Microsoft

AZ-801

Configure Windows Server Hybrid Advanced Services

Agenda AZ-801

1 Security – Windows Server
2 Security – Hybrid

3 Failover Cluster

4 Disaster Recovery – Windows Server
5 Disaster Recovery – Hybrid

6 Upgrade and Migrate – Windows Server
7 Migrate Windows Server to the Cloud

8 Monitoring – Windows Server ←
9 Monitoring – Hybrid

DCR

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

Learning Objectives – Monitor Windows Server Performance

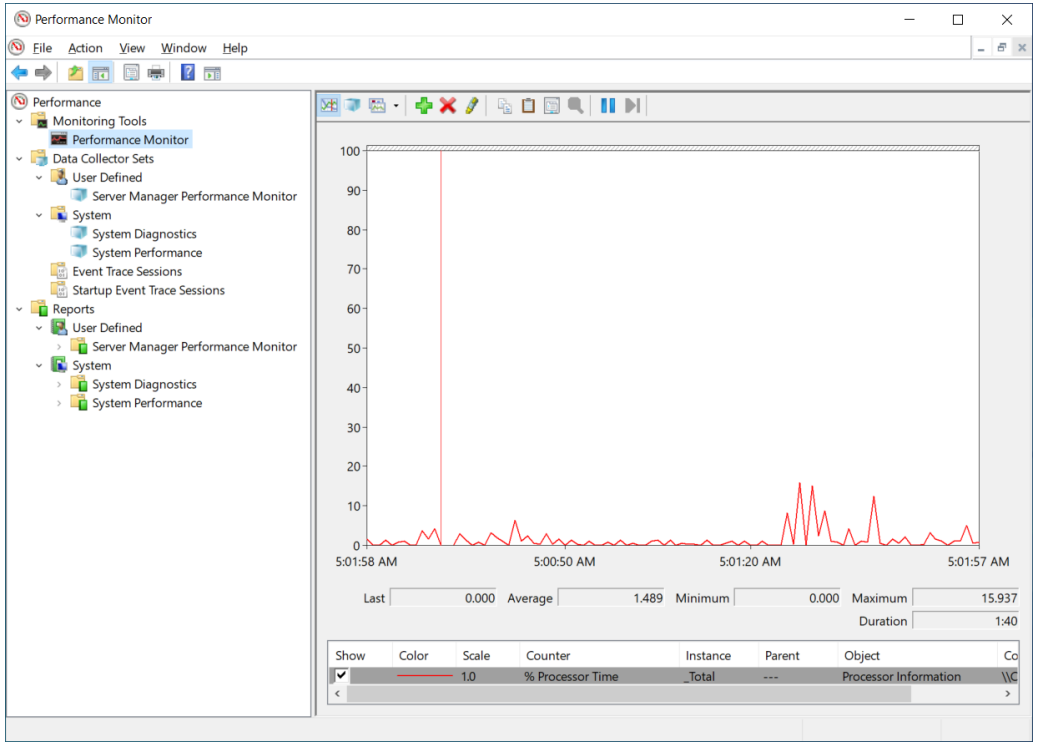
- Use Performance Monitor to identify performance problems
- Use Resource Monitor to review current resource usage
- Review reliability with Reliability Monitor
- Implement a performance monitoring methodology
- Use Data Collector Sets to analyze server performance
- Learning recap

Monitor Windows Server performance (*Continued*)

