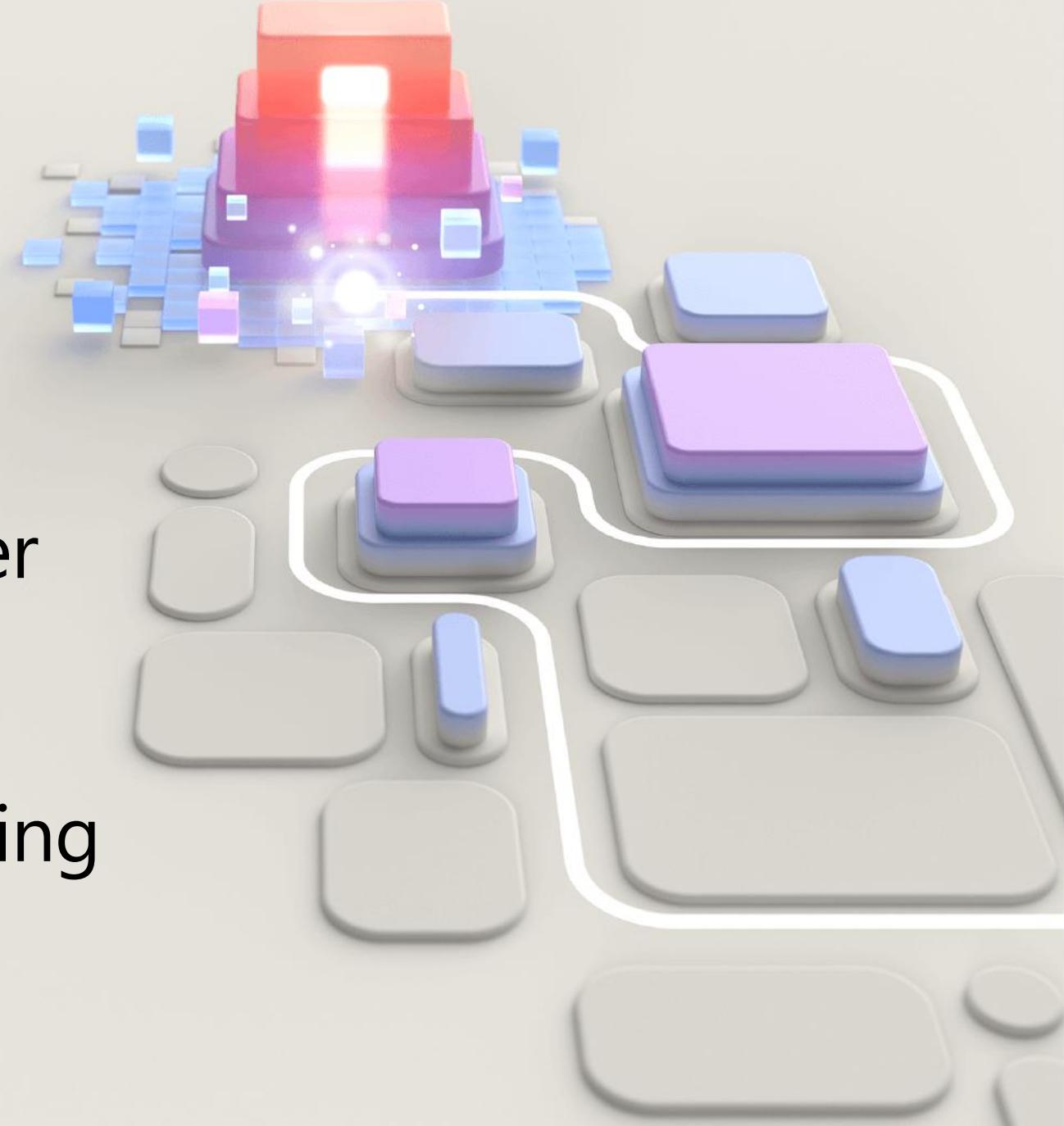


AZ-801

Guten Morgen!

Configuring Windows Server  
Hybrid Advanced Services

8 Windows Server Monitoring



# AZ-801 Course Outline

- 1 Windows Server Security on Prem
- 2 Windows Server Security Cloud
- 3 Failover Cluster
- 4 Disaster Recovery on Prem
- 5 Disaster Recovery Cloud
- 6 Windows Server Upgrade and Migrate
- 7 Migrate Windows Server to Cloud

- 8 Windows Server Monitoring
- 9 Monitoring in the Cloud

Perfmon Counter % CPU Lab 8 ✓

30 Tage Azure Monitor ← Counter % CPU

LA Workspace ← VM old X  
Log Analytics ← NMA Agent old X  
AMA Agent new ✓

Lab 9 X

→ APL

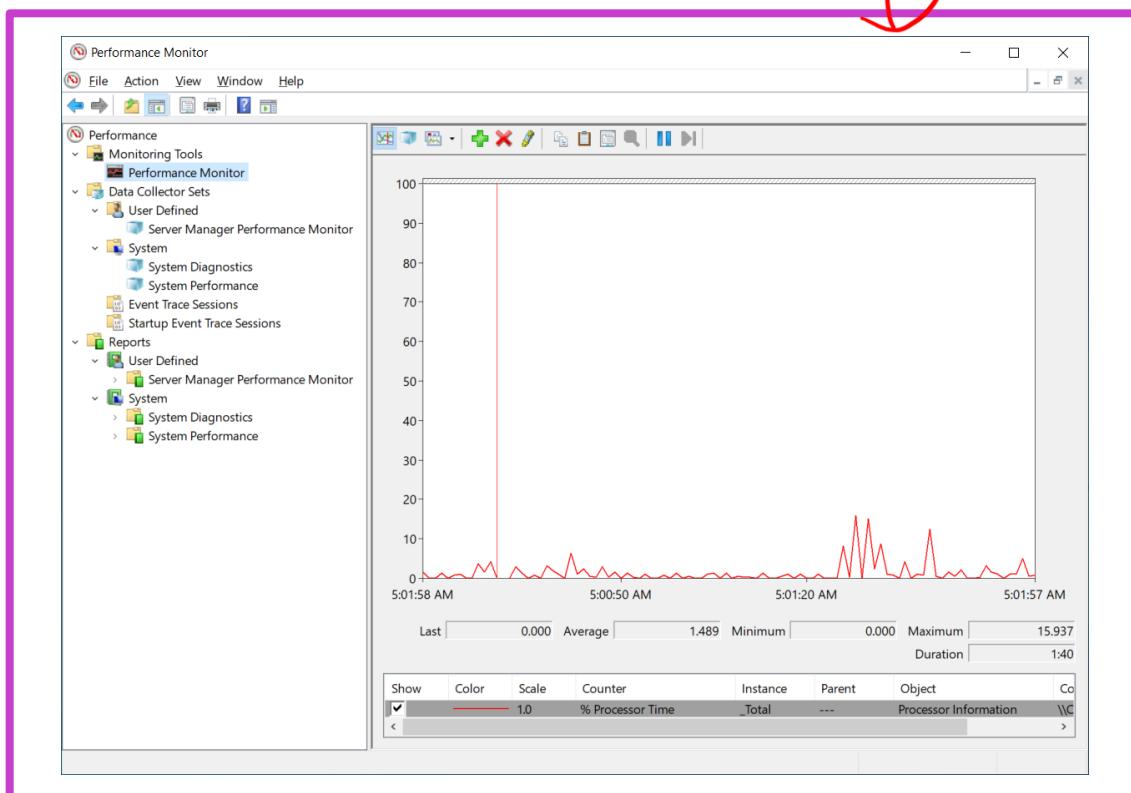
# Monitor and Troubleshoot Windows Server Environment (*Server and performance monitoring in Windows Server*)

- Monitor Windows Server performance /
- Manage and monitor Windows Server event logs /
- Implement Windows Server auditing and diagnostics /
- Troubleshoot Active Directory / 
- Lab 08 – Monitoring and troubleshooting Windows Server ✓

