

Episode Title: Manage event logs

Objectives:

At the end of this episode, I will be able to:

1. Describe the built-in logs
2. Explain event log levels
3. Configure event subscriptions

Key Points:

Key Point 1

Windows Server provides several built-in event logs for many services and features. However, there are three primary logs to be aware of: Application, Security, and System.

Key Point 2

Event entries into the logs will have a severity of event included with the log indicating its importance. The severity levels are: Informational, Warning, Error, Critical, and Verbose.

Key Point 3

You can easily aggregate the logs across multiple servers by configuring Event Subscriptions using the Windows Event Collector Service.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- View and Configure Performance, Event, and Service Data
: <https://learn.microsoft.com/en-us/windows-server/administration/server-manager/view-and-configure-performance-event-and-service-data>