor in /*`relocation_path`*/opt/ISS.

If /opt is...	Then...
read-write	As /opt is read-write, you can specify any installation directory. To use the default installation directory (/opt/ISS), type the following: • **installp -Y -a -d** *path_to_package* **ISSXss** To use a non-default installation directory: 1. Type the following command to add a User Specified Install Location (USIL) to the system database: **mkusil -R** *relocation_path* 2. Type the following command to install the sensor: **installp -R** *relocation_path* **-Y -a -d** *package_location* **ISSXss** **Note:** This installs the sensor in /*relocation_path*/opt/ISS.

After you install

Introduction

This topic provides information about your system following the installation of Server Sensor Lite.

Processes related to the sensor

After the installation completes, the following additional processes will be running on the system:

- issCSF
- tclproc
- issDaemon

Default policy

After the installation completes, the sensor will be running with the Low policy applied.

Reference: See "Configuring the policy level" on page 14.

Configuring the policy level

Introduction

Policies determine what types of events Server Sensor Lite monitors for. The sensor detects suspicious activity or attacks on your system based on the policy that is applied.

Available policies

Server Sensor Lite comes with preconfigured policies that provide three levels of detection.

Policy	Description
Low	Monitors for certain High risk operating system events and High risk network attack events, based on recommendations from the X-Force research and development team.
Medium	Monitors for certain High and Medium risk operating system events and High and Medium risk network attack events, based on recommendations from the X-Force research and development team.
High	Monitors for certain High, Medium, and Low risk operating system events and High, Medium, and Low risk network attack events, based on recommendations from the X-Force research and development team.

Table 6: *Levels of detection provided by policies*

Definition of risk levels

The following list defines the risk levels mentioned in Table 6:

- High risk events are events that allow immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges.
- Medium risk events are events that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components.
- Low risk events are events that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not to directly gain unauthorized access.

Setting the policy level

1. Select **Security & Users→RealSecure Server Sensor→Set Policy Level**.
2. Select one of the following:
   - **Apply Low Policy**
   - **Apply Medium Policy**
   - **Apply High Policy**
3. Restart the sensor. The sensor applies the selected policy.

   Reference: See "Starting and stopping the sensor" on page 21.

Viewing the current policy level

1. Select **Security & Users→RealSecure Server Sensor**
2. Select **Show Current Policy Level**. The current policy level is displayed in SMIT.

Viewing detected events

Introduction

When Server Sensor Lite detects suspicious activity or an attack, it logs details about the event. You can view the details of the event to help you determine the threat the event poses to your system. View event information in the following formats:

- summary information about several events
- detailed information about a specific event

About the log

The sensor logs event information in the SensorEventLog file, which is located in the directory where the sensor is installed.

The sensor logs 24 hours worth of events to the log file and then rotates to a new log file named **`SensorEventLog.`***`date`*, where *`date`* is the date the log was created. On the eighth day of logging, the sensor deletes the oldest log file.

Viewing summary information for several events

1. Select **Security & Users→RealSecure Server Sensor→Display Security Events**.
2. Select **Multiple Security Events - Summary View**.
3. In the **[Entry Fields]** field of the **Match Security Events With** option, do one of the following:
   - to view all events, press ENTER
   - to view a subset of events, specify the string that should be present in the event to include it in the search results

     Note: You can use regular expressions to define the string.

   The sensor displays events based on the specified criteria.

   Tip: If you want to see more detail about a specific event, note the record number from the **Rec** column, and then see "Viewing details of a specific event" below.

Event summary information

The following table describes the output from a summary view query:

Column	Description
Rec	Specifies the log record number for this event. **Note:** Use the procedure "Viewing details of a specific event" on page 16 and this number to view the details of an event.
Name	Indicates the name of the detected event. **Tip:** Use the procedure "Searching the X-Force database" on page 18 and this name to get more information about this type of event.
Time	Specifies the date and time the event was detected.
Address	Indicates the IP address of the system that is the source of the event. If the sensor cannot determine the source address, it lists the address of the system the attack was destined for; if the sensor cannot determine the destination address, it lists the sensor address.
User	Indicates the user name of the user logged in at the time of the attack.

Table 7: *Summary view field descriptions*

Viewing details of a specific event

1. Select **Security & Users→RealSecure Server Sensor→Display Security Events**.
2. Select **Single Security Event - Detail View**.
3. In the **[Entry Fields]** field of the **Security Event Record Number** option, type the record number for the event you want to see the details of.

   Tip: Determine the record number for an event from the **Rec** column of the output from the **Multiple Security Events - Summary View** query.

