12.4.4 Windows Event Subscriptions Facts

Use Event Subscriptions to collect events from multiple computers and store the events on one computer.

This lesson covers the following topics:

- Process
- Subscription types
- Event subscription configuration

Process

When you create an event subscription, events are sent from a source (also called 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. Events forwarded to a collector computer 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 file the forwarded events are stored in on the collector.

Be aware of the following processes when implementing event forwarding and subscriptions:

Process	Description
Setup	Event forwarding uses HTTP to transfer the events from the source to the collector. - You can use HTTPS instead of HTTP to secure the transmission. - HTTP or HTTPS makes setup relatively easy because most firewalls are already configured for HTTP and HTTPS traffic.
Configuration	You must configure both the source and collector computers for event forwarding: - 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.
Implementation	Event forwarding is implemented in one of two ways: - Collector-initiated subscriptions - Source-initiated subscriptions

Subscription Types

The type of subscription determines the specific tasks required to configure event forwarding, as explained in the following table.

Subscription Type	Description

Collector-initiated	In collector-initiated subscriptions, a collector computer sends to the source computer a message requesting the event logs. Collector-initiated subscriptions require that manual configuration settings be made on each source computer. Accordingly, use this type of subscription only if you have a limited number of source computers that forward events. To prepare source computers to use collector-initiated subscriptions, take following steps: 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. It will use delivery optimization options other than the default.
Source-initiated	For source-initiated subscriptions, the source computer initiates the transfer to the collector computer. This type of subscription is most efficient in environments with a large number of source computers. To increase efficiency, you can use Group Policy to automatically push event subscription configuration settings to the source computers. To prepare source computers to use source-initiated subscriptions: 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. 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.

Event Subscription Configuration

After the source and collector have been properly prepared, the next step is to configure event subscriptions. The subscriptions are used to transfer events from the source computer to the collector computer. Be aware of the following when configuring event subscriptions:

Area	Description
Source-initiated subscriptions	For source-initiated subscriptions, you configure event forwarding using the Configure target Subscription Manager Group Policy setting under Computer Configuration > Administrative Settings > Windows Components > Event Forwarding. This setting configures the source computers to forward events to the specified collector computer.

	For collector-initiated subscriptions, you must manually define each source computer name in the event subscription.
Subscription configuration	On the collector, you configure a subscription in Event Viewer. You must specify: - A subscription name. - The destination log (usually Forwarded Events). - The subscription type (collector-initiated or source-initiated). - The computer (for a collector-initiated subscription) or the computer group (for a source-initiated subscription). - The filter criteria for selecting the events to forward.
Type of service account	You can use one of the following options for the type of service account that will be used by the subscription: - Default machine account - A specific user service account Either type of account must be a member of either the Source Computers Event Log Readers group (the most secure choice) or a member of the local Administrators group.
Event saving	By default, events received from source computers are saved in the Forwarded Events log.
Filters	If a filter is not defined, all events are collected.
Runtime status	After you have created the subscription, you can use the **Runtime Status** link to verify communications. If you need to change the subscription type after it has been created, you must delete and recreate the subscription.