Chapter 97. Linux

IBM QRadar supports the a range of Linux DSMs.

Linux DHCP

The Linux DHCP Server DSM for IBM QRadar accepts DHCP events using syslog.

QRadar records all relevant events from a Linux DHCP Server. Before you configure QRadar to integrate with a Linux DHCP Server, you must configure syslog within your Linux DHCP Server to forward syslog events to QRadar.

For more information on configuring your Linux DHCP Server, consult the man pages or associated documentation for your DHCP daemon.

Syslog log source parameters for Linux DHCP

If QRadar does not automatically detect the log source, add a Linux DHCP log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Linux DHCP servers:

Table 549. Syslog log source parameters for the Linux DHCP DSM

Parameter	Value
Log Source type	Linux DHCP Server
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Linux DHCP Server.

Related tasks

Adding a log source

Linux IPtables

The Linux IPtables DSM for IBM QRadar accepts firewall IPtables events by using syslog.

QRadar records all relevant from Linux IPtables where the syslog event contains any of the following words: Accept, Drop, Deny, or Reject. Creating a customized log prefix in the event payload enables QRadar to easily identify IPtables behavior.

Configuring IPtables

IPtables is a powerful tool, which is used to create rules on the Linux kernel firewall for routing traffic.

About this task

To configure IPtables, you must examine the existing rules, modify the rule to log the event, and assign a log identifier to your IPtables rule that can be identified by IBM QRadar. This process is used to determine which rules are logged by QRadar. QRadar includes any logged events that include the words: accept, drop, reject, or deny in the event payload.

Procedure

1. Using SSH, log in to your Linux Server as a root user.
2. Edit the IPtables file in the following directory:

   `/etc/iptables.conf`

   Note: The file that contains the IPtables rules can vary according to the specific Linux operating system you are configuring. For example, a system using Red Hat Enterprise has the file in the `/etc/sysconfig/iptables` directory. Consult your *Linux operating system documentation* for more information about configuring IPtables.
3. Review the file to determine the IPtables rule you want to log.

   For example, if you want to log the rule that is defined by the entry, use:

   `-A INPUT -i eth0 --dport 31337 -j DROP`
4. Insert a matching rule immediately before each rule you want to log:

   `-A INPUT -i eth0 --dport 31337 -j DROP -A INPUT -i eth0 --dport 31337 -j DROP`
5. Update the target of the new rule to LOG for each rule you want to log,For example:

   `-A INPUT -i eth0 --dport 31337 -j LOG -A INPUT -i eth0 --dport 31337 -j DROP`
6. Set the log level of the LOG target to a SYSLOG priority level, such as info or notice:

   `-A INPUT -i eth0 --dport 31337 -j LOG --log-level info -A INPUT -i eth0 --dport 31337 -j DROP`
7. Configure a log prefix to identify the rule behavior. Set the log prefix parameter to :

   `Q1Target=<rule>`

   Where <*rule*> is one of the following: **`fw_accept`**, **`fw_drop`**, **`fw_reject`**, or **`fw_deny`**.

   For example, if the rule that is logged by the firewall targets dropped events, the log prefix setting is:

   `Q1Target=fw_drop`

   ```
   -A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-prefix
    "Q1Target=fw_drop " -A INPUT -i eth0 --dport 31337 -j DROP
   ```

   Note: You must have a trailing space before the closing quotation mark.
8. Save and exit the file.
9. Restart IPtables using the following command:

   `/etc/init.d/iptables restart`
10. Open the `syslog.conf` file.
11. Add the following line:

    `kern.<log level>@<IP address>`

    Where:

    - <*log level*> is the previously set log level.
    - <*IP address*> is the IP address of QRadar.
12. Save and exit the file.
13. Restart the syslog daemon by using the following command:

    `/etc/init.d/syslog restart`

    After the syslog daemon restarts, events are forwarded to QRadar. IPtable events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

Syslog log source parameters for Linux IPtables

If QRadar does not automatically detect the log source, add a Linux IPtables log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Linux IPtables firewalls:

Table 550. Syslog log source parameters for the Linux IPtables DSM

Parameter	Value
Log Source type	Linux IPtables Firewall
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Linux IPtables firewall.

Related tasks

Adding a log source

Linux OS

The Linux OS DSM for IBM QRadar records Linux operating system events and forwards the events using syslog or syslog-ng.

If you are using syslog on a UNIX host, upgrade the standard syslog to a more recent version, such as, syslog-ng.

Note: Do not run both syslog and syslog-ng at the same time.

To integrate Linux OS with QRadar, select one of the following syslog configurations for event collection:

- "Configuring syslog on Linux OS" on page 834
- "Configuring syslog-ng on Linux OS" on page 834

You can also configure your Linux operating system to send audit logs to QRadar. For more information, see "Configuring Linux OS to send audit logs" on page 835.