Event detail information

The information logged by the sensor varies depending on the type of event the sensor has detected, but the following table describes some of the commonly logged fields:

Field	Description
AlertFormatVersion	An internal number that describes the format of the data. You can safely ignore this information.
AlertNameType	An internal enumeration that represents the category of the event. You can safely ignore this information.
AlertName	Name assigned to the event by the X-Force research and development team.
AlertDateTime	Date and time that the sensor detected the event.
LocalTimezoneOffset	Local time zone offset of the sensor in seconds from UTC (Coordinated Universal Time). Use this value along with the AlertDateTime to reconstruct the local time at the sensor where the event occurred. This value will increment by 60*60 (1800) for every hour west of the meridian to the location of the sensor.
AlertTimePrecision	A number that augments AlertDateTime with additional sub-second precision time information. This field contains the time offset in nanosecond (10E-9) units.
AlertTimeSequenceID	A number that represents how many times an identical event has been detected in a one second period. This number is set to one for the first instance of the event, and increases for each successive instance of the event that occurs during the same second.
AlertID	MD5 hash of the contents of the event data record. This provides a unique key for each record and an integrity seal on the record.
SensorAddress	Location of the sensor within the network. This is usually the IP address of the sensor.
SensorName	An identifier for the sensor. **Note:** The name for all Server Sensor Lite sensors is server_sensor_1.
ProductID	Type of sensor that detected the event. **Note:** For all Server Sensor Lite sensors, this will be 35.

Table 8: *Detail view field descriptions*

Field	Description
AlertType	Classifies the type of data contained in the event. Some alert types include the following: 101 SuspiciousTCP 102 SuspiciousUDP 103 SuspiciousICMP 104 SuspiciousARP 105 SuspiciousNetworkActivity 203 HostIDSLoginEvent 204 HostIDSUserNormalActivity 205 HostIDSUserAbnormalActivity 206 HostIDSAdminNormalActivity 207 HostIDSAdminAbnormalActivity 208 HostIDSResourceShortage 209 HostIDSSecurityEvent
AlertPriority	Number that ranks the priority of this event, where 1 is a high priority.
AlertFlags	Flag used for miscellaneous properties of this event. **Note:** For most events, this will be 1, which indicates the event data must be stored by the sensor.
ResponseList	Lists the response the sensor takes for this event. **Note:** For Server Sensor Lite, this will always be DISPLAY.
SystemAgent	Name of the system where the sensor is installed.
C2 Event	Type of C2 audit event detected by the sensor.
UserName	Name of the user account, the group account, or the system account.
RealUserName	Real name of the user, if the sensor can determine this information.
PID	Number used to uniquely identify a process.
PPID	Number used to identify the parent process.
File Name	Name of the file affected by this event.
SourceAddress	IP address of the source of the event. If the sensor cannot determine the source address, it lists the destination address as the source of the event. If the sensor cannot determine the destination address, it lists the sensor address as the source of the event.
DestinationAddress	IP address of the target/destination of the event. If the sensor cannot determine the destination address, it lists the source address as the target/destination of the event. If the sensor cannot determine the source address, it lists the source address as the target/destination of the event.
AttackOrigin	Represents the origin of the attack. **Unknown**—sensor cannot determine where the attack originates from **IPAdr: xxx.xxx.xxx.xxx**—IP address of the origin **Local**—the attack originated from the host system

Table 8: *Detail view field descriptions (Continued)*

Understanding detected events

Introduction

When the sensor detects an event, it logs information about the event so that you can review the event details. The information the sensor logs may be enough for you to determine the risk the event poses to your system, however, you can find more information about an event by consulting the X-Force research and development team's database of vulnerabilities.

Getting more information about an event

The X-Force research and development vulnerability database provides additional information about events detected on your system. This information can help you better understand potential threats to your system and minimize system downtime and data recovery costs.

Searching the X-Force database

1. Note the event name reported by the sensor.
2. Open the following Website:

   http://xforce.iss.net/
3. In the **X-Force Database Search** section, type the event name as reported by the sensor.
4. Click **Go**.

Understanding X-Force database entries

The following table describes the sections within each database entry:

Section	Description
Name	Tag name given to the event. The tag name is based on keywords that relate to the security issue, and typically includes the affected item and other distinguishing characteristics.
X-Force ID	A number used to uniquely identify the security issue.
Risk	The X-Force research and development team assigns risk levels to each security issue to describe the extent of damage that it could cause. There are three possible risk levels: **High**—Security issues that allow immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges. **Medium**—Security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. **Low**—Security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access.
Description	Detailed description of how the security issue has compromised your system.
Platforms affected	Lists all platforms known to be affected by this security issue.
Remedy	Identifies actions you can take to mitigate or eliminate the threat posed by this security issue.