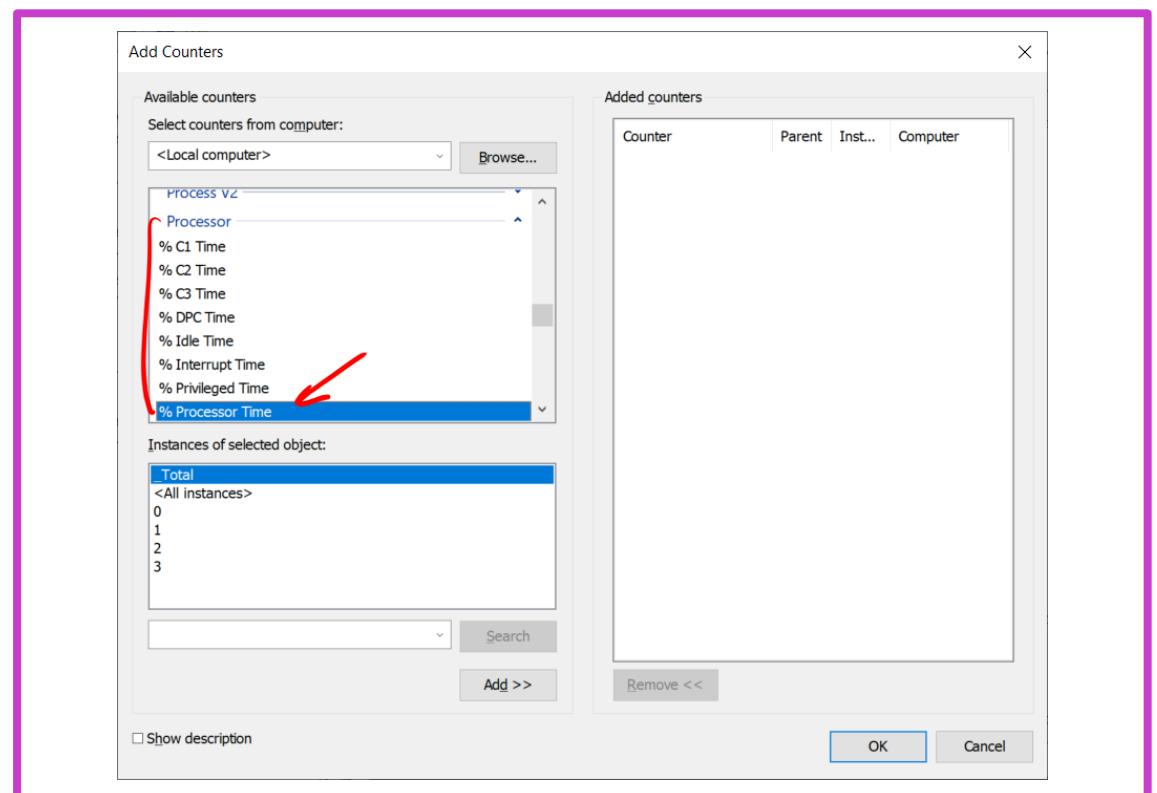
# Monitor Windows Server performance

# Use Performance Monitor to identify performance problems

## Performance Monitor



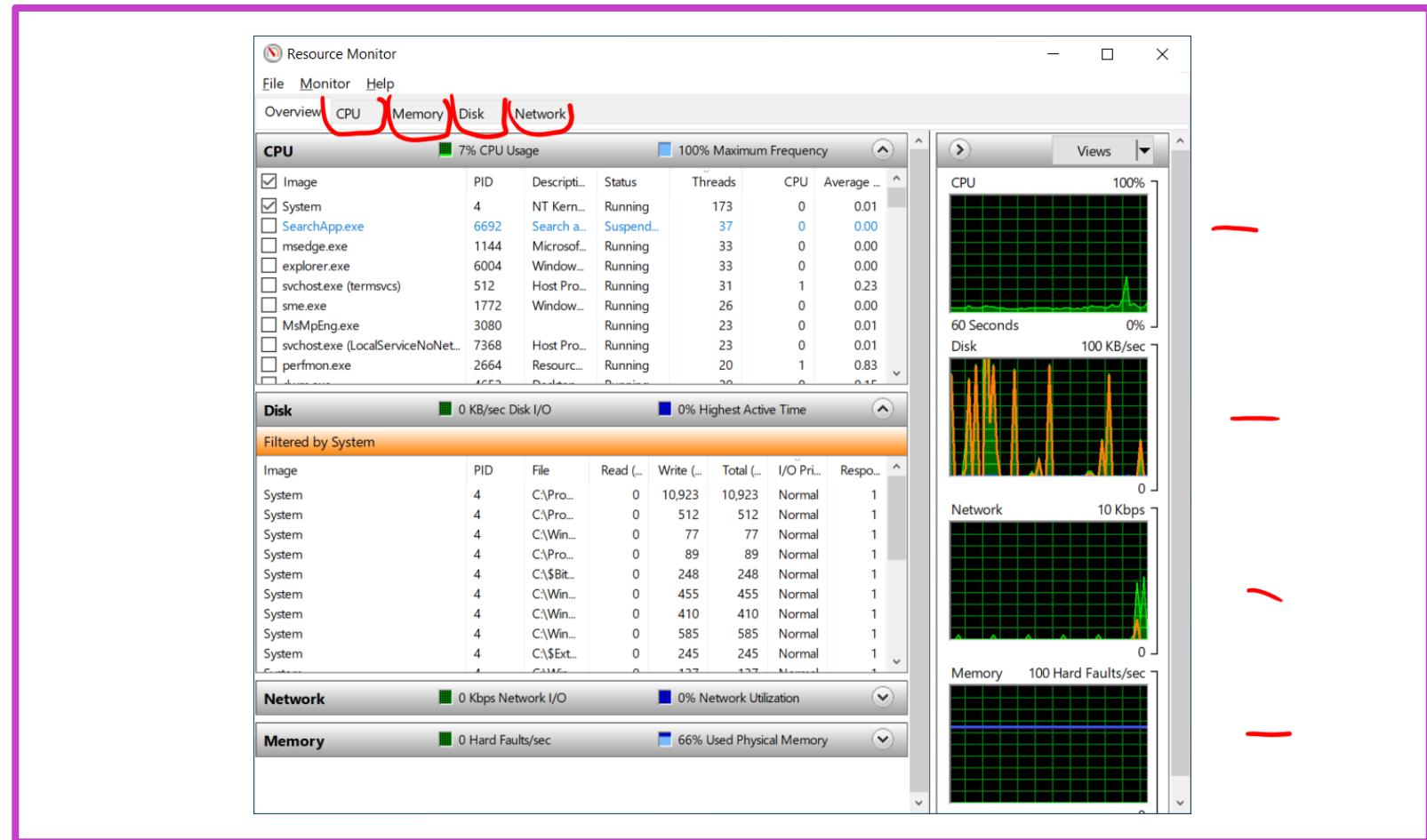
## Common performance counters



# Use Resource Monitor to review current resource usage

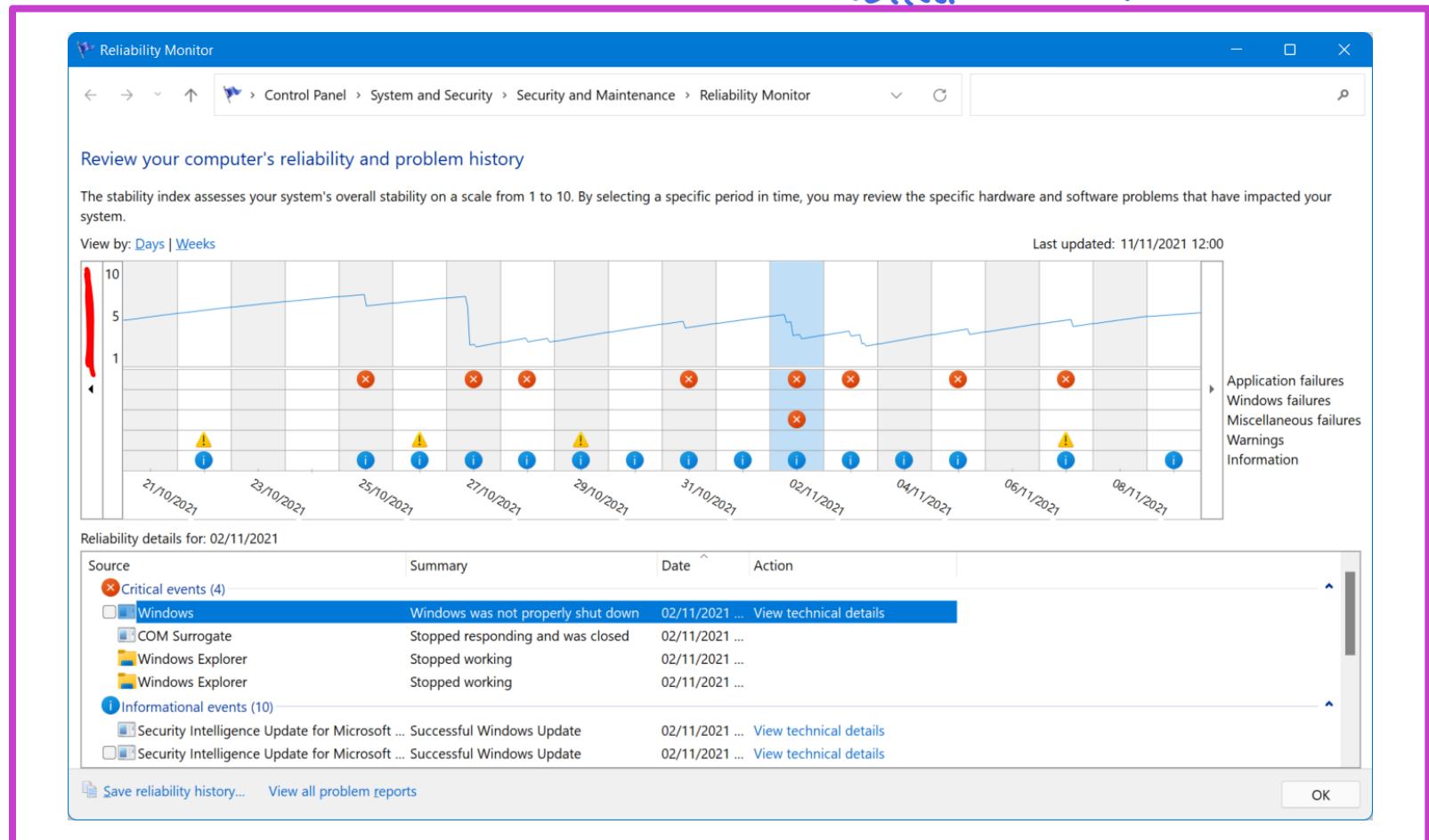
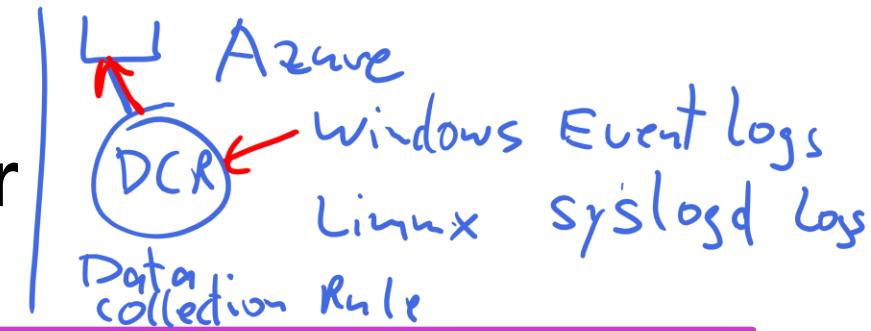
Resource Monitor monitors the use and performance of a CPU, disk, network, and memory resources in real time.

- In Resource Monitor, if you expand the monitored elements, you can identify which processes are using which resources
- Use Resource Monitor to track a process or processes by selecting their check boxes.



# Review reliability with Reliability Monitor

- Reliability Monitor is installed in Windows Server by default, which monitors hardware and software issues.
- To load Reliability Monitor, you can go to **Control Panel → Security and Maintenance → Maintenance** → Click the link of **View reliability history**



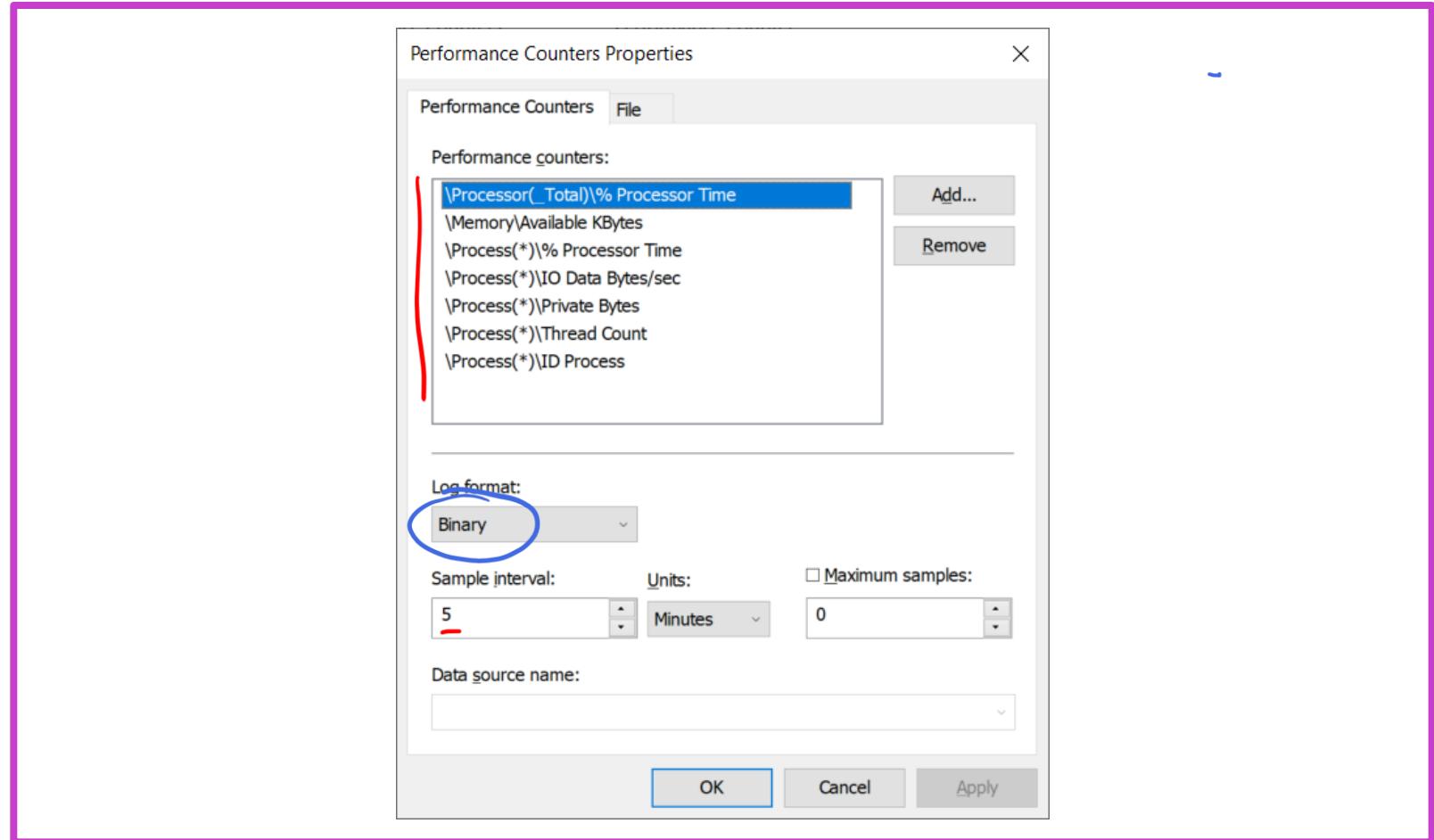
# Implement a performance monitoring methodology

- 1 **Perform trends analysis** – Predict when existing capacity is likely to be exhausted. Review historical analysis and use data to determine when more capacity is required.
- 2 **Consider capacity planning** – Focuses on assessing server workload, the number of users that a server can support and the ways to scale systems to support more workload and users in the future
- 3 **Understand bottlenecks** – Occurs when a computer is unable to service requests for a specific resource or the shortage of a component within an application package might also cause the bottleneck
- 4 **Analyze key hardware components** – The four key hardware components are processor, disk, memory, and network.