Supported event types

The Linux OS DSM supports the following event types:

- cron
- HTTPS
- FTP
- NTP
- Simple Authentication Security Layer (SASL)
- SMTP
- SNMP
- SSH
- Switch User (SU)
- Pluggable Authentication Module (PAM) events.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring syslog on Linux OS

Configuring Linux OS to forward events by using the syslog protocol.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog.conf` file and add the following facility information:

```
authpriv.*@<ip_address>
```

   where:

   <ip_address> is the IP address of IBM QRadar.
3. Save the file.
4. Restart syslog by typing the following command:

   `service syslog restart`
5. Log in to the QRadar Console.
6. Add a Linux OS log source on the QRadar Console.

   For more information about syslog, see the Linux documentation (https://www.linux.com/what-is-linux/).

Configuring syslog-ng on Linux OS

If you are using syslog on a UNIX host to forward events, upgrade the standard syslog to syslog-ng, which is a more recent version.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog-ng/syslog-ng.conf` file and add the following facility information:

```
source qr_source {
    internal();
    system();
};
filter qr_filter {
    facility(auth, authpriv);
};
destination qr_destination {
    tcp("<qradar_ip_address>" port(514));
};
log{
    source(qr_source);
    filter(qr_filter);
    destination(qr_destination);
};
```

   where:

   <qradar_ip_address> is the IP address of IBM QRadar.
3. Save the file.
4. Restart syslog-ng by typing the following command:

   `service syslog-ng restart`
5. Log in to the QRadar Console.
6. Add a Linux OS log source on the QRadar Console.

   For more information about syslog-ng, see the Linux documentation (https://www.linux.com/what-is-linux/).

Related tasks

"Adding a log source" on page 5

Configuring Linux OS to send audit logs

Configure Linux OS to send audit logs to QRadar.

About this task

This task applies to Red Hat® Enterprise Linux V6 operating systems.

If you use a SUSE, Debian, or Ubuntu operating system, see your vendor documentation for specific steps for your operating system.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Type the following command:

   yum install audit service auditd start chkconfig auditd on
3. Open the `/etc/audisp/plugins.d/syslog.conf` file and verify that the parameters match the following values:

   `active = yes direction = out path = builtin_syslog type = builtin args = LOG_LOCAL6 format = string`
4. Open the `/etc/rsyslog.conf` file and add the following line at the end of the file:

   ```
   local6.* @@<QRadar_Collector_IP_address>
   ```
5. Type the following commands:

   service auditd restart

   service syslog restart
6. Log in to the QRadar Console.
7. Add a Linux OS log source on the QRadar Console.

Related tasks

"Adding a log source" on page 5

Linux OS Sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Linux OS sample event messages when you use the syslog protocol

Sample 1: The following sample event message shows a PAM authentication failure for a user.

```
<118>Jul 7 15:54:13 kernel: Jul 7 15:54:13 gnu.linuxserver.test sshd[708]: error: PAM:
 authentication error  for  root  from  172.16.197.55
```

Table 551. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	authentication error
Source IP	172.16.197.55
Username	root

Sample 2: The following sample event message show that an incorrect or failed password was received from an invalid user.

```
<38>2015-06-24T14:15:51Z sshd[12239959]:  Failed password  for invalid user  test  from
 192.168.8.75  port  57436  ssh2
```

Table 552. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	Failed password
Source IP	192.168.8.75
Source Port	57436
Username	test

Chapter 98. LOGbinder

Configure your LOGbinder system to send event logs to IBM QRadar.

The following LOGbinder systems are supported:

- LOGbinder EX event collection from Microsoft Exchange Server.
- LOGbinder SP event collection from Microsoft SharePoint.
- LOGbinder SQL event collection from Microsoft SQL Server.

LOGbinder EX event collection from Microsoft Exchange Server

The IBM QRadar DSM for Microsoft Exchange Server can collect LOGbinder EX V2.0 events.

The following table identifies the specifications for the Microsoft Exchange Server DSM when the log source is configured to collect LOGbinder EX events:

Table 553. LOGbinder for Microsoft Exchange Server

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	LOGbinder EX V2.0
Protocol type	Syslog LEEF
QRadar recorded event types	Admin Mailbox
Automatically discovered?	Yes
Included identity?	No
More information	Microsoft Exchange website (http://www.office.microsoft.com/en-us/exchange/)

The Microsoft Exchange Server DSM can collect other types of events. For more information on how to configure for other Microsoft Exchange Server event formats, see the Microsoft Exchange Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft Exchange Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs:
   - DSMCommon RPM
   - Microsoft Exchange Server DSM RPM
2. Configure your LOGbinder EX system to send Microsoft Exchange Server event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft Exchange Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder EX event collection: