7.8.7 Remote Logging Facts

Sending log message to a remote server increases security for log files and centralizes log file locations.

To centralize logging for Linux hosts, complete the following:

- On the logging host where log files will be stored, complete the following:
  1. In the **/etc/sysconfig/rsyslog** file, set the **SYSLOGD_OPTIONS** parameter to a value of **-c 2 -r**.

     On some older distributions, you must set the value of the **SYSLOGD_PARAMS** parameter to **-r** in the **/etc/sysconfig/syslog** file.

  2. In the **/etc/rsyslog.conf** file, make the following changes:
     - Under **Provides UDP syslog reception**, un-comment the following lines:
       - **$ModLoad imudp.so**
       - **$UDPServerRun 514**
     - Under **Provides TCP syslog reception**, un-comment the following lines:
       - **$ModLoad imtcp.so**
       - **$InputTCPServerRun 514**
  3. Ensure UDP port 514 is open in the firewall.
  4. Restart the rsyslog daemon.
- On the clients that will send logging messages to the logging host, complete the following:
  1. In the **/etc/rsyslog.conf** file, add the following line: ***.* @[IP_address_of_logging_host]:RSYSLOG_TraditionalFileFormat**
  2. Restart the rsyslog daemon.

On Windows, use *event subscriptions* to collect events from multiple computers on one computer. When you create an event subscription, events are sent from a *source*, or *forwarder*, computer to the *collector* computer. The source computer is the computer where the event is generated. The collector computer is the computer where the events are sent.

Be aware of the following when implementing event forwarding and event subscription:

- Events are forwarded to a collector computer, where they can be manipulated in the event logs like any other log.
- Event forwarding allows you to:
  - Establish the criteria for identifying events to be forwarded.
  - Specify the log files where the events are stored on the collector.
- Event forwarding uses HTTP to transfer the event logs from the source to the collector.
  - HTTPS can be used instead of HTTP to ensure secure event log transmission.
  - The use of HTTP or HTTPS makes setup relatively easy because most firewalls are already configured for HTTP and HTTPS traffic.
- You must configure both the source and collector computers for event subscriptions. Configuration tasks include:
  - On the source and collector computers, start Windows Remote Management service.
  - On the collector computer, start the Windows Event Collector service.
  - On the source computers, configure a Windows Firewall exception for HTTP or HTTPS.

Event forwarding is implemented in one of two ways, collector-initiated subscriptions or source-initiated subscriptions. The subscription type determines specific configurations for each computer:

Subscription Type	Description
Collector-Initiated	In collector-initiated subscriptions, a collector computer sends a message to the source computer requesting the event logs. This requires that manual configuration settings be made on each source computer. Therefore, use this subscription type if you have a limited number of source computers that will forward events. To configure the collector-initiated subscription type: 1. On the source computer, run the **winrm qc -q** command to initiate the Windows Remote Management service. 2. On the source computer, add the collector computer account to the local Event Log Readers group. You must also add a user account with administrative privileges to the Event Log Readers group. 3. On the collector computer, run the **wecutil qc** command to run Windows Event Collector Service. You must also run **winrm qc** on the collector computer if you want to use delivery optimization options other than the defaults.
Source-Initiated	For source-initiated subscriptions, the source computer initiates the transfer to the collector computer. This type is most efficient for environments that have a large number of source computers. Efficiency is increased if the source computers are managed using Group Policy.

	Be aware of the following before configuring the source computer-initiated subscription type: 1. On the source computer, run the **winrm qc -q** command to start the Windows Remote Management service. 2. On the source computer, configure and enable the Event Forwarding policy through Group Policy or the local security policy and specify the collector computer's FQDN. 3. On the collector computer, run the **winrm qc -q** command to start the Windows Remote Management service. 4. On the collector computer, run the **wecutil qc /q** command to start Windows Event Collector Service. 5. In Active Directory or on the collector computer, add the source computers to a computer group.

After the source and collector are configured with the above services running, it is time to configure Event Subscriptions. The subscriptions are used for transferring the events from the source computer to the collector computer. Be aware of the following when configuring Event Subscriptions:

- For source-initiated subscriptions, you can configure a subscription without defining the event source computers on the collector. To do this, you use Group Policies to configure the source computers to forward events to the collector computer.

  For collector-initiated subscriptions, you must manually define all of the source computer names in the event subscriptions.

- You can use the Advanced Subscription setting to configure the different types of delivery for event subscriptions:

Option	Description
Normal	By default, normal delivery uses collector-initiated event forwarding. This type of delivery: ▪ Batches five items at a time. ▪ Sets a batch timeout of 15 minutes. ▪ Is recommended unless you need tight control over bandwidth or if you need forwarded events delivered as quickly as possible.
Minimized Bandwidth	By default, this option uses source-initiated event forwarding. This type of delivery: ▪ Sends events to the collector on a regular basis. ▪ Sets a batch timeout of six hours. ▪ Sets a heartbeat interval of six hours. Use this option to control the use of bandwidth for event delivery.
Minimized Latency	By default, this option uses source-initiated event forwarding and sets a batch timeout of 30 seconds. Use this option to ensure that events are quickly forwarded.
Custom	The Custom option is available if you are using Event Viewer to manage an event that was created by the Windows Event Collector Service. You cannot use Event Viewer to create or manage custom event delivery. If the custom option is available, the subscription is using delivery settings that do not correspond to those supported by Event Viewer.

- You can use one of the following options for the service account that will be used by the subscription:
  - Use the default machine account
  - Use a specific user service account

  Either type of account must be a member of the source computer's Event Log Readers group, which is the most secure choice, or a member of the local Administrators group.

- By default, events received from source computers are saved in the Forwarded Events log.
- If a filter is not defined, all events are collected.
- After you have created the subscription:
  - Use the Runtime Status link to check communication with the remote servers.
  - Delete and recreate the subscription if you need to change the subscription type.
- Supported Windows versions are listed below.

Subscription Type	Supported Windows Versions
Collector Computer	The following Windows versions support collector computers: ▪ Windows Server 2003 R2 ▪ Windows Server 2008 R0 or R2 ▪ Windows Server 2012 ▪ Windows Server 2016 ▪ Windows Vista ▪ Windows 8 or 8.1 ▪ Windows 10
Source Computer	The following Windows versions support source computers:

	▪ Windows XP with SP2 ▪ Windows Server 2003 with SP1 ▪ Windows Server 2003 R2 ▪ Windows Server 2008 R0 or R2 ▪ Windows Vista ▪ Windows 8 or 8.1 ▪ Windows 10