# Use Data Collector Sets to analyze server performance

## How can you use data collector sets?

- Use a data collector set on its own or group it with other data collector sets.
- Incorporate a data collector set into logs or observe it in Performance Monitor.
- Configure a data collector set to generate alerts
- Configure a data collector set to run at a scheduled time
- Configure a schedule for performance monitoring



# Monitor network infrastructure services

## Monitor DNS

You can monitor the Windows Server DNS Server role to determine the following aspects of your DNS infrastructure:

- General DNS server statistics
- UDP or TCP counters
- Dynamic update and secure dynamic-update counters
- Memory-usage counter for measuring a system's memory usage and memory-allocation patterns that are created by operating the server computer as a DNS server
- Recursive lookup counters for measuring queries and responses
- Zone transfer counters

## Monitoring DHCP

DHCP provides dynamic IP configuration services for your network, and it provides data on a DHCP server, including:

- The Average Queue Length counter indicates the current length of a DHCP server's internal message queue
- The Milliseconds per packet counter is the average time that a DHCP server uses to process each packet that it receives

Azure:  
Network Watcher  
ping  
traceroute  
NSG  
Topo

# Monitor virtual machines running Windows Server

You can use Hyper-V Resource Metering to monitor VMs by measuring below parameters:

- Average graphics processing unit (GPU) use
- Average physical memory use, including:
  - Minimum memory use
  - Maximum memory use
- Maximum disk-space allocation
- Incoming network traffic for a network adapter
- Outgoing network traffic for a network adapter

You can use the following cmdlets to perform resource metering tasks:

- `Enable-VMResourceMetering`
- `Disable-VMResourceMetering`
- `Reset-VMResourceMetering`
- `Measure-VM`

# Monitor virtual machines running Windows Server

```
Administrator: Windows PowerShell C:\Users\thesc> enable-vmresourcemetering
cmdlet Enable-VMResourceMetering at command pipeline position 1
Supply values for the following parameters:
VMName[0]: 2022__Contoso-SVR1
VMName[1]:
PS C:\Users\thesc> measure-VM
cmdlet Measure-VM at command pipeline position 1
Supply values for the following parameters:
Name[0]: 2022__Contoso-SVR1
Name[1]:
VMName          AvgCPU(MHz)  AvgRAM(M)  MaxRAM(M)  MinRAM(M)  TotalDisk(M) NetworkInbound(M) NetworkOutbound(M)
----          27           2554       2554       2554       135460        0             1
2022__Contoso-SVR1 27           2554       2554       2554       135460        0             1
PS C:\Users\thesc>
```

Typical output from the measure-VM cmdlet is displayed in the screenshot.

PS 5.1

PS 7.0

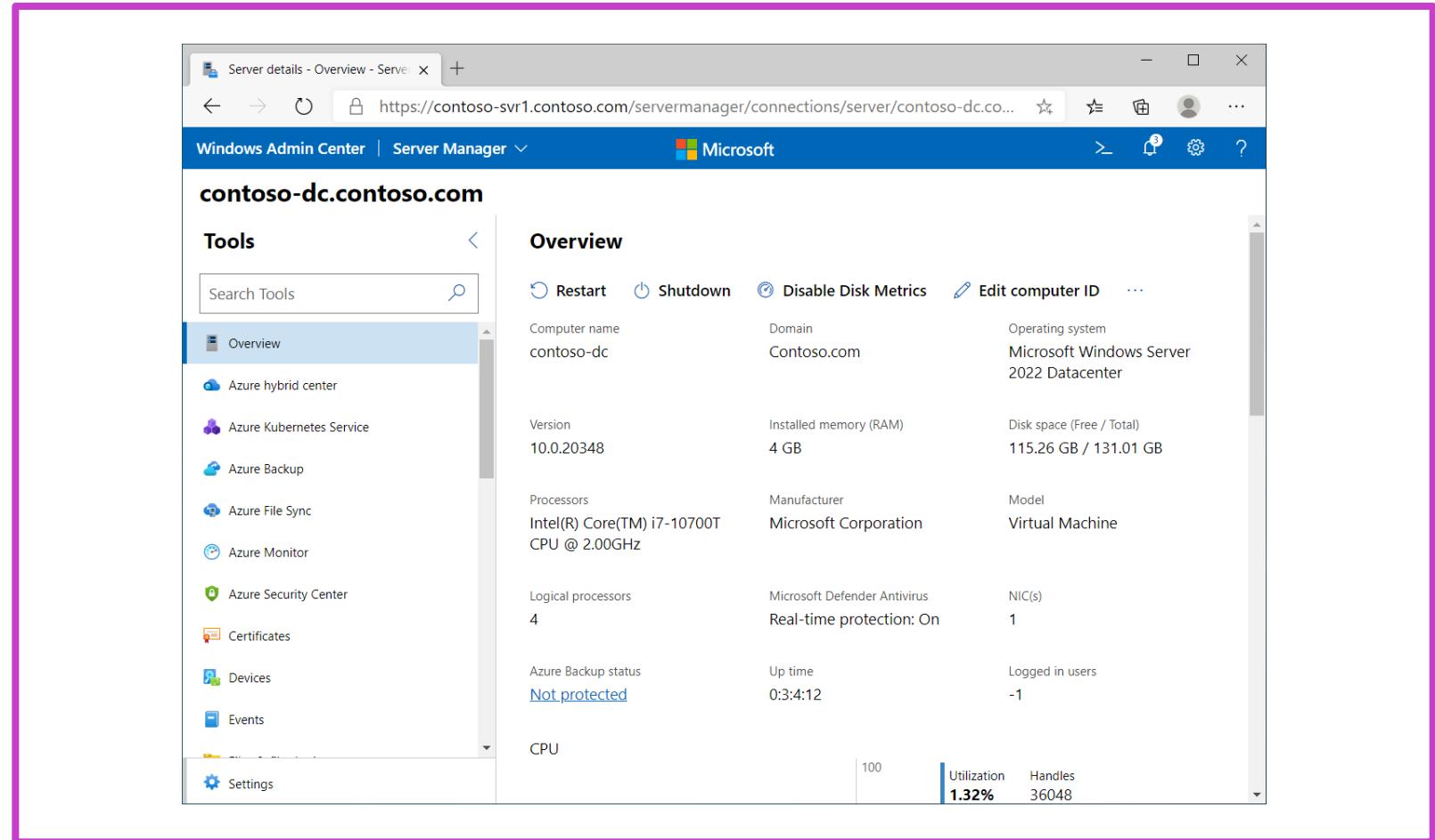
Azure module

Az  
Az. Compute

# Monitor performance with Windows Admin Center

You can perform many tasks with Windows Admin Center, including:

- Overview – Helps you observe current performance details similar to Task Manager
- Performance Monitor – Enables you to compare performance counters for Windows operating systems, apps, or devices in real time
- System Insights – Enables you to determine future capacity needs



WAC

# Use System Insights to help predict future capacity issues

System Insights node displays a number of capabilities:

- CPU capacity forecasting
- Network capacity forecasting
- Total storage consumption forecasting
- Volume consumption forecasting

Prediction status:

- Ok
- Warning
- Critical
- Error
- None

Event Log

Azure Monitor  
Alert

# Optimize the performance of Windows Server

## Tune server hardware

Two key areas to consider:

- Hardware performance
- Hardware power

## Tune server roles

Key roles to consider: Active Directory Domain Services

- File and Storage Services
- Hyper-V
- Remote Desktop Services
- Web Server
- Windows Server Containers

## Tune server subsystem

Consider the following areas:

- Cache and memory management
- Networking
- Software Defined Networking

# Manage and monitor Windows Server event logs

# Describe Windows Server event logs (1 of 2)

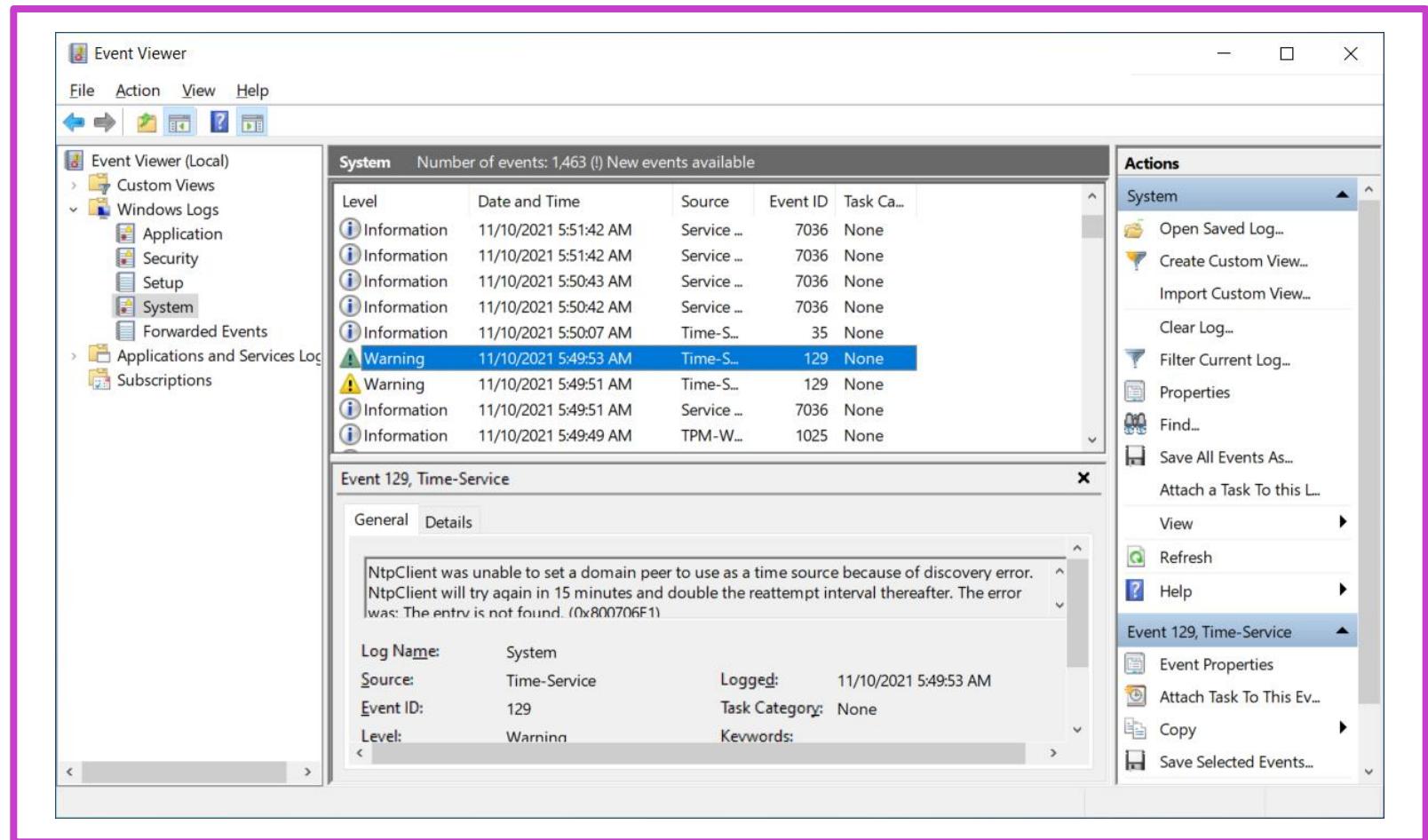
## What is Event Viewer?

Event Viewer provides categorized lists of essential Windows log events, including application, security, setup, and system events.

## What are the Windows Server logs?

Built-in Event Viewer logs:

- Built-in log
- Application log
- Security log
- Setup log
- System log
- Forwarded events



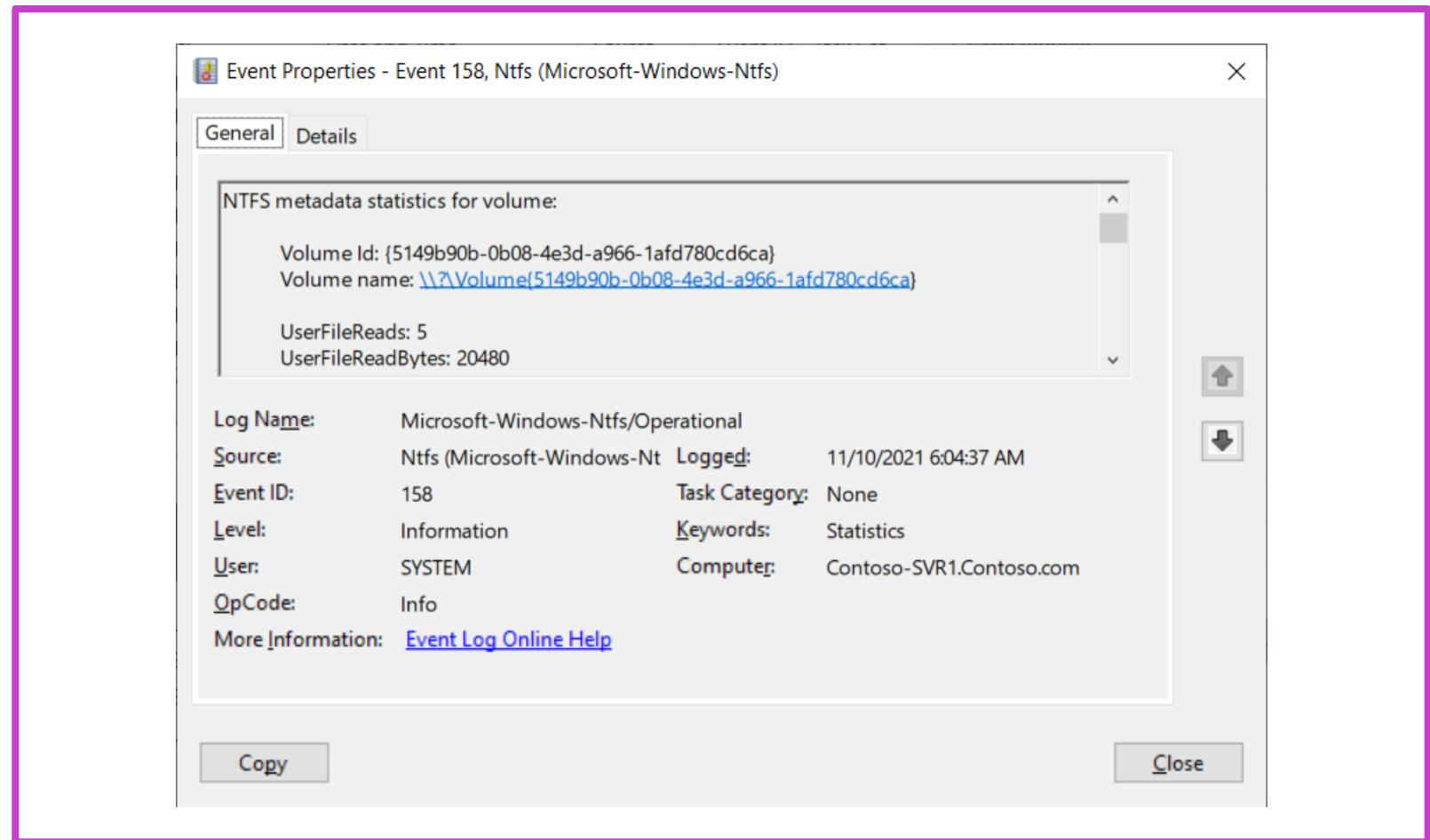
# Describe Windows server event logs (2 of 2)

## Application and service logs

The Applications and Services Logs node stores events from a single application or component rather than events that might have system-wide effects.

## Category of logs:

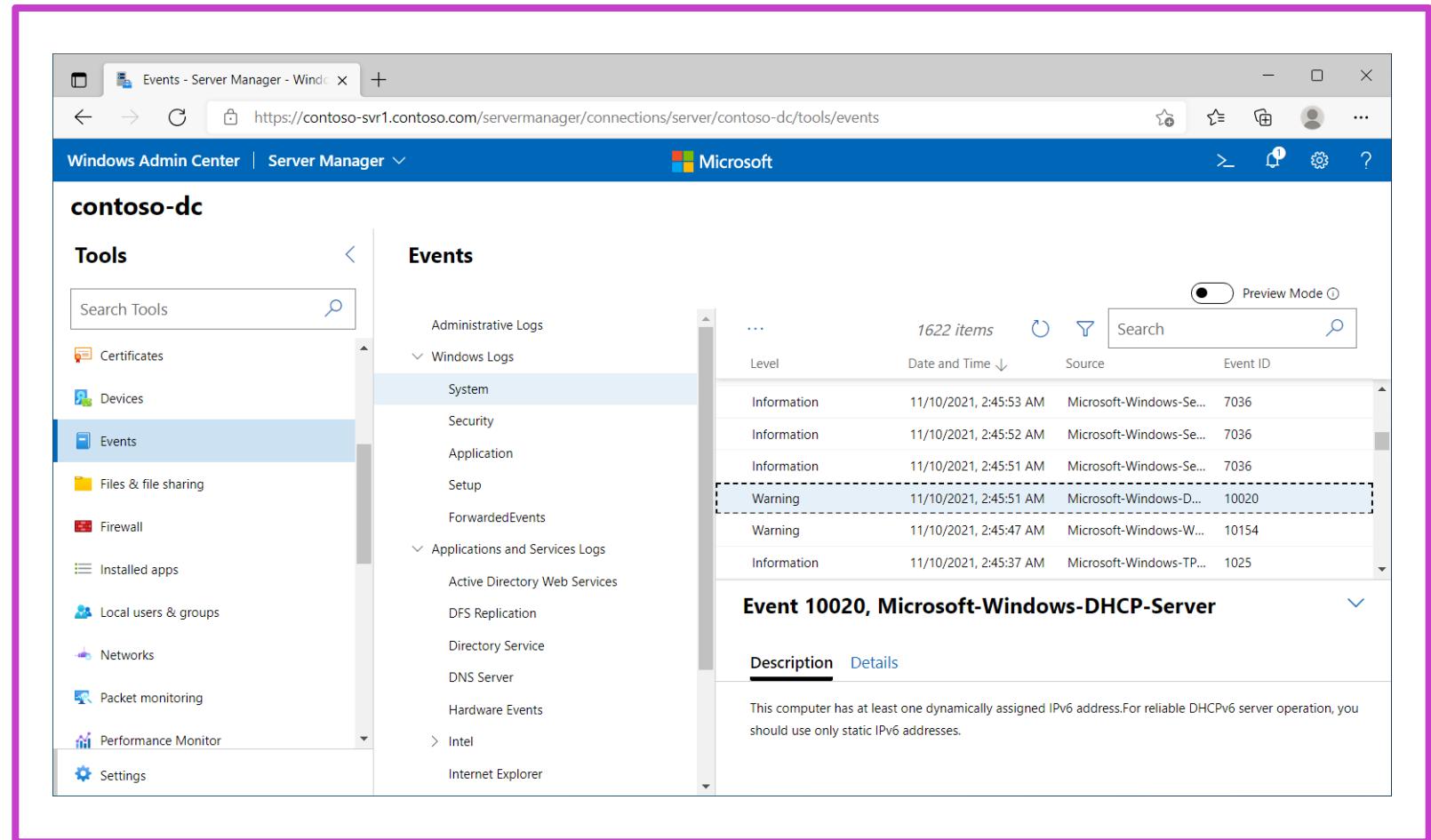
- Admin
- Operational
- Analytic
- Debug



# Use Windows Admin Center to review logs (1 of 2)

**Windows Admin Center**  
A web-based console that you can use to manage computers that are running Windows Server and Windows 10.

**Review event logs**  
You can use Windows Admin Center to review logs on added server computers.

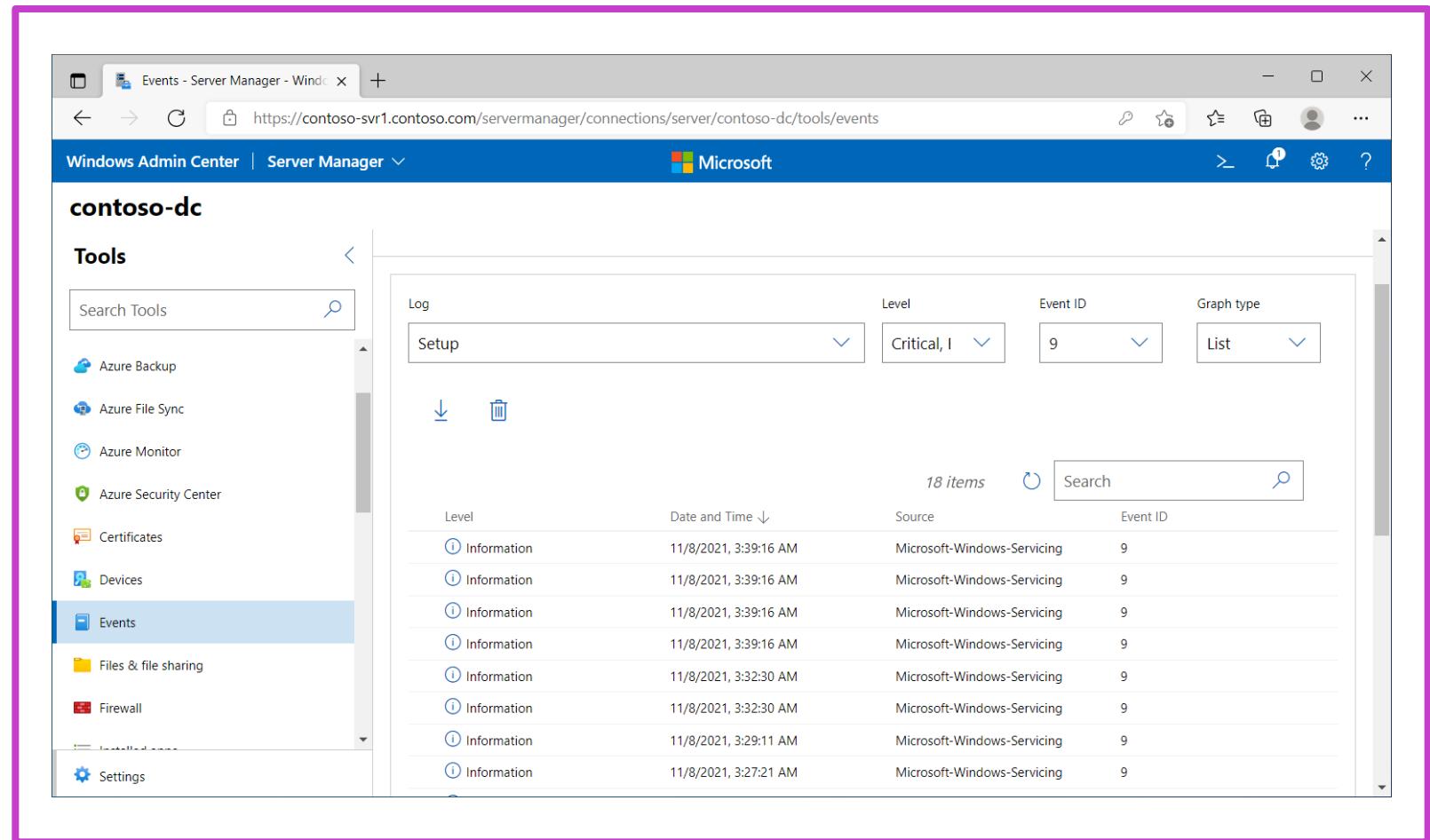


# Use Windows Admin Center to review logs (2 of 2)

## Use preview features

Use Events to perform the following functions:

- Create workspaces
- Save workspaces
- Delete workspaces
- View events in a stacked bar format



The screenshot shows the Windows Admin Center interface with a pink border around the main content area. The left sidebar is titled 'Tools' and lists several options: Azure Backup, Azure File Sync, Azure Monitor, Azure Security Center, Certificates, Devices, Events (which is selected and highlighted in blue), Files & file sharing, and Firewall. The main right pane is titled 'Log' and displays a table of event logs. The table has columns for Level, Date and Time, Source, and Event ID. There are dropdown menus at the top of the log table for Log (Setup), Level (Critical, I), Event ID (9), and Graph type (List). A search bar is also present at the top of the log table. The log table shows 18 items, all of which are Information level events from Microsoft-Windows-Servicing with Event ID 9, occurring between 11/8/2021, 3:39:16 AM and 11/8/2021, 3:27:21 AM.

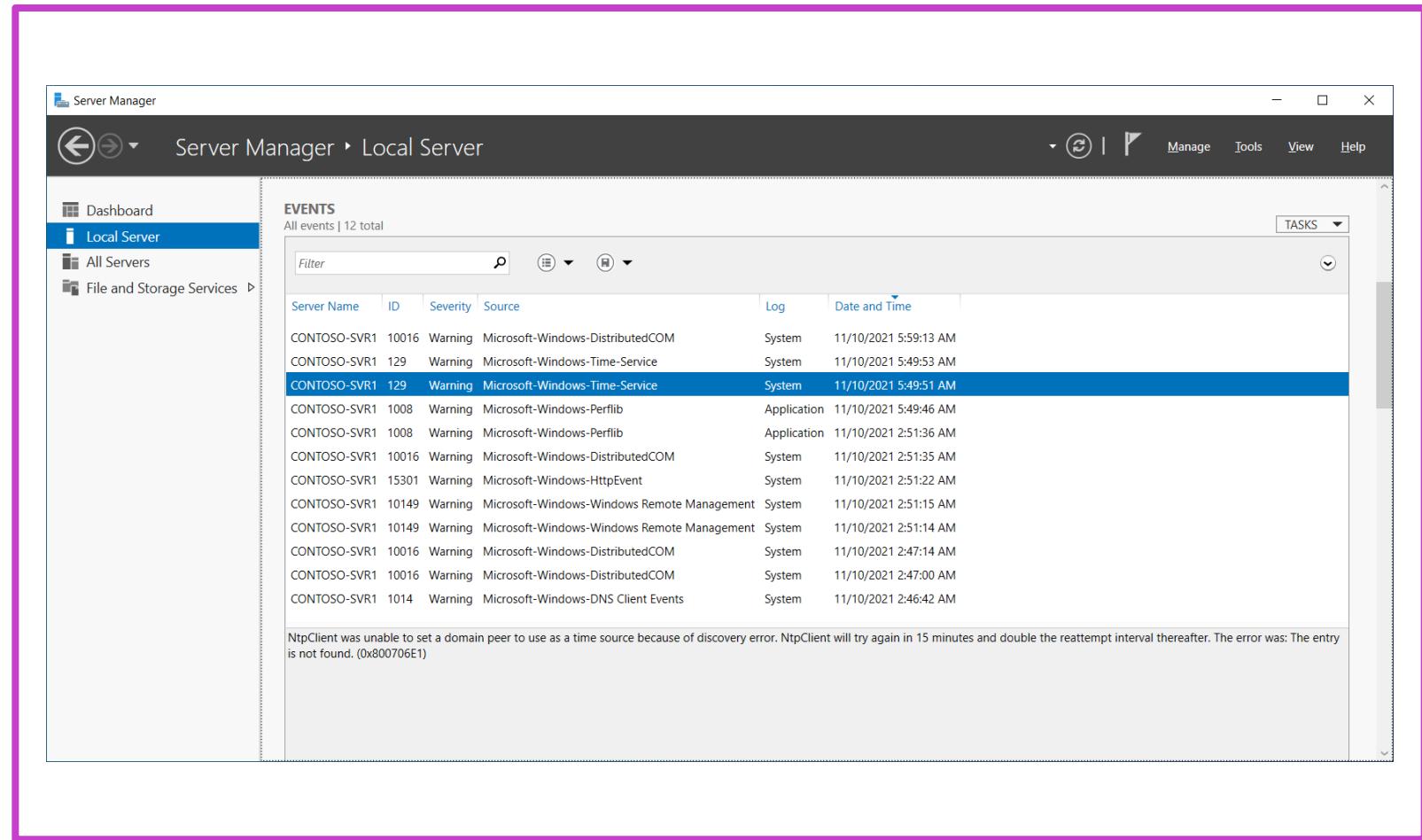
Level	Date and Time	Source	Event ID
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:32:30 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:32:30 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:29:11 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:27:21 AM	Microsoft-Windows-Servicing	9

# Use Server Manager to review logs (1 of 2)

Server Manager provides a monitoring and troubleshooting solution in which administrators can review, in one console, information regarding specific events from different servers and applications.

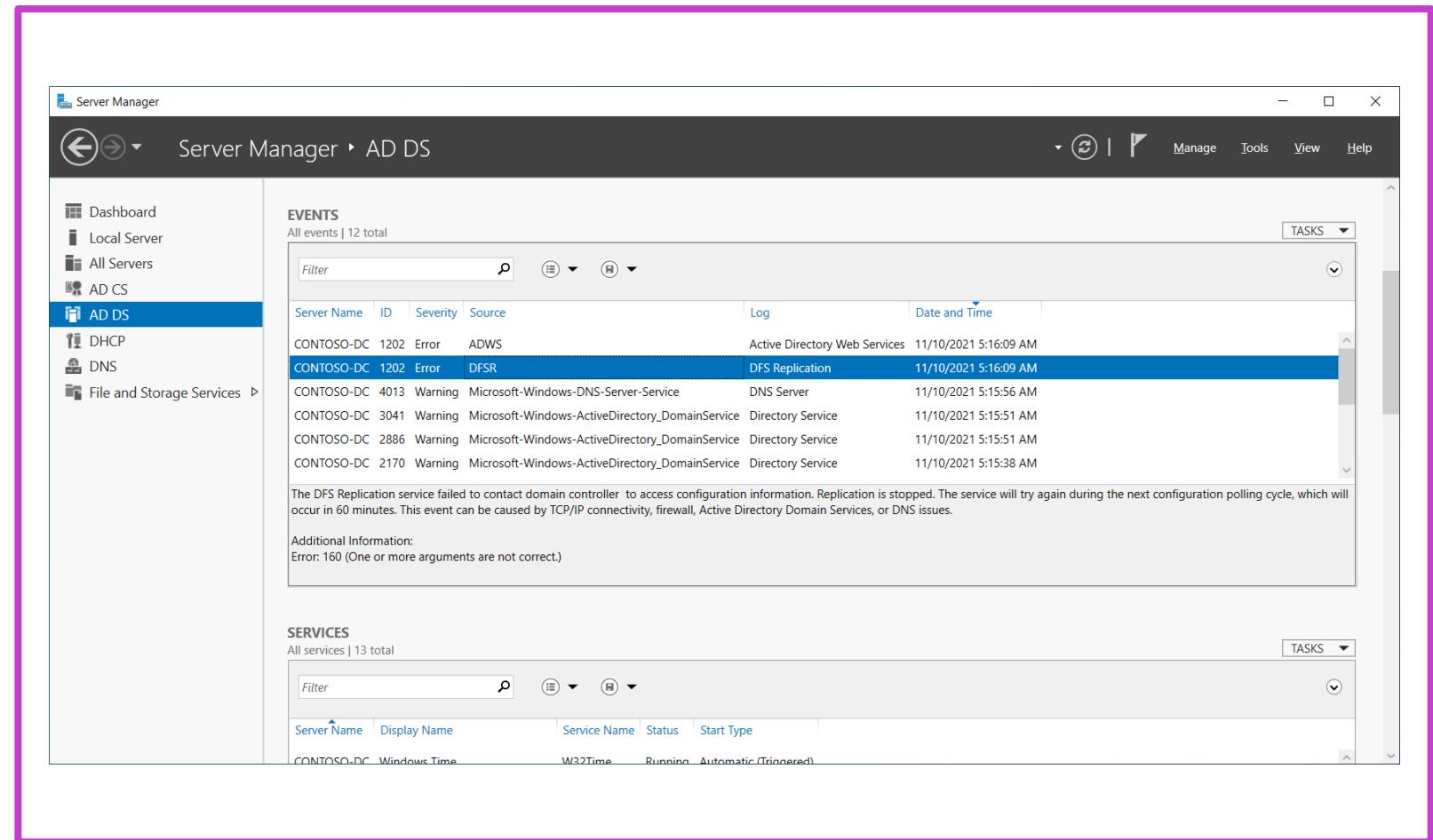
## How can you use Server Manager to review logs?

- Local Server



# Use Server Manager to review logs (2 of 2)

- All Servers
- AD DS, DNS, and Remote Access
- Roles and Server Groups tiles in Server Manager Dashboard



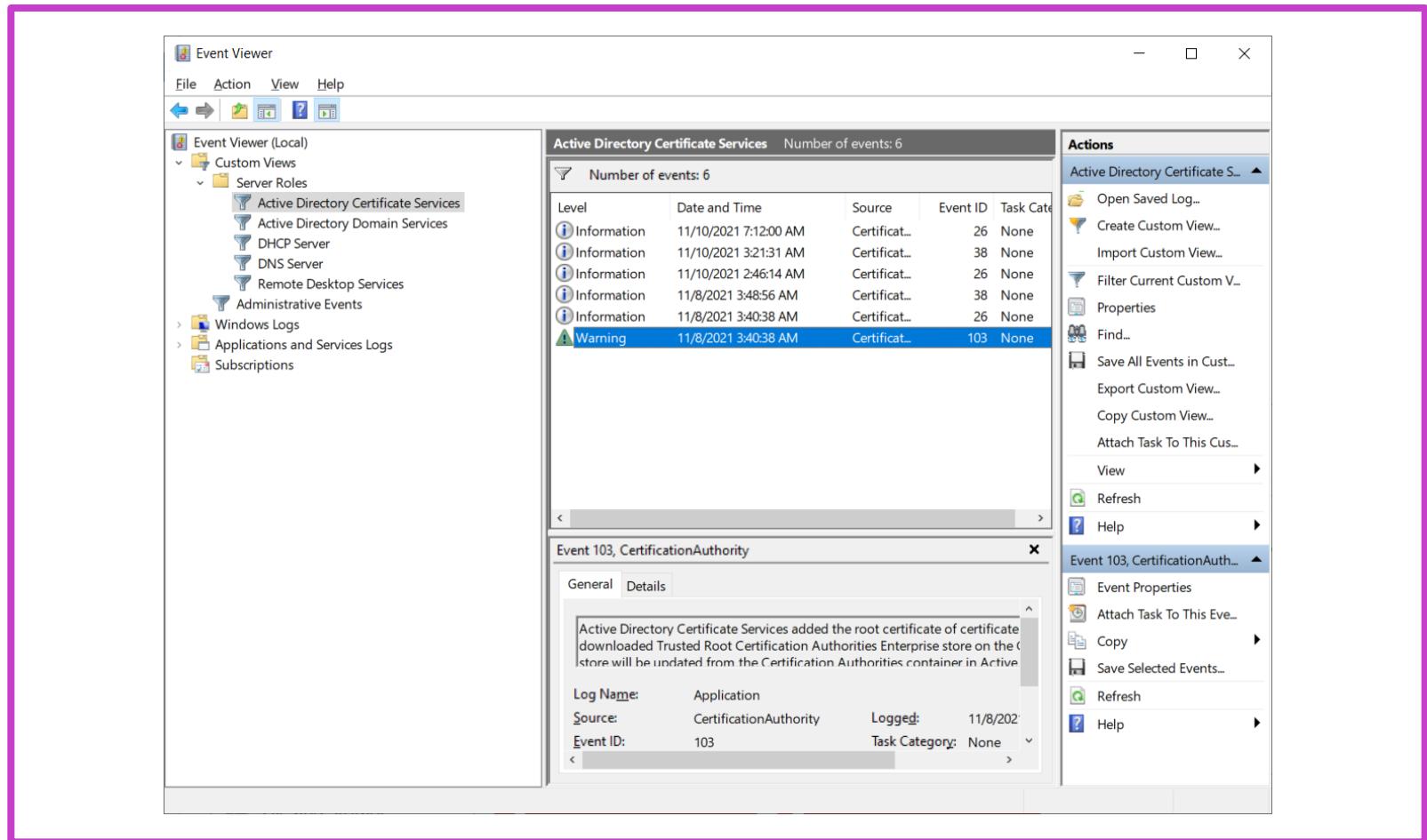
# Use custom views

## Predefined Server Roles custom views

Windows Server Event Viewer provides custom roles based on the installed server roles

## Create custom views

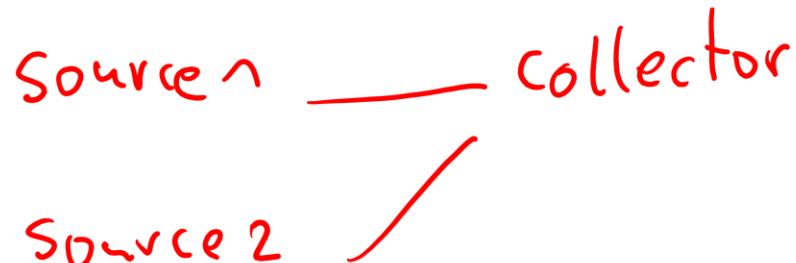
- Event Viewer allows you to filter specific events across multiple logs
- To specify a filter that spans multiple logs, you must create a custom view



# Implement event log subscriptions

## Subscriptions type:

- Collector-initiated
- Source computer-initiated



## Enable subscriptions

- Configure the forwarding and the collecting computers
- The event-collecting functionality depends on the WinRM service and Webservice:  
    :5985
- Both of these services must be running on computers that are participating in the forwarding and collecting process

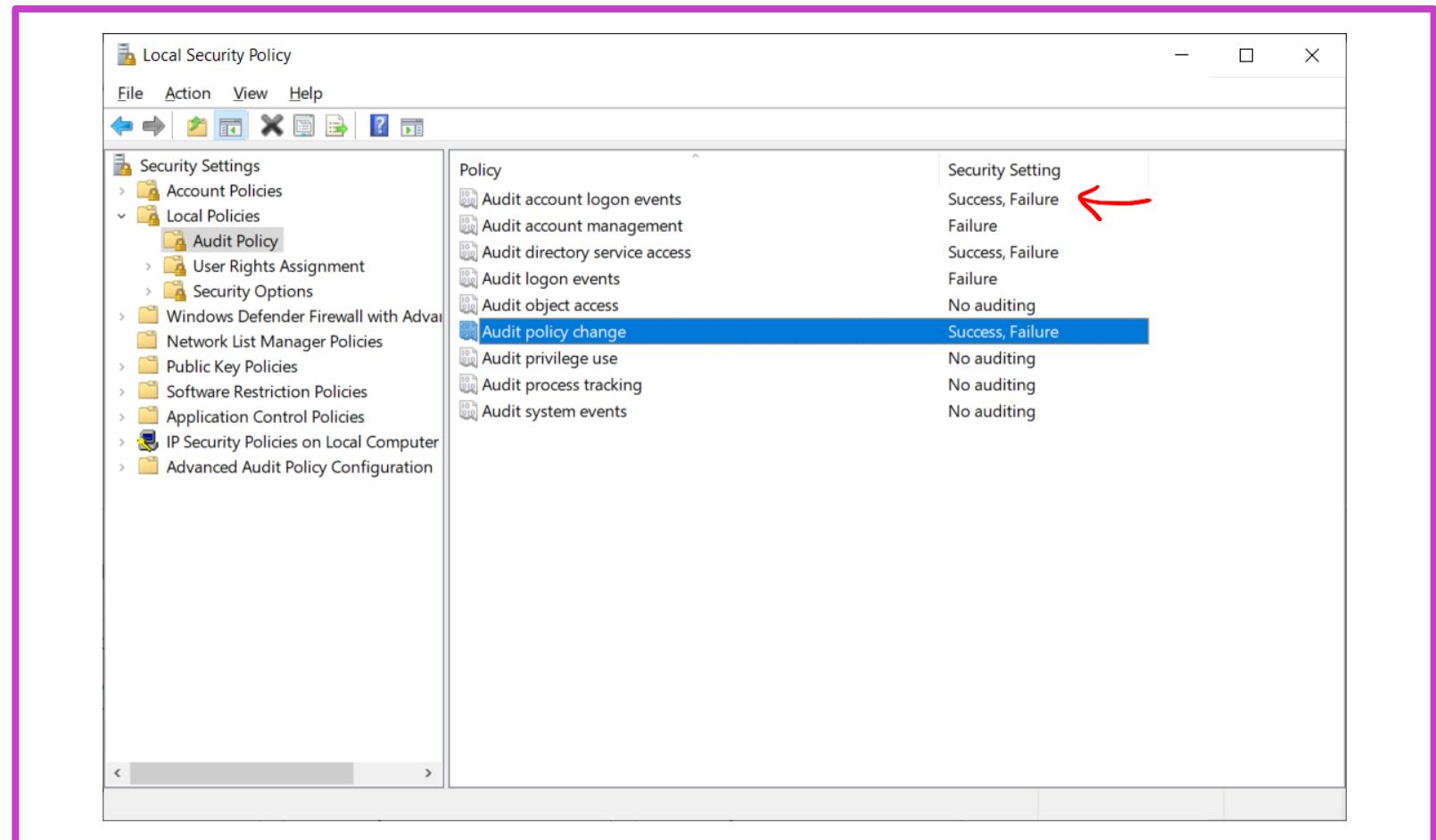
winrm quickconfig

# Implement Windows Server Auditing and Diagnostics

# Describe basic auditing categories (1 of 2)

## Basic auditing values:

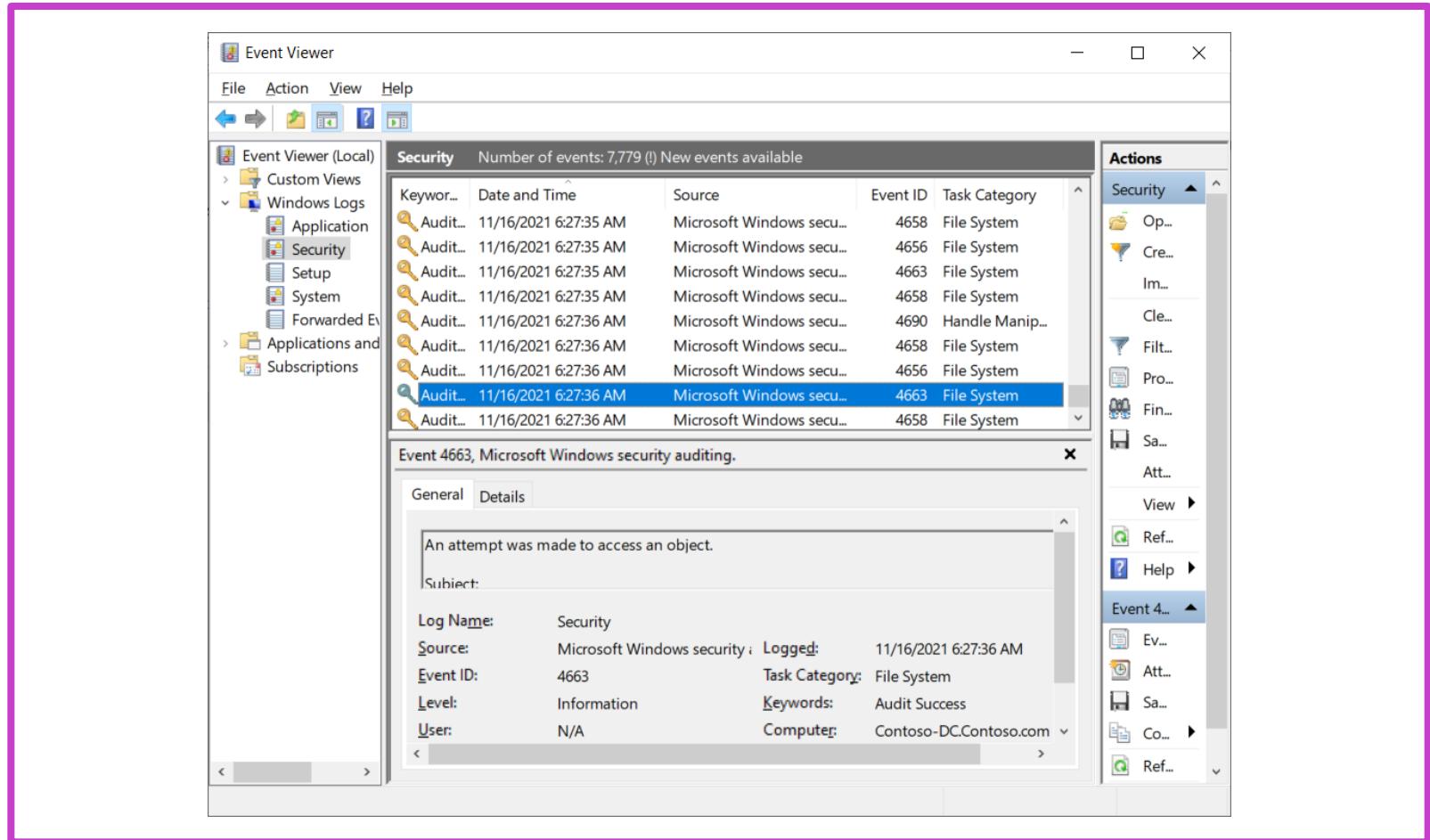
- Audit account logon events
- Audit logon events
- Audit account management
- Audit directory service access
- Audit policy change
- Audit privilege use
- Audit system events
- Audit process tracking
- Audit object access



# Describe basic auditing categories (2 of 2)

Specify auditing settings on a file or folder:

- Typical usage
- Evaluate events in the security log

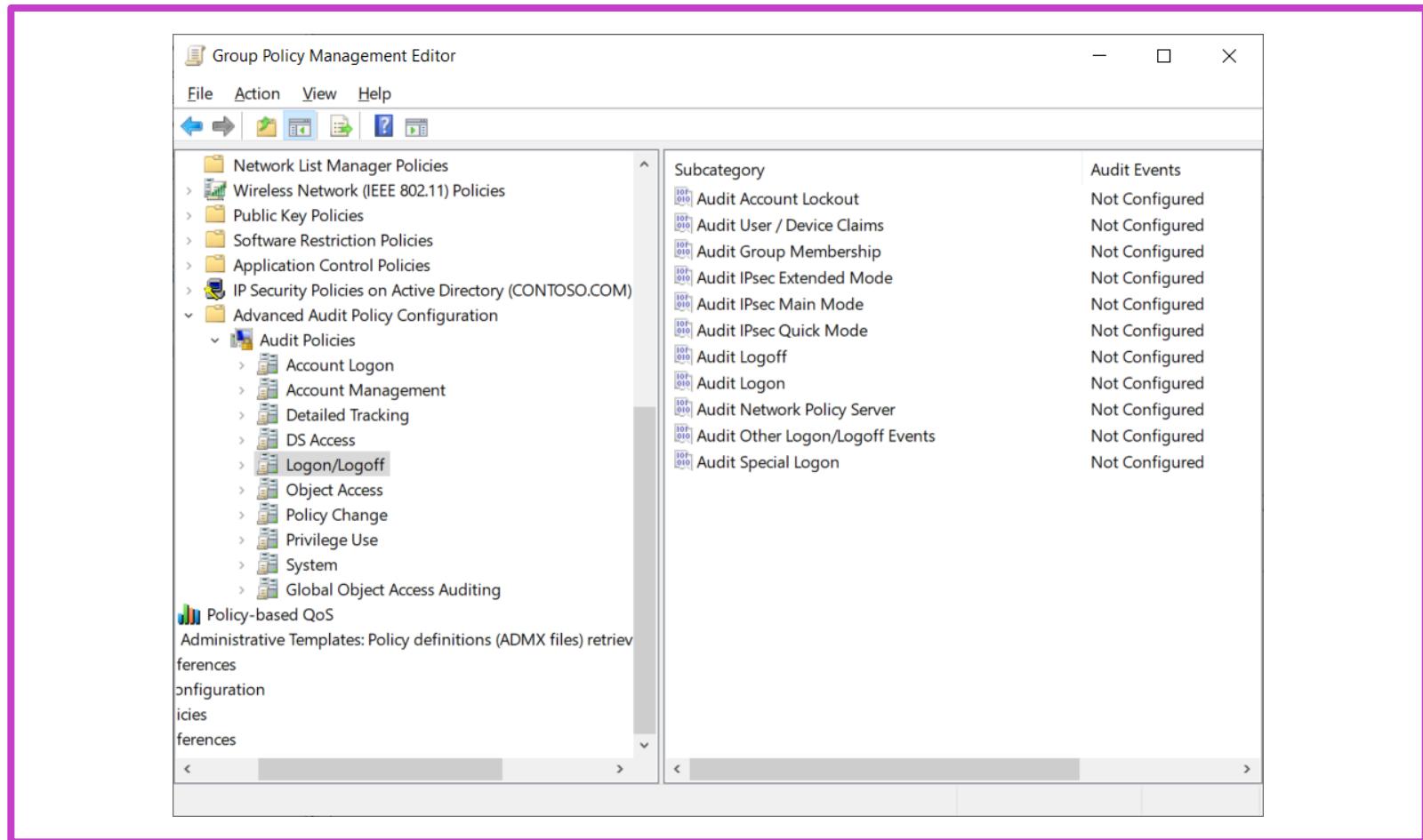


# Describe advanced auditing categories

## Advanced auditing

Ten categories of events, which contain more detailed policy settings. There are over 60 configurable policy settings available.

- Use AuditPol
- Use expression-based audit policies



# Log user access

User Access Logging (UAL) helps you quantify the number of unique client requests of the roles and services on a local server.

**1 What server roles and services are supported?**

**2 What data is logged?**

UAL can log both user and device-related data.

**3 Collect UAL data**

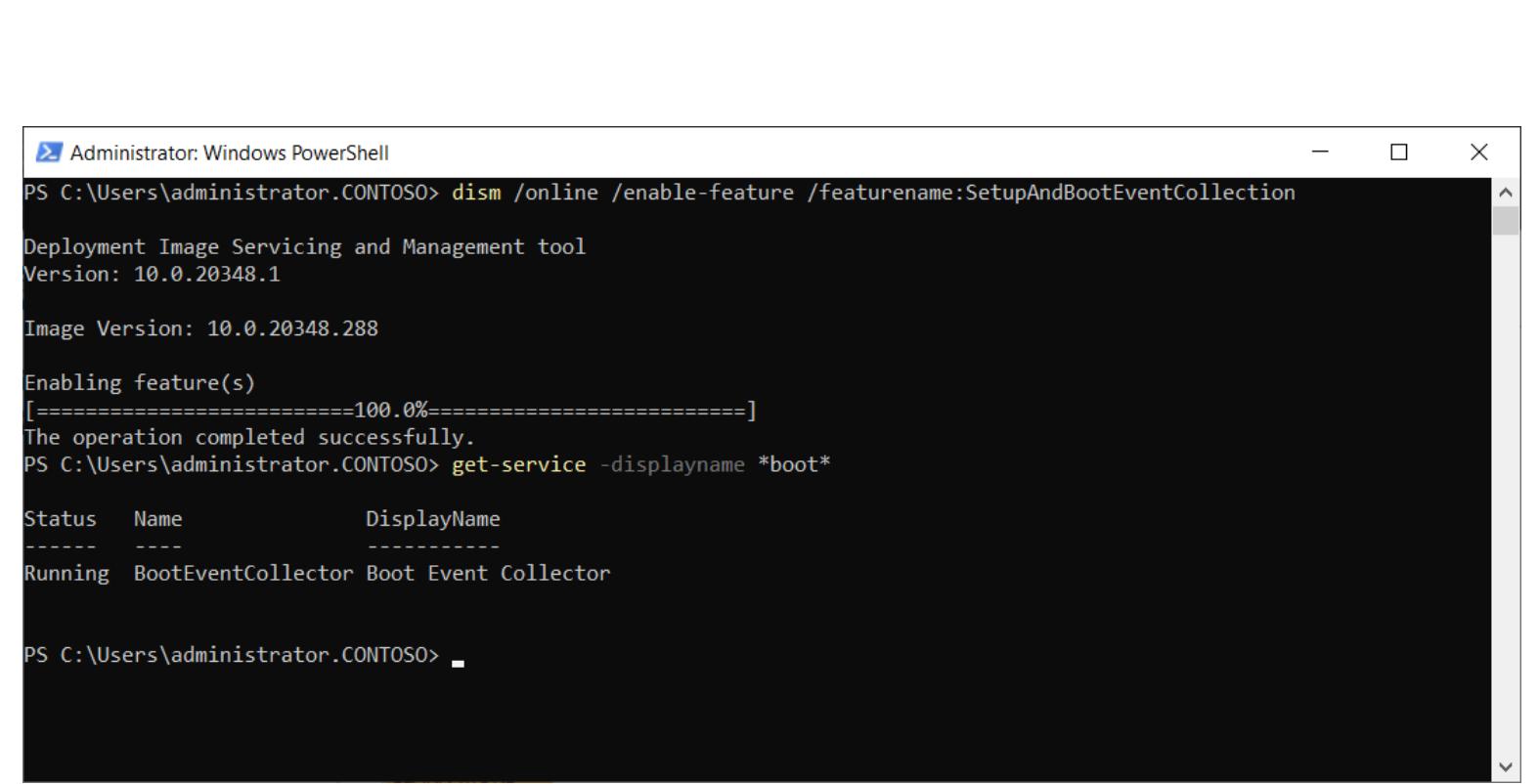
You can use Windows PowerShell to collect UAL data.

# Enable Setup And Boot Event Collection

You can use Setup and Boot Event Collection to review startup and setup events from several source computers on a designated collector computer.

To enable boot event collection:

- Install the collector service
- Configure the collector service
- Review logs



```
Administrator: Windows PowerShell
PS C:\Users\administrator.CONTOSO> dism /online /enable-feature /featurename:SetupAndBootEventCollection
Deployment Image Servicing and Management tool
Version: 10.0.20348.1

Image Version: 10.0.20348.288

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
PS C:\Users\administrator.CONTOSO> get-service -displayname *boot*
Status     Name               DisplayName
-----   -----
Running   BootEventCollector  Boot Event Collector

PS C:\Users\administrator.CONTOSO>
```

# Troubleshoot Active Directory

# Recover Objects from the AD Recycle Bin

Your recovery options depend on whether you have enabled the Active Directory Recycle Bin feature

If you have not enabled Active Directory Recycle Bin, you can reanimate a deleted object if it meets two conditions:

- It must not have reached the end of its tombstone lifetime
- It must not have been scavenged by the garbage collection process

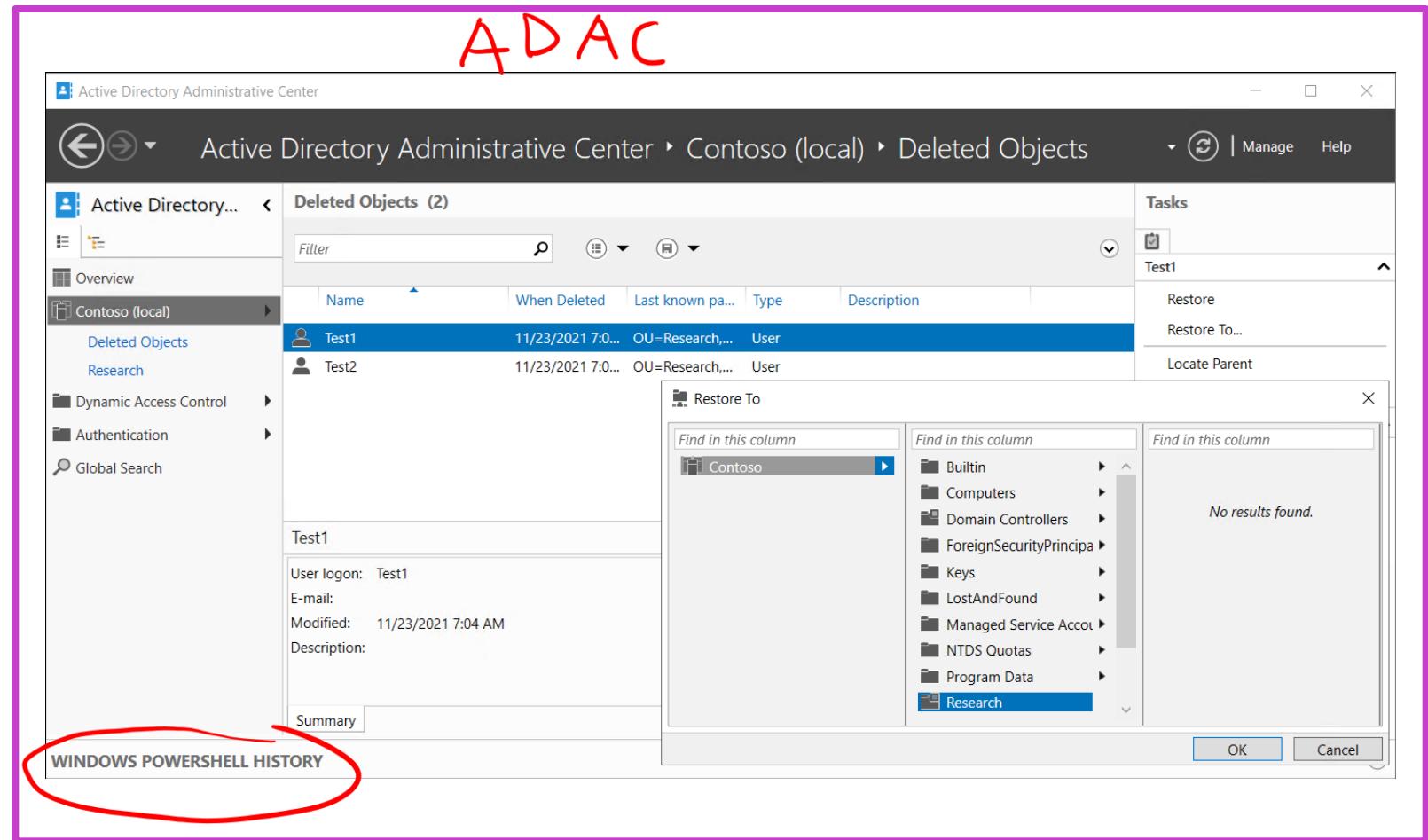
# Recover Objects from the AD Recycle Bin

## Implement Active Directory Recycle Bin

Active Directory Recycle Bin simplifies the process for restoring deleted.

Enabling Active Directory Recycle Bin enables you to:

- Preserve all link-valued and non-link-valued attributes of the deleted Active Directory objects
- Restore the objects to the same consistent logical state that they were in immediately prior to deletion



# Recover the AD DS database (1 of 2)

## What is the AD DS database?

- A collection of files on the domain controller's local file system
- The AD DS database is stored as a file named Ntds.dit

## Manage the AD DS database with NtdsUtil:

- Creating snapshots
- Relocating database files
- Offline defragmentation
- Perform domain-controller metadata cleanup
- Resetting the password used to sign in to the Directory Services Restore Mode (DSRM)

USN

# Recover the AD DS Database (2 of 2)

## What is restartable AD DS?

Windows Server enables administrators to stop and start AD DS just like any other service – Without restarting a domain controller – To perform some management tasks quickly.

You can use the following methods to restart AD DS:

- Services console
- Command prompt
- Windows PowerShell

## Restore Active Directory data

When a domain controller or its directory experiences corruption, damage, or failure, you have several options to restore the system. This requires restarting the domain controller in DSRM.

- Perform nonauthoritative restore
- Perform authoritative restore **USN**

# Recover SYSVOL

GPOs

## What is Group Policy replication?

Group Policy containers and Group Policy templates are both replicated between all domain controllers in a single domain in AD DS.

But these two elements use different replication mechanisms:

- The Group Policy container
- The Group Policy template in SYSVOL

## How to rebuild and recover SYSVOL

Typically, you'll recover SYSVOL as part of a system state restore.

There are a number of ways to perform an authoritative restore of SYSVOL, you can:

- Edit the msDSR-Options attribute
- Perform a system state restore using `wbadmin -authsysvol`

# Troubleshoot AD DS replication (1 of 4)

## Overview

Four Active Directory partitions on each domain controller:

- Domain
- Configuration
- Schema
- Application

Therefore, each domain controller has at least three replicas: the domain partitions for its domain, configuration, and schema.

## How does replication work?

Active Directory replication ensures that all instances of all partitions are synchronized.

It starts this process by building and maintaining a replication topology that ensures no two DCs are more than three hops apart.

# Troubleshoot AD DS replication (2 of 4)

## Available tools for troubleshooting

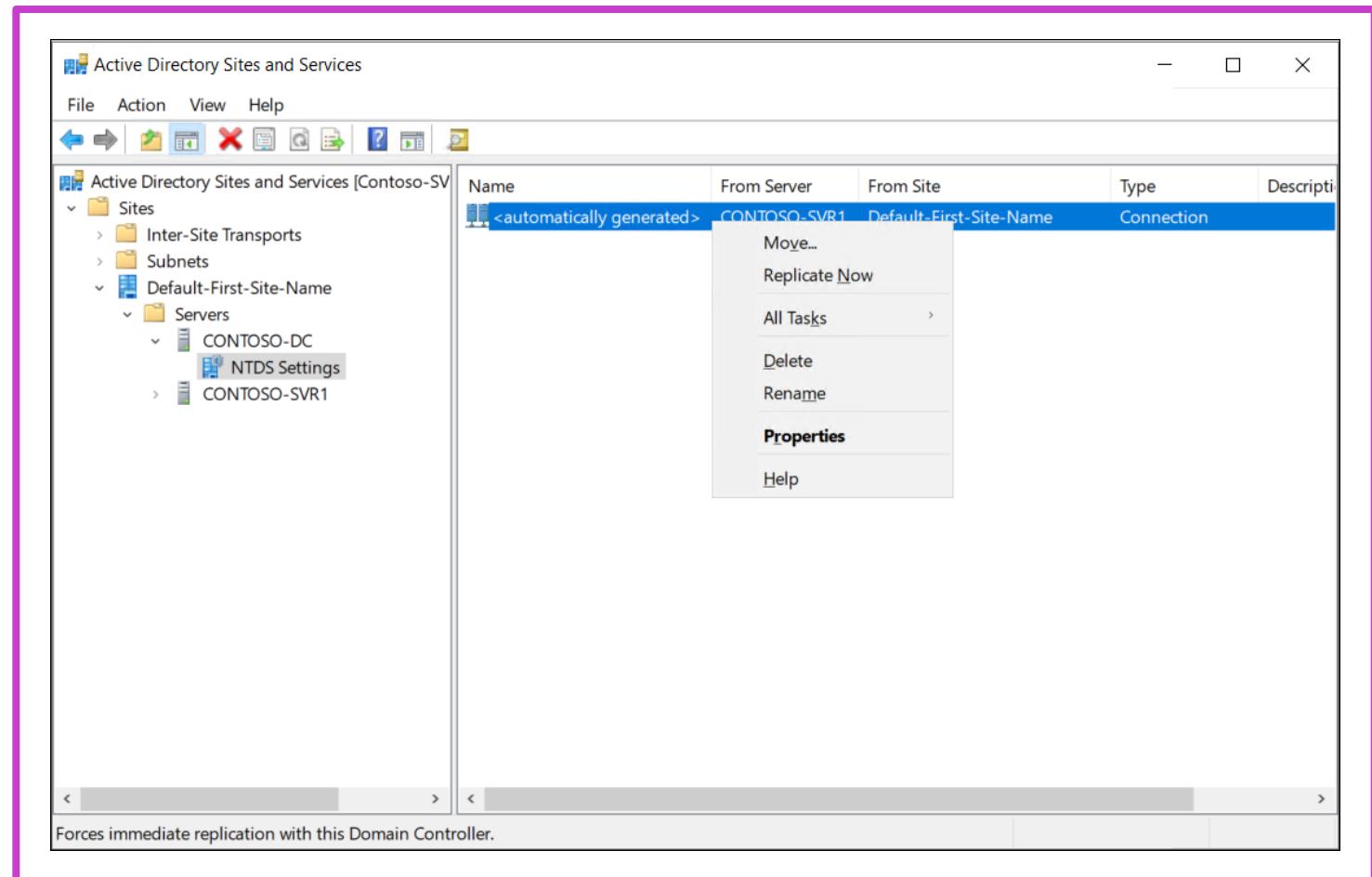
You can investigate and resolve most Active Directory replication using one of two tools:

- Active Directory Sites and Services
- The Repadmin.exe command-line tool

## Use Active Directory Sites and Services

This graphical tool enables you to:

- Determine the replication partners for a given domain controller
- Force replication from listed partner domain controllers



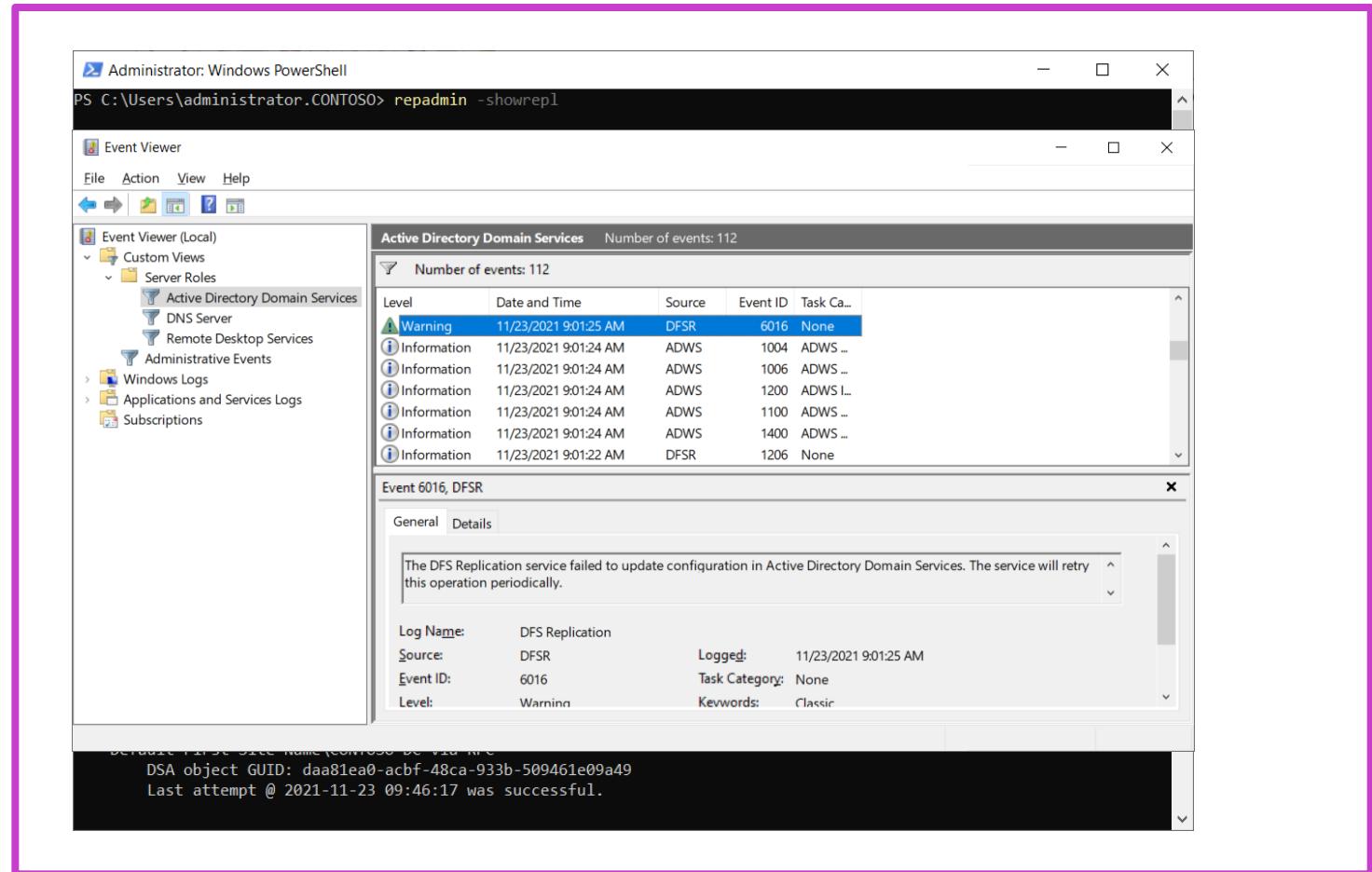
# Troubleshoot AD DS replication (3 of 4)

You can use the Repadmin.exe command-line tool to troubleshoot Active Directory replication:

- Repadmin –replicate
- Repadmin –replsummary
- Repadmin –showrepl
- Repadmin –syncall

Review events in Event Viewer:

Also consider reviewing AD DS logs in Event Viewer. You'll find the logs under the Server Roles node.



# Troubleshoot AD DS replication (4 of 4)

## Manage operation masters

Although AD DS is multimaster, there are certain operations can be performed only by a specific role, on a specific domain controller. A domain controller that holds one of these roles is an operations master. Five operations master roles exist.

### The five operations masters' role distribution:

- Each forest has one **schema master** and one **domain naming master**
- Each AD DS domain has one **RID master**, one **Infrastructure master**, and one **PDC emulator**

### The operations masters' functions:

- Domain naming master
- Schema master
- RID master
- Infrastructure master
- PDC emulator master

# Troubleshoot hybrid authentication issues (1 of 3)

## What are the AD DS integration options?

- Extending on-premises AD DS to Azure
- Synchronizing on-premises AD DS with Azure AD
- Synchronizing AD DS with Azure AD by using password hash synchronization
- Implementing SSO between on-premises AD DS and Azure AD

## What is Azure AD Connect?

- Install a Directory synchronization component on a server in your on-premises domain
- Then provide an account with Domain Admin and Enterprise Admin access to on-premises AD DS, and another account with administrator access to Azure AD, and let it run

# Troubleshoot hybrid authentication issues (2 of 3)

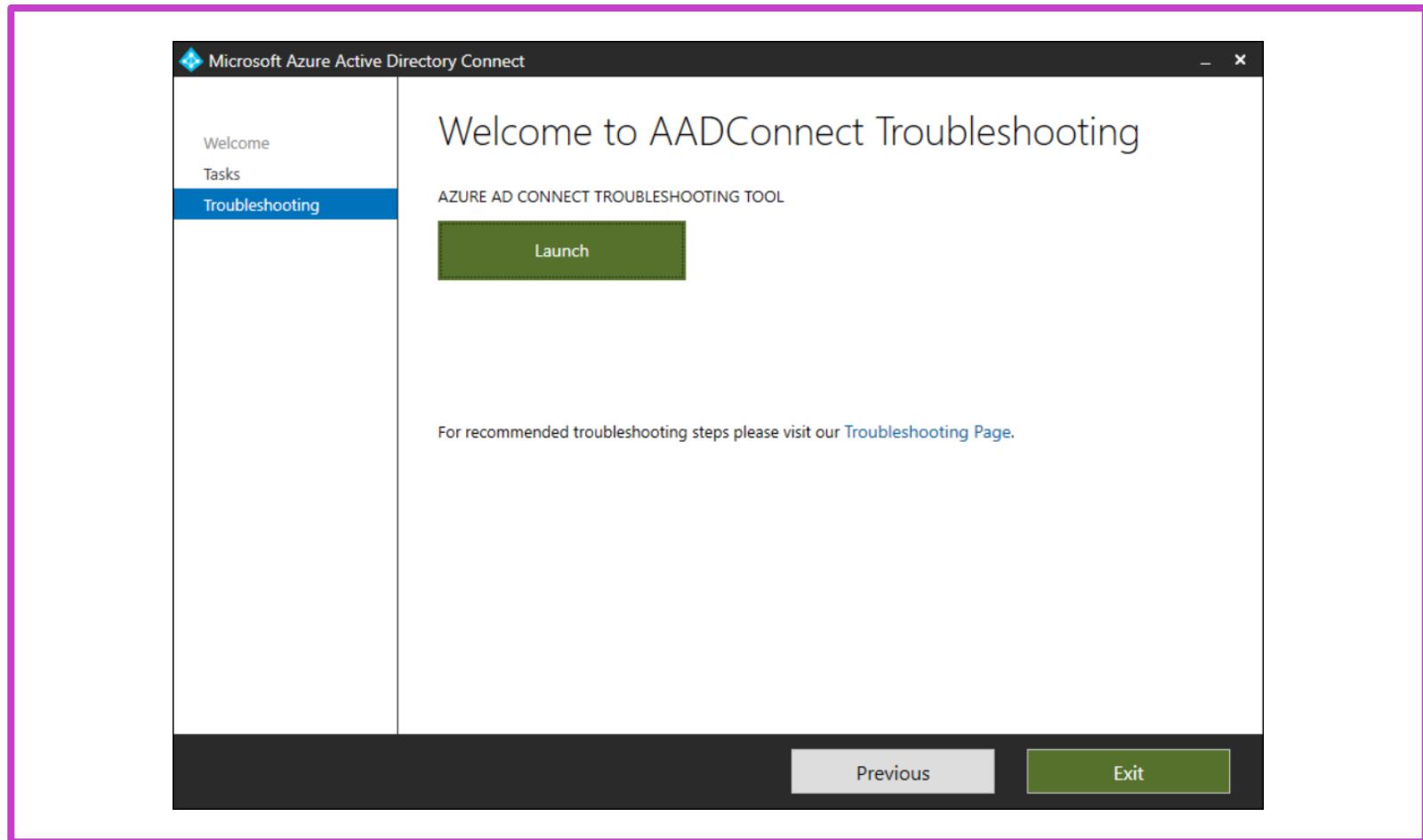
## Prepare to synchronize

A very good way of avoiding problems with synchronizing identities.

## Perform health checks of AD DS

- IdFix tool
- ADModify.NET tool

## Troubleshoot issues with Azure AD Connect sync



# Troubleshoot hybrid authentication issues (3 of 3)

## Monitor Azure AD Connect

The screenshot shows the Azure Active Directory Connect Health dashboard for the Contoso tenant. The main area displays the status of sync services, with a table showing one service named 'M365x.onmicrosoft.com' as 'Unhealthy'. The left sidebar includes links for Quick start, Sync errors, Sync services (which is selected), Active Directory Federation Services, AD FS services, Active Directory Domain Services, AD DS services, Configure (Settings and Role based access control (IAM)), Troubleshooting + SUPPORT (Troubleshoot and New support request), and a TROUBLESHOOTING + SUPPORT section.

## Review Azure AD sign-in logs

The screenshot shows the Azure Active Directory Sign-in logs dashboard for the Contoso tenant. The left sidebar lists various log types: Password reset, Company branding, User settings, Properties, Security, Monitoring (Sign-in logs, Audit logs, Provisioning logs, Log Analytics, Diagnostic settings, and Workbooks), and a note about switching back to the default sign-in experience. The main area displays a table of sign-in logs with columns for timestamp, user principal name, user name, source, and result. The logs show several successful sign-ins from Microsoft 365 and Azure Portal, along with two failure entries at the bottom.

Timestamp	User Principal Name	User Name	Source	Result
11/14/2021, 1:22:15...	cb3826b7-8fd7-4a7...	MOD Administrator	Microsoft App Acces...	Success
11/14/2021, 12:44:25...	3ac29971-344e-45c2...	MOD Administrator	Azure Portal	Success
11/14/2021, 12:44:22...	3ac29971-344e-45c2...	MOD Administrator	Azure Portal	Success
11/13/2021, 10:50:44...	7fe6e13f-9643-4ab5...	MOD Administrator	Bing	Success
11/13/2021, 10:47:32...	b640072f-5eed4-45c2...	MOD Administrator	Microsoft 365 Suppo...	Success
11/13/2021, 10:47:31...	ecf4ee2c-f7b6-4bc2...	MOD Administrator	Microsoft 365 Suppo...	Success
11/13/2021, 10:47:31...	faacb8b0-94cf-43f2...	MOD Administrator	Microsoft 365 Suppo...	Success
11/13/2021, 10:47:31...	b1924367-3300-4fa4...	MOD Administrator	Microsoft 365 Suppo...	Failure
11/13/2021, 10:47:31...	9397b9bc-4c54-4c2...	MOD Administrator	Microsoft 365 Suppo...	Failure
11/13/2021, 10:47:31...	97897db7-247f-4a8...	MOD Administrator	Microsoft 365 Suppo...	Failure

# Lab 08: Monitoring and Troubleshooting Windows Server

# Lab 08 – Monitoring and Troubleshooting Windows Server



## Lab scenario

Contoso, Ltd is a global engineering and manufacturing company with its head office in Seattle, Washington, in the United States. An IT office and datacenter are in Seattle to support the Seattle location and other locations. Contoso recently deployed a Windows Server 2019 server and client infrastructure.

Because the organization deployed new servers, it's important to establish a performance baseline with a typical load for these new servers. You've been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decided to perform centralized monitoring of event logs.

## Objectives

- Establish a performance baseline. ✓
- Identify the source of a performance problem. ✓
- Review and configure centralized event logs. *subscription*

# End of presentation