Alex Phillips

Kenyatte Simuel

SVAD 260

06/09/2024

Log Research

1. Where are they?

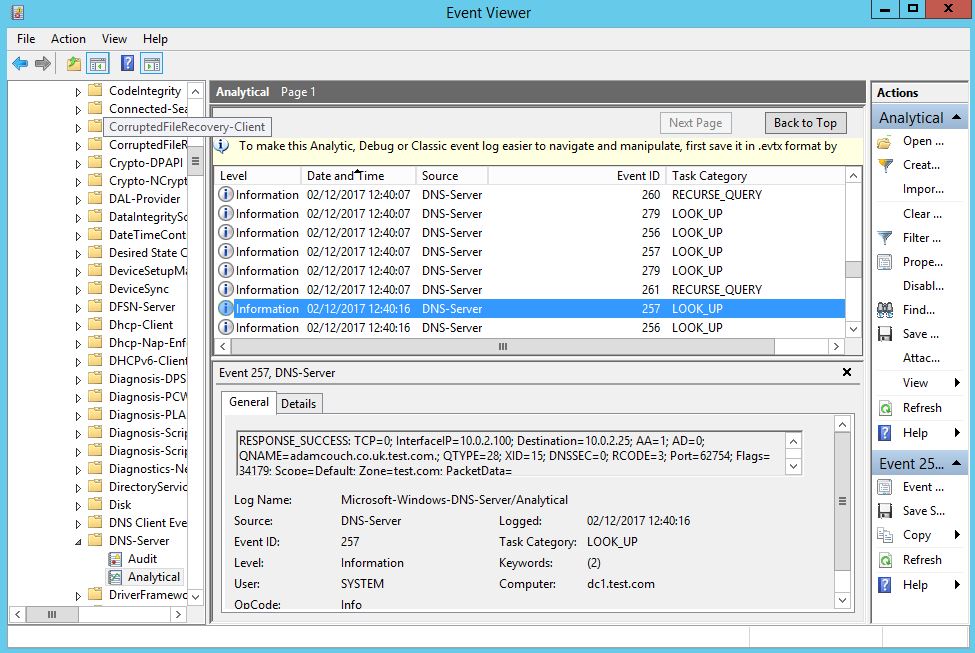
Active Directory and Domain Controller event/system logs are stored on the servers running the Windows Server operating system and are usually accessible via Event Viewer.

A screenshot of a computer

Description automatically generated

1. What is there?

Active Directory and Domain Controller event/system logs have system, application, security, directory service, and DNS server logs.



1. Local Windows events, what are the components?

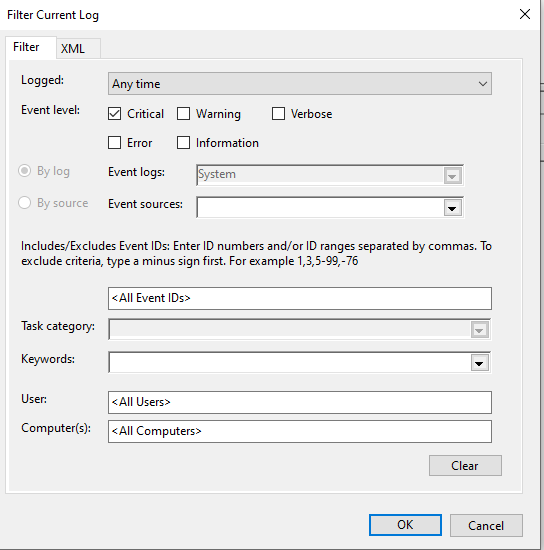
Local Windows events components consist of event source, event ID, log name, date and time, event level, event description, user, computer, event data, task category, keywords.

A screenshot of a computer

Description automatically generated

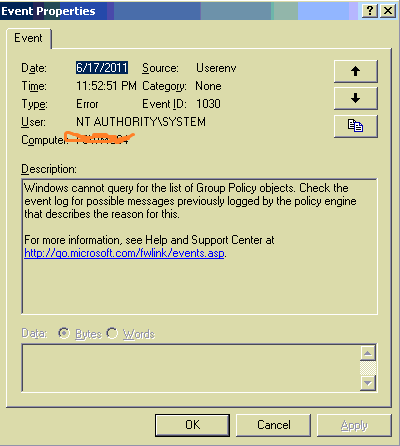
1. How can they be filtered and sorted?

Active Directory and Domain Controller logs can be filtered by event level, event ID’s, date and time, keywords, user, and computer.