Table 9: *Event information available from the X-Force database*

Section	Description
Consequences	Describes the threat posed to your system by a particular security issue. Consequences are listed from most severe to least severe. **Gain Access**—An attacker can obtain local and/or remote access. **Gain Privileges**—Privileges can be gained on the local system. **Bypass Security**—An attacker can bypass, change, or disable security mechanisms. **File Manipulation**—An attacker can create, delete, read, modify, corrupt, or overwrite files. **Data Manipulation**—An attacker can modify or corrupt data streams. **Obtain Information**—An attacker can obtain information such as file and path names, source code, passwords, banners, or server configuration details. **Denial of Service**—An attacker can crash or hang a service or system or can take down a network. **Configuration**—A system utility was installed or executed with incorrect or insecure setup parameters or in the wrong place. **Informational**—Incidental data that does not correlate with more severe categories. **Other**—Used when none of the other consequences apply. **None**—Used for non-security issues that don't have significant effects.
References	Provides links to supporting or additional information about the security issue. References include a brief description of the reference, the exact title (including any spelling errors made by the author), and the URL or Web address to the reference. **Note:** Due to the nature of the Internet, reference links may sometimes become outdated.
Reported	Identifies the earliest documented public disclosure that the X-Force research and development team can locate for this security issue. The reported date may not be available for audit or product-related auditing issues.

Table 9: *Event information available from the X-Force database (Continued)*

Exporting event data

Introduction

You can export event data from the sensor if, for example, you need to archive event information or if you need to create event reports for other members of your team.

Event log format

The sensor event log stores event information in a comma-separated values (.csv) file format, using one line for each event.

Exporting data

1. Copy the contents of the log file from:

   /*installation_directory*/server-sensor_1/SensorEventLog.*date*

2. Open the application you want to import the data to, such as Microsoft® Excel.
3. Use the options available in the application to paste or import the data.

Starting and stopping the sensor

Introduction

There are certain times when you may need to stop, start, or restart the sensor. For example, whenever you change the policy level, you will need to restart the sensor for the new policy level to take effect.

Start the sensor

1. Select **Security & Users→RealSecure Server Sensor**.
2. Select **Start RealSecure Server Sensor**. SMIT displays the status of the command.

Stop the sensor

1. Select **Security & Users→RealSecure Server Sensor**.
2. Select **Stop RealSecure Server Sensor**. SMIT displays the status of the command.

Restart the sensor

1. Select **Security & Users→RealSecure Server Sensor**.
2. Select **Restart RealSecure Server Sensor**. SMIT displays the status of the command.

Uninstalling the sensor

Introduction

This topic provides information about uninstalling a sensor.

Consideration

If, when you installed the sensor, you synchronized the installation from the global environment to a workload partition, you must not uninstall the sensor from the global environment without first uninstalling the sensor from the workload partition. As the workload partition shares files from the global environment, uninstalling the sensor from only the global environment removes files needed by the sensor in the workload partition.

Uninstalling the sensor

1. Log in using a superuser account, such as **`root`**.
2. Do one of the following:
   - To uninstall from the /opt/ISS directory, type the following command:

     `# installp -u ISSXss`

     Note: Use this option for all installations that were not relocated to an alternate directory.
   - To uninstall from a custom location, type the following command:

     `#installp -R` *`custom_path`* **`-u ISSXss`**
3. If the C2 audit feature was enabled when you uninstalled the sensor, you must restart the feature to completely uninstall the sensor.

Remove the installation package

Manually remove the installation package, `ServerSensor.pkg file`.

System restoration

Upon uninstallation of the sensor:

- the syslog is restored
- changes to the audit settings are reversed
- the kernel driver is removed
- the inittab is restored

Upgrading to RealSecure Server Sensor

Introduction

The Server Sensor Lite package offers a subset of the features provided by RealSecure Server Sensor. While Server Sensor Lite offers intrusion detection capabilities, RealSecure Server Sensor offers intrusion prevention capabilities that can protect your server against malicious activity.

Additional capabilities

In addition to providing an intrusion prevention system (IPS), RealSecure Server Sensor also offers:

- an integrated firewall
- customizable policies
- log auditing
- centralized management
- security content updates
- product updates
- technical support

Upgrading

If you are interested in upgrading to RealSecure Server Sensor, please contact your sales representative.