

Windows Logging

Reading

30 minutes

✓ Status Incomplete

Introduction

Logs are records of events in your computer, either by a person or a running process. They help you track what happened and troubleshoot problems. The Windows event log contains logs from the OS and applications such as **SQL Server** or **Internet Information Services (IIS)**. The logs use a structured data format, making them easy to search and analyze. Some applications also write to log files in text format.

Reading

Different Logs with Event Viewing Mechanisms in Windows

- **DNS Manager**: If the Windows server is provisioned as a **DNS** server, the DNS Manager is installed. In small networks, this is typically the Active Directory Domain Server.
- **Failover Cluster Manager**: Windows Server Failover Clustering service enables two or more Windows servers to work as a cluster in a fault-tolerant configuration where one server's physical failure is automatically detected and replaced by the other server. Windows Server Failover Clustering service is the foundation of modern **SQL Server High Availability (HA)** solutions like AlwaysOn Availability Groups.
- **The Internet Information Services Access Logs (IIS Access Logs)**: These logs include information about requested URLs and status indicating the connection's response. These logs are files in the W3C extended log format. This format is a type of **comma-separated value (CSV)**.

The log file location is specified within the **IIS Manager** logging settings.

By default, the location is: `%SystemDrive%\inetpub\logs\LogFiles`

The log file on `[C:\]`, with `W21SVC1` as the virtual host and `u_e221024` as a file name coded with the date `2022-10-24`: ->
`C:\inetpub\logs\LogFiles\W21SVC1u_e221024.log`



TIP: [%SystemDrive%] is a particular system variable or environment variable used on Microsoft Windows.

- **Task Scheduler History Logs:** Task Scheduler runs background tasks and applications on scheduled scripts or applications, much like the **Linux CRON** subsystem. An example is a nightly backup script that backs up local SQL Server databases.

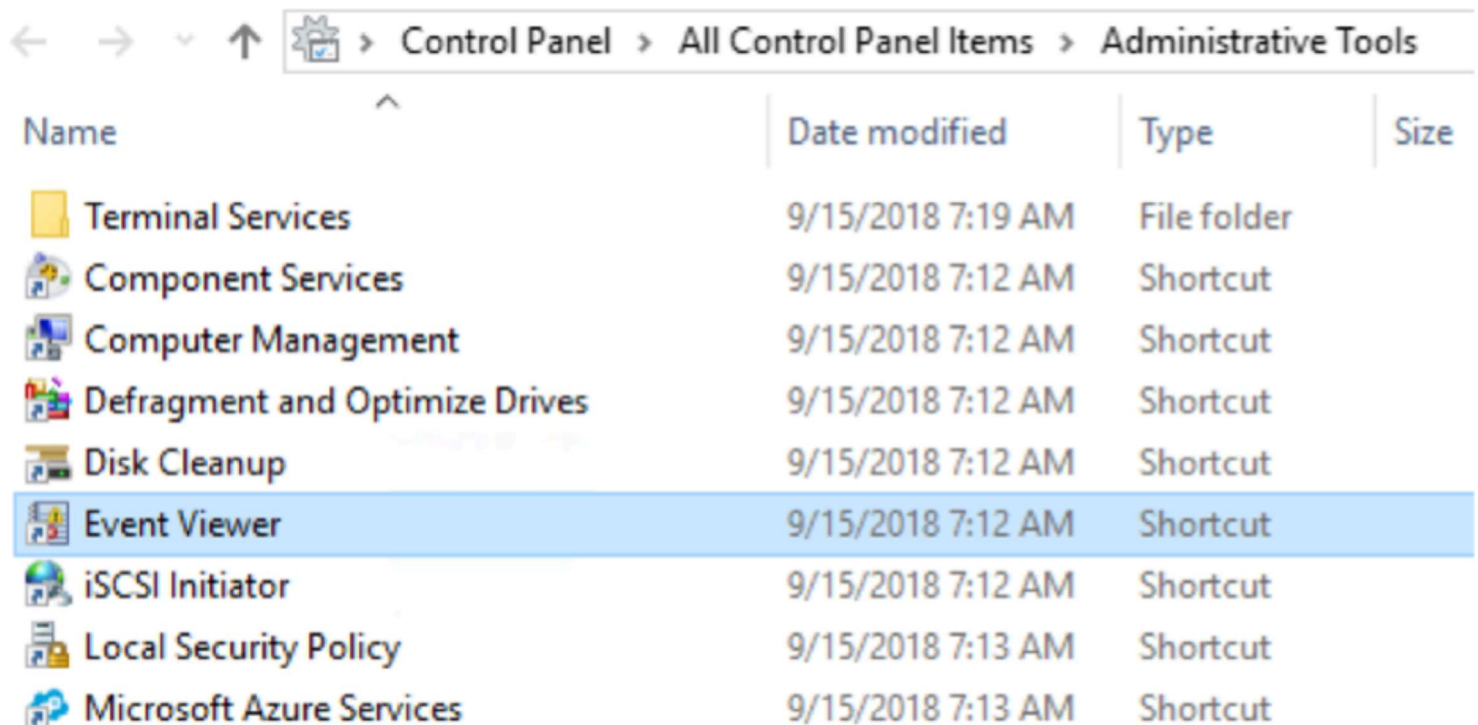
Windows Event Logs

Windows Event Viewer displays the Windows event logs. Use this application to view and navigate the logs, search and filter particular types of logs, and export logs for analysis. You will learn how to access Windows Event Viewer and be shown available features.

Windows Event Viewer can be opened in many ways:

- **Windows Control Panel:** Control Panel is the standard Windows component for viewing and changing system settings. It can be found in Windows server and Windows desktop editions.

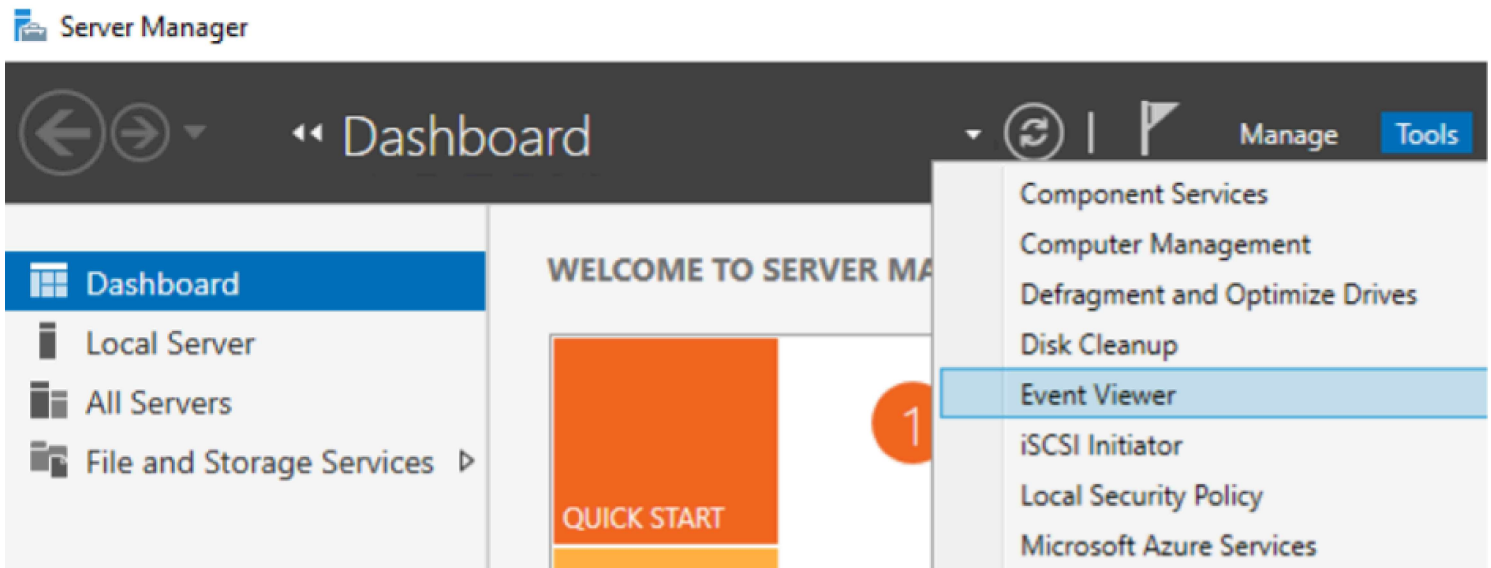
To access the Event Viewer: Open Control Panel > Administrative Tools > Event Viewer



Name	Date modified	Type	Size
Terminal Services	9/15/2018 7:19 AM	File folder	
Component Services	9/15/2018 7:12 AM	Shortcut	
Computer Management	9/15/2018 7:12 AM	Shortcut	
Defragment and Optimize Drives	9/15/2018 7:12 AM	Shortcut	
Disk Cleanup	9/15/2018 7:12 AM	Shortcut	
Event Viewer	9/15/2018 7:12 AM	Shortcut	
iSCSI Initiator	9/15/2018 7:12 AM	Shortcut	
Local Security Policy	9/15/2018 7:13 AM	Shortcut	
Microsoft Azure Services	9/15/2018 7:13 AM	Shortcut	

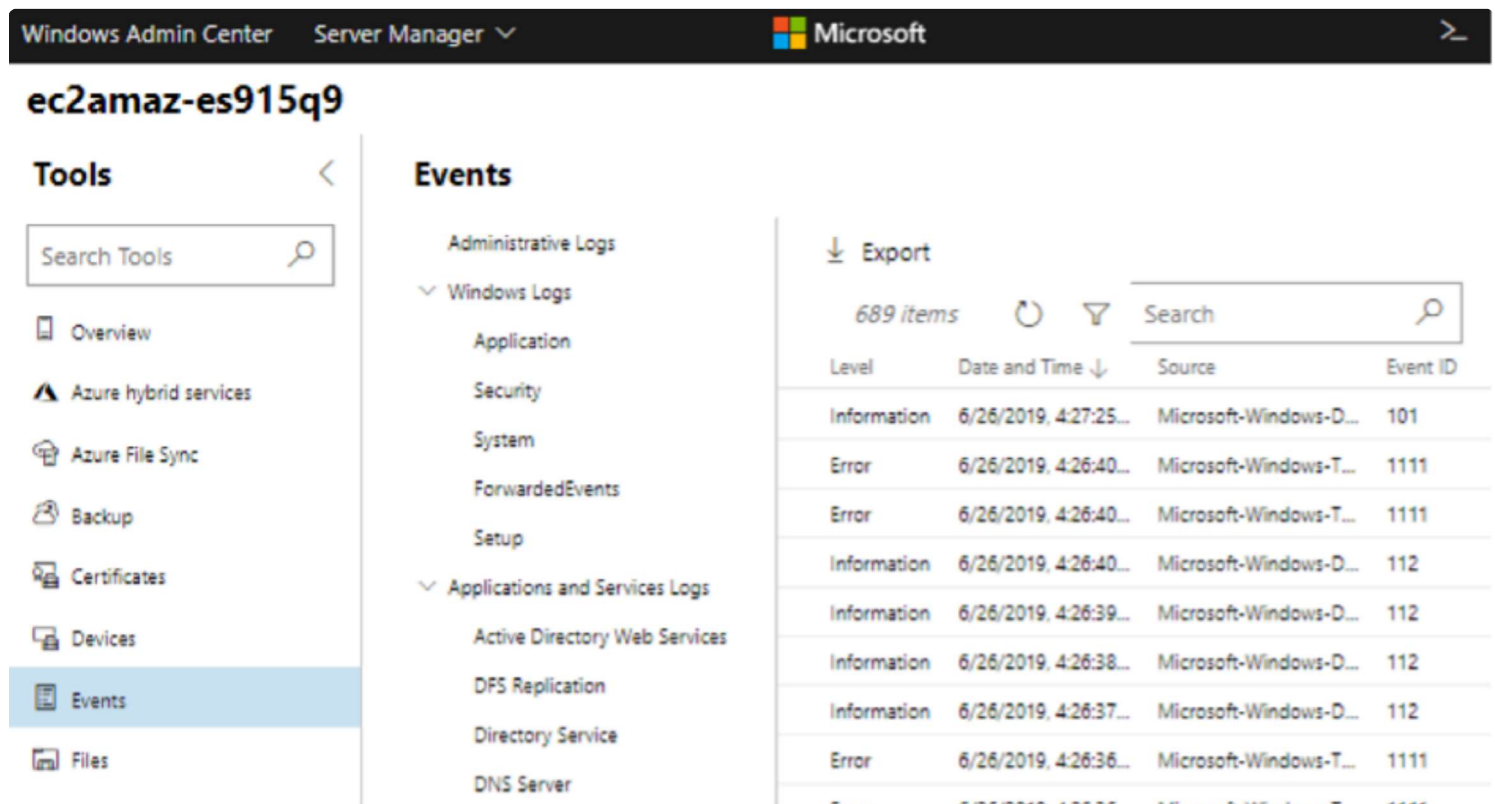
- **Server Manager:** The Server Manager console lets you manage settings on the local server and remote servers.

To access Event Viewer from Server Manager: Open Server Manager > Open Tools > Event Viewer



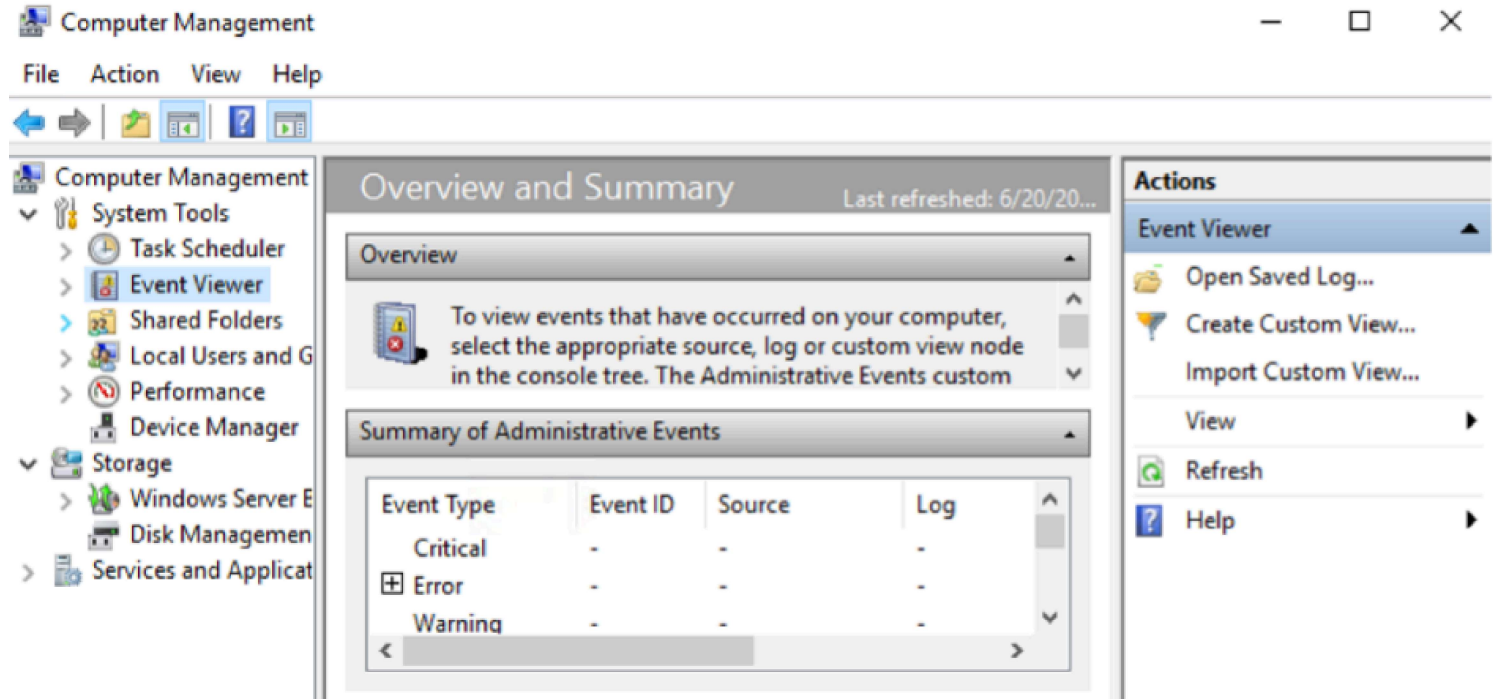
- **Windows Admin Center:** This is a browser-based application for managing servers, clusters, desktop PCs, and other infrastructure components.

To access Event Viewer from the Windows Admin Center: Open Windows Admin Center in a supported browser > Click Events.



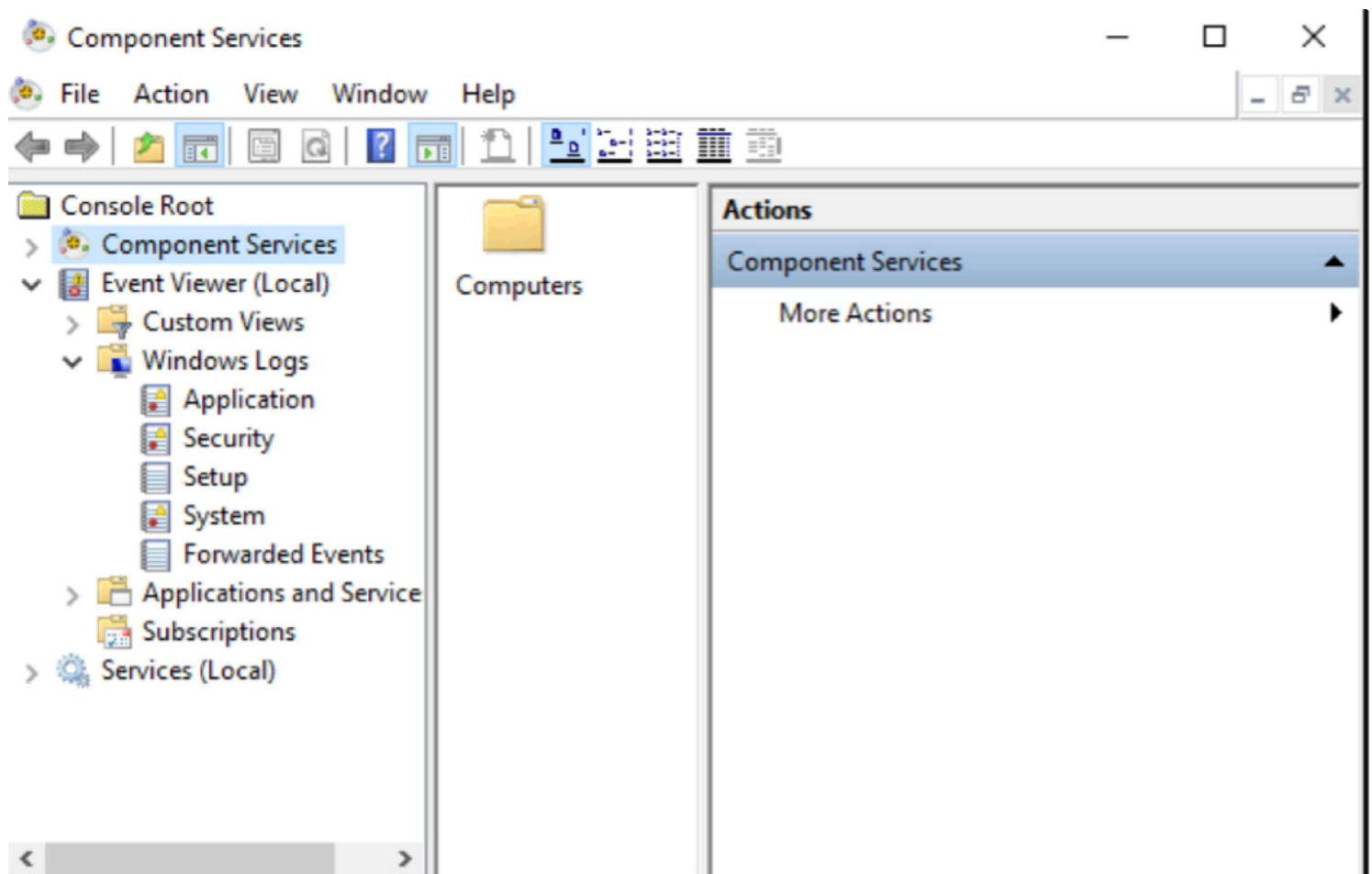
- **Computer Management:** This provides access to administrative tasks on a local or remote server.

To open Event Viewer from Computer Management: Open Computer Management > Click Event Viewer.



- **Windows Component Service:** This enables you to configure **DCOM** applications running on Windows.

To open Event Viewer from Component Services Manager as well: Open Component Services > Click Event Viewer



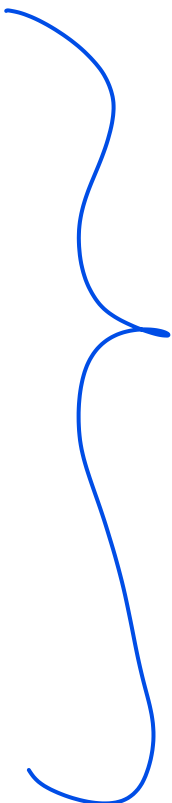
- **Command Prompt:** You can open the Event Viewer directly from a **command prompt (cmd)**.

To open using cmd: Open a Command Prompt > Type: eventvwr

The Events

Event entries are listed by default in chronological order, with the latest events at the top, and each event has a severity Level:

	Information messages indicate a successful action.
	Warning messages indicate an event occurred that might become a problem.
	Error messages indicate a significant problem occurred.
	Critical messages indicate a severe problem occurred.
	Audit success is associated with security events.
	Audit failure is associated with security events.



► Read the table in text format

References

- 1. [Event Logging](#)
- 2. [Monitor Event Log](#)

✓ Mark Completed

←

Previous

Network Administration Quiz

Next

Linux Logging: Syslog and Log Collection

→

How well did this activity help you to understand the content?
Let us know how we're doing



W01D4

Thu Jun 27

› Lectures (1)

▼ Work (7)

4 hrs

 Common Network Conversations & Their Protocols

? Network Administration Quiz



 Windows Logging

 Linux Logging: Syslog and Log Collection

 Centralized Logging

? Logs

 Troubleshooting Approaches

[W01D4 Schedule »](#)