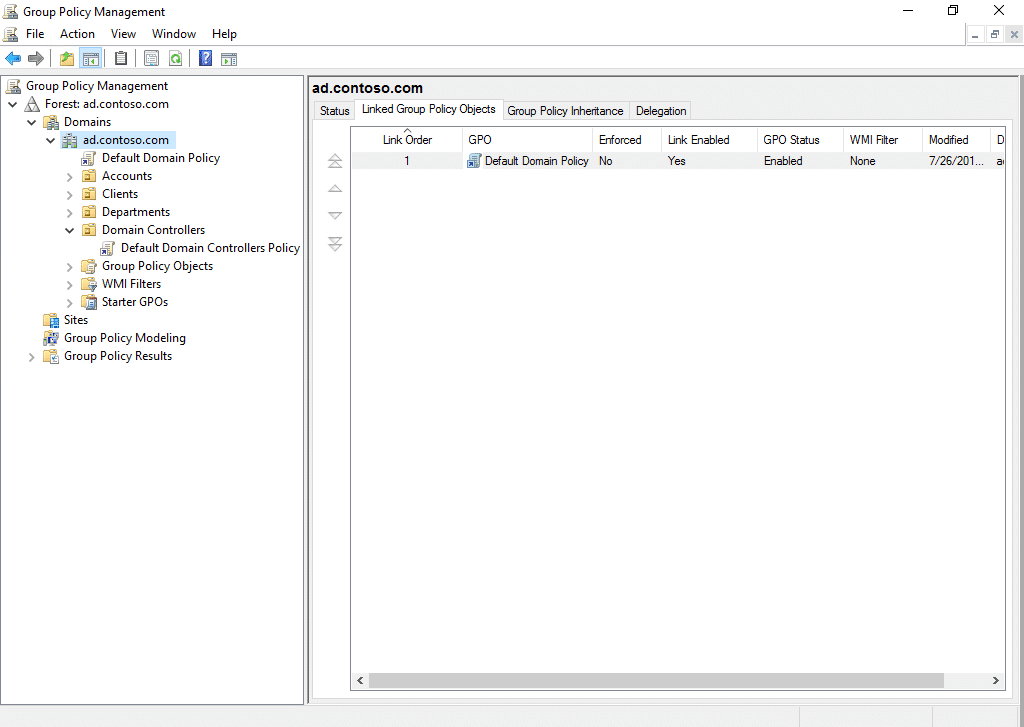
1. Where is the official MS event logs repository?

The official Microsoft event logs repository can be found on the Microsoft Documentation website and within the Microsoft Event ID and Source Message Center.



1. What can be added?

Group Policy Objects can be modified to capture additional events related to security, access, and system changes.



1. How can you create your own events?

You can create custom event logs to capture specific types of information that are not logged by default using PowerShell.

A screenshot of a computer

Description automatically generated

1. Where are the files stored locally?

By default, event logs are stored in the form of .evtx files in C:\Windows\System32\winevt\Logs\.

A screenshot of a computer program

Description automatically generated

1. How can you move them to a network share?

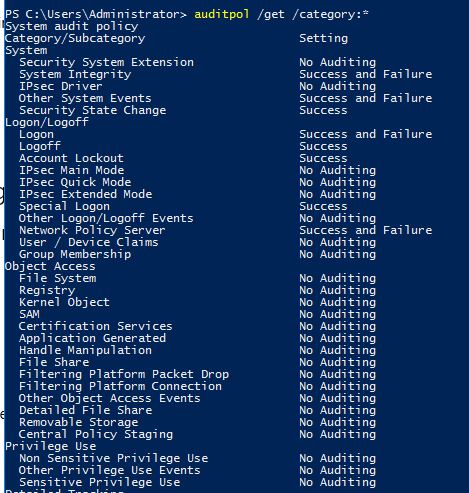
On the server you plan to store the logs to, create a folder, go to properties, sharing, advanced sharing, and set permissions to allow the necessary accounts to write to the share. Set NTFS permissions under the security tab by giving full control permissions to necessary accounts. Configure event log redirection by going to regedit.exe, going to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog, and within the EventLog key select a log and modify the File value by double clicking on it and changing the file patch to the network share, then restart the event log service.

A screenshot of a computer

Description automatically generated

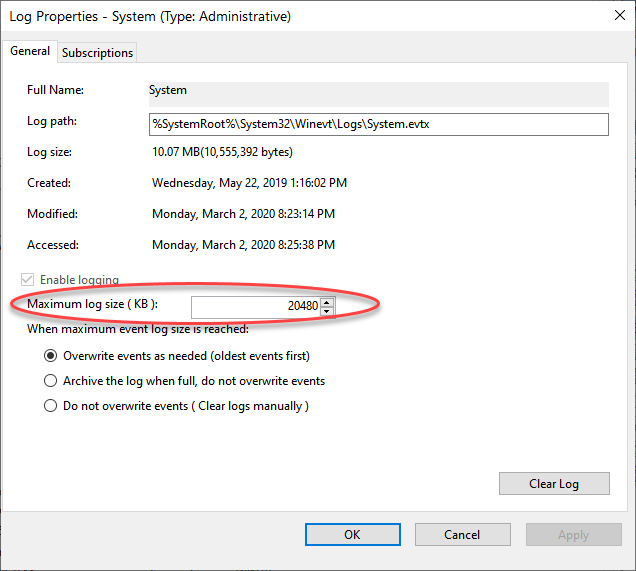
1. How do you adjust what gets recorded?

You can adjust what gets recorded by going into group policy management, navigating to the policy, configuring advanced audit policy settings, or you can configure audit policies through PowerShell.



1. How do you adjust the size of the logs?

Open event viewer, navigate to directory service log, adjust log settings, and adjust setting such as maximum log size and action to take when the log is full.



1. What are the options when the logs are full?

The options for when the logs are full are overwrite events as needed; archive the log when full, not overwrite events; and do not overwrite events (clear log manually).