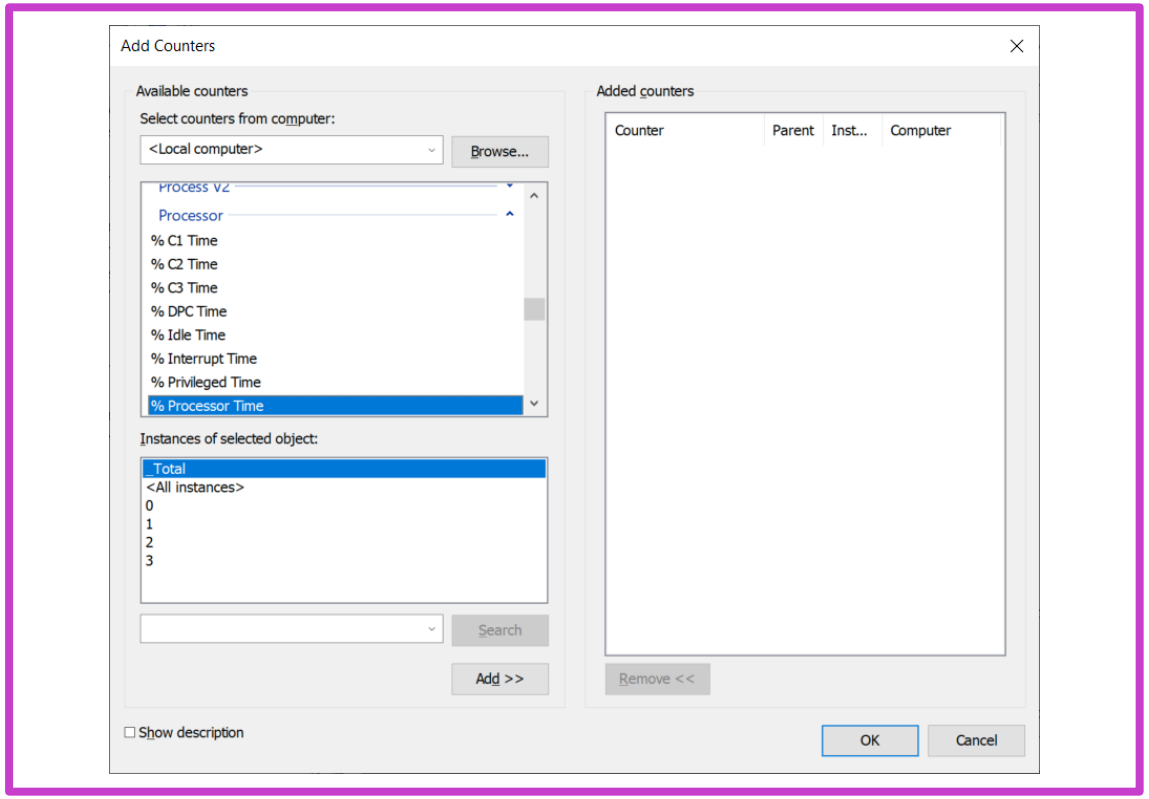
- Monitor network infrastructure services
- Monitor virtual machines running Windows Server
- Monitor performance with Windows Admin Center
- Use System Insights to help predict future capacity issues
- Optimize the performance of Windows Server
- Knowledge check and resources

Use Performance Monitor to identify performance problems

Performance Monitor



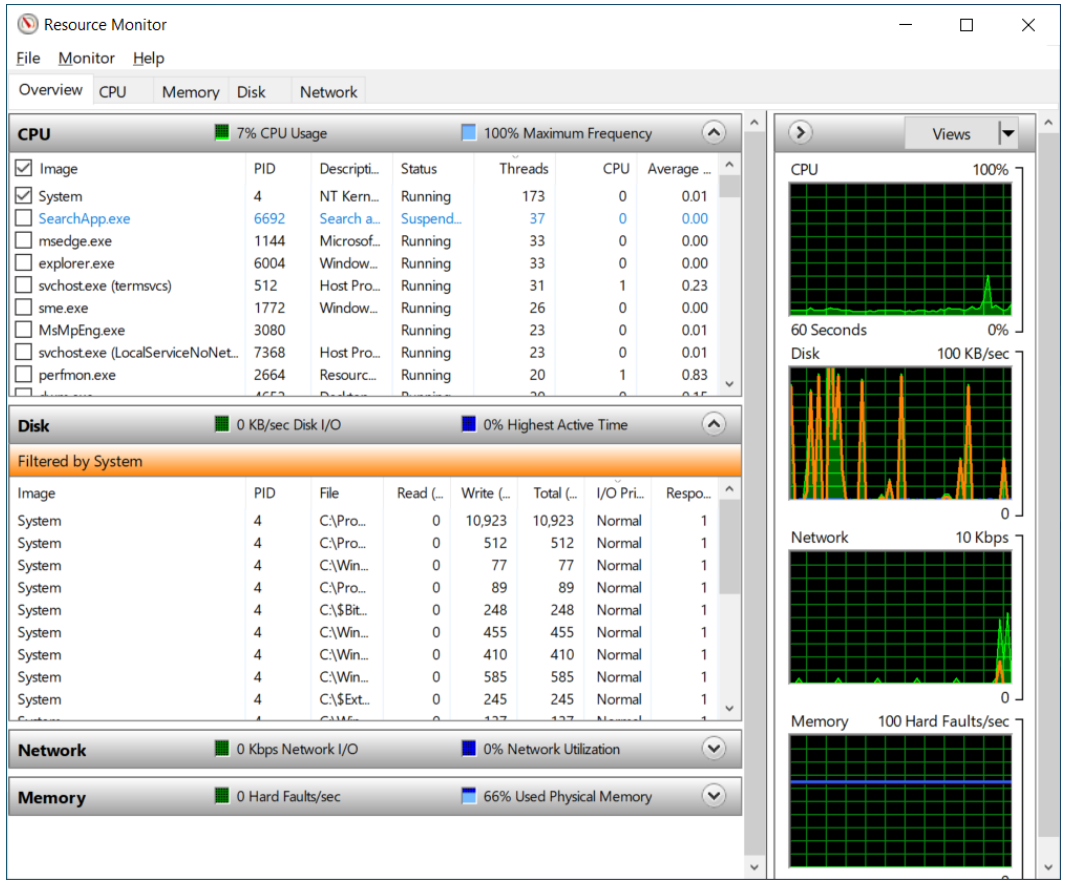
Common performance counters



Use Resource Monitor to review current resource usage

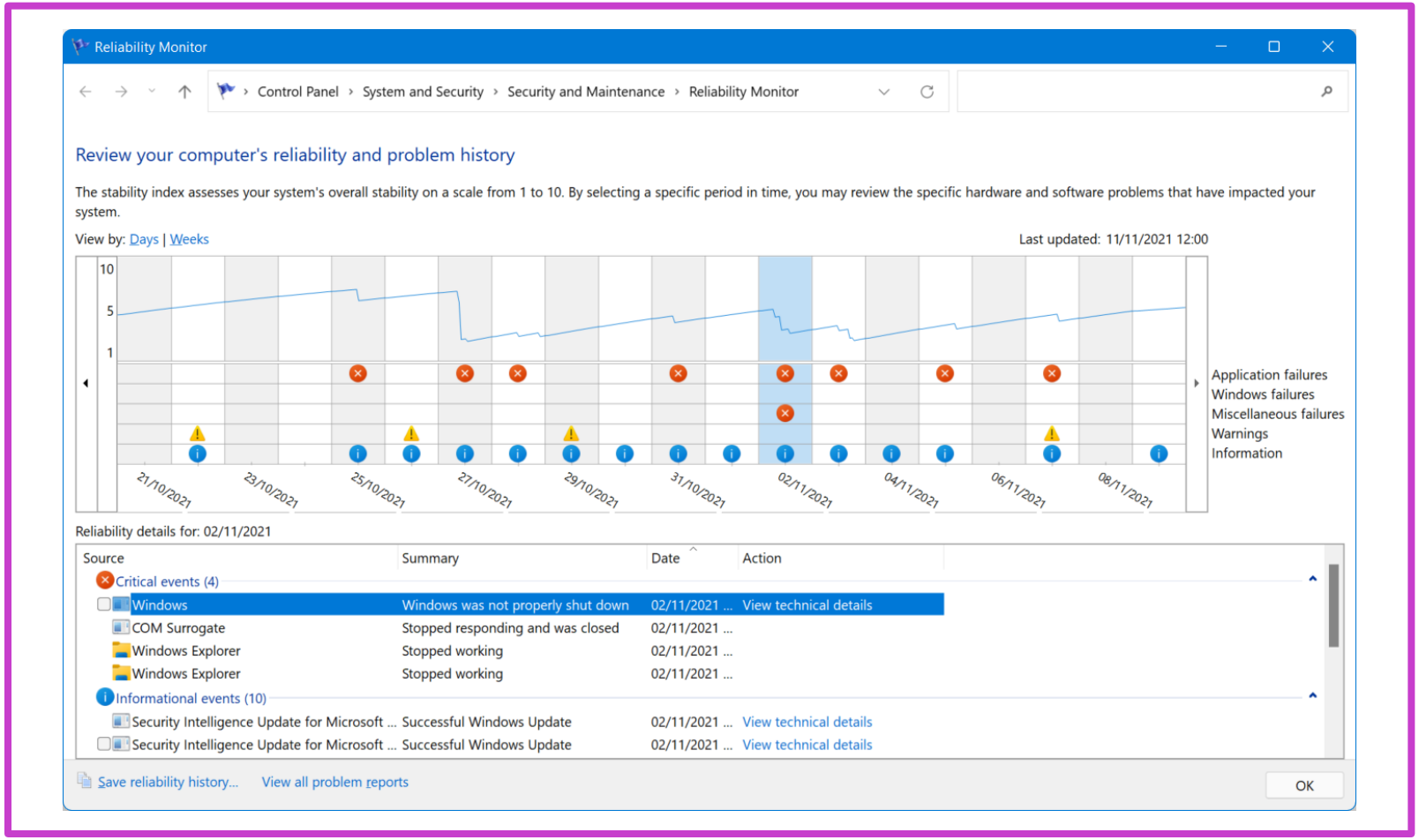
Resource Monitor monitors the use and performance of a CPU, disk, network, and memory resources in real time.

- 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

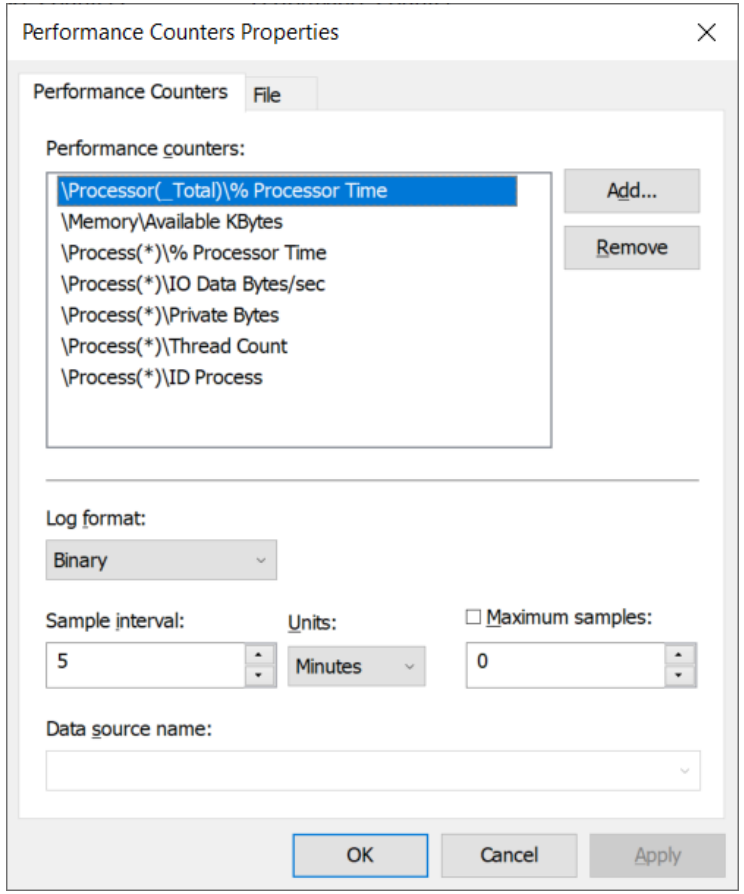
3. **Understand bottlenecks –** Occurs when a computer is unable to service requests for a specific resource or the shortage of a component within an application package might also cause the bottleneck

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

Monitor virtual machines running Windows Server

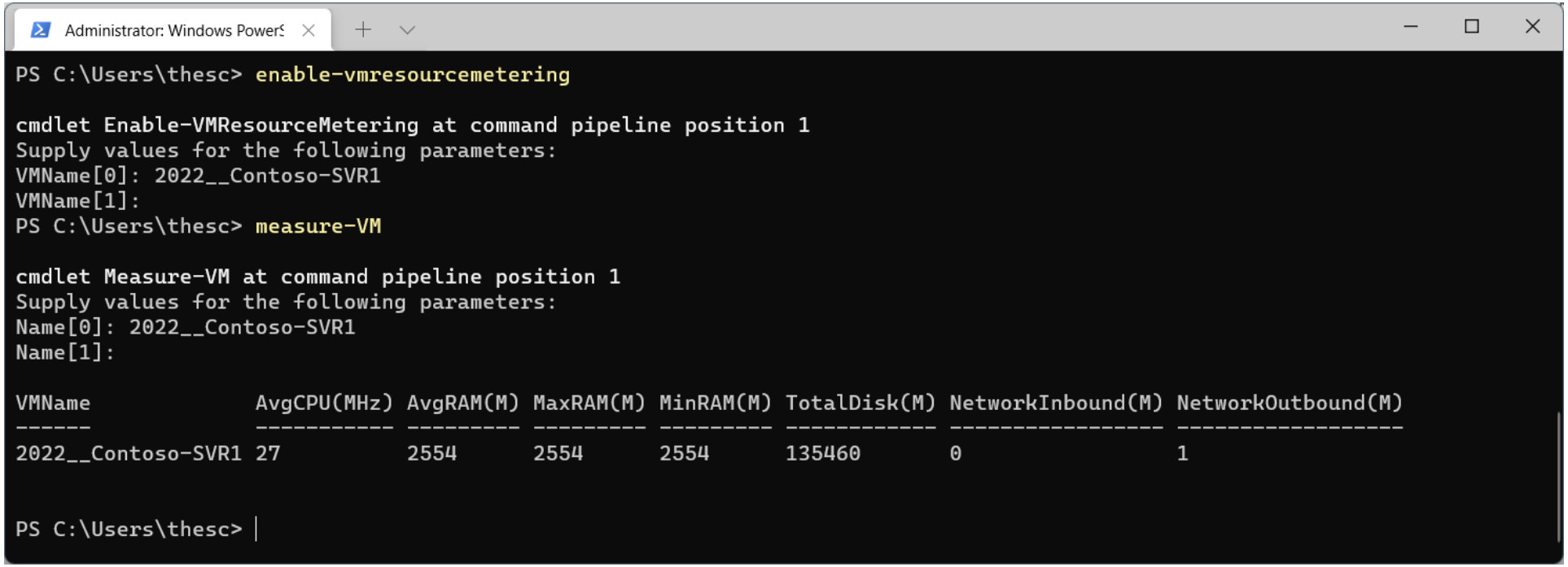
You can use Hyper-V Resource Metering to monitors VMs by measuring below parameters:

- 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

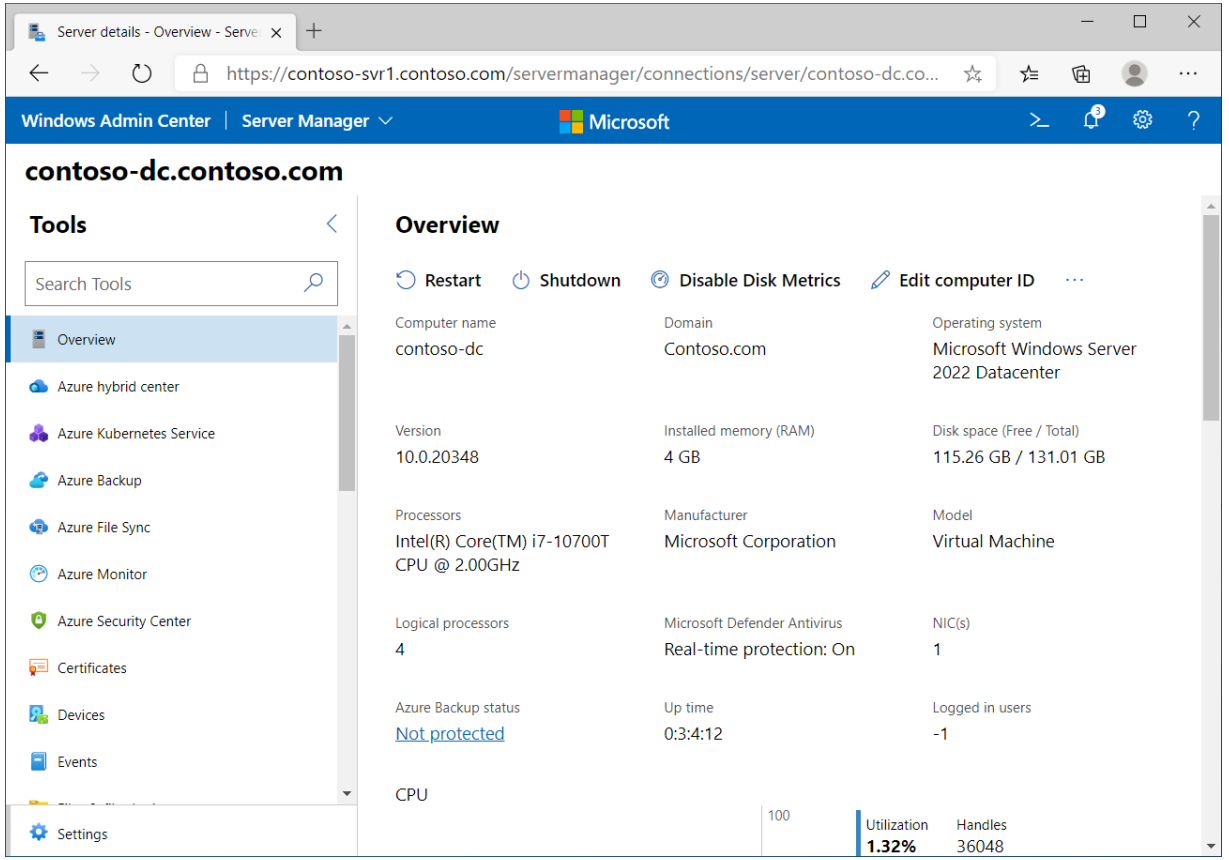


Typical output from the `measure-VM` cmdlet is displayed in the screenshot.

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



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

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

Learning recap – Monitor Windows Server performance

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Monitor Windows Server performance

Manage and monitor Windows Server event logs

Learning Objectives – Manage and monitor Windows Server event logs

- Describe Windows Server event logs
- Use Windows Admin Center to review logs
- Use Server Manager to review logs
- Use custom views
- Implement event log subscriptions
- Learning recap

Describe Windows Server event logs (1 of 2)

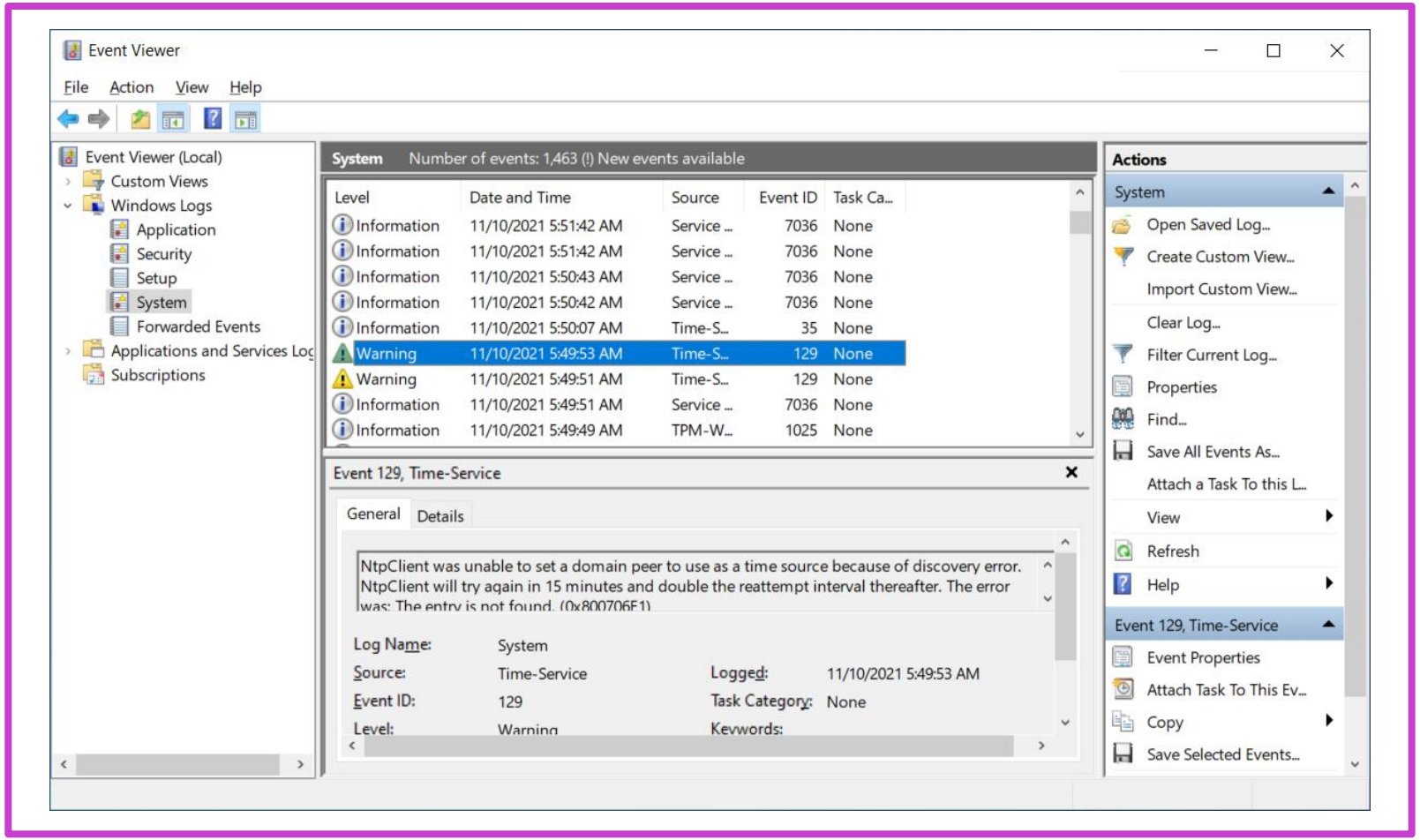
What is Event Viewer?

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



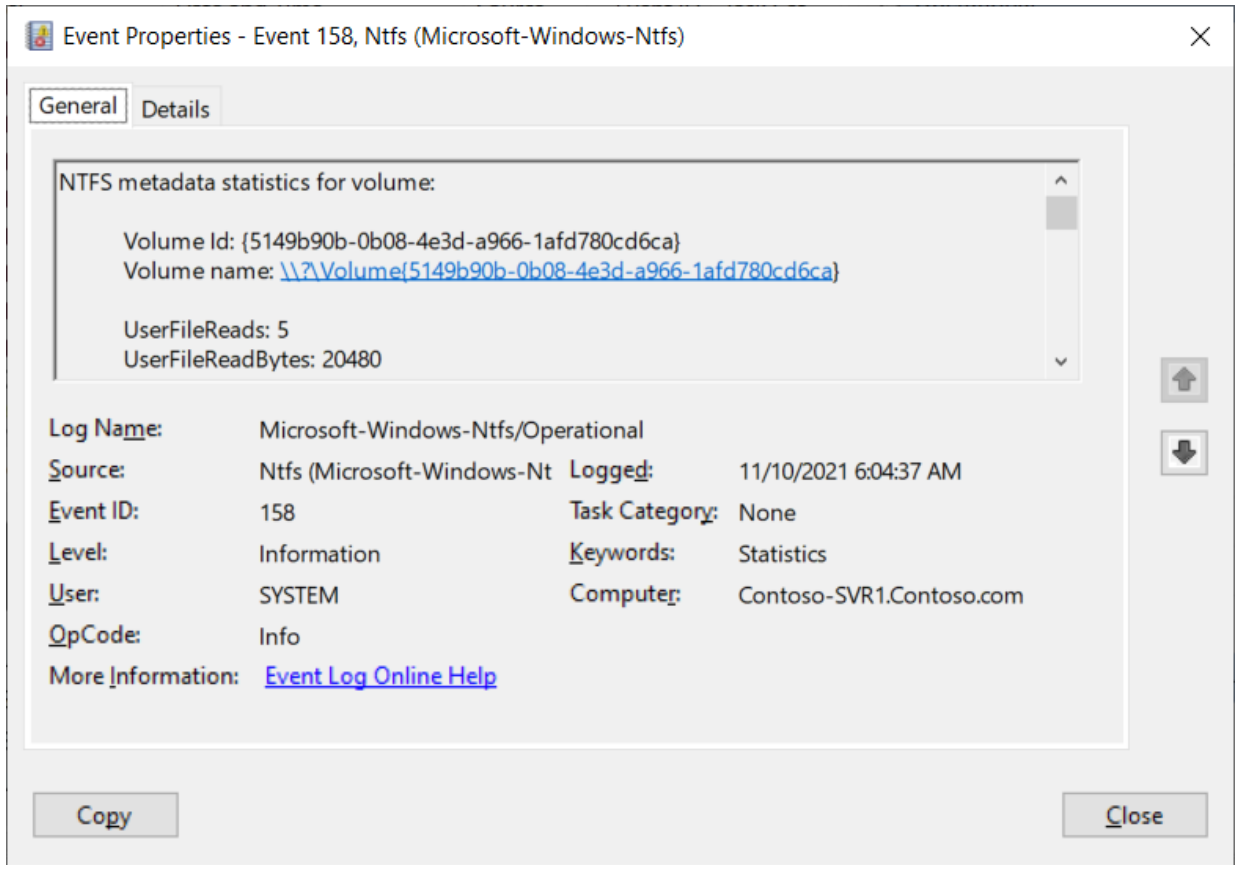
Describe Windows server event logs (2 of 2)

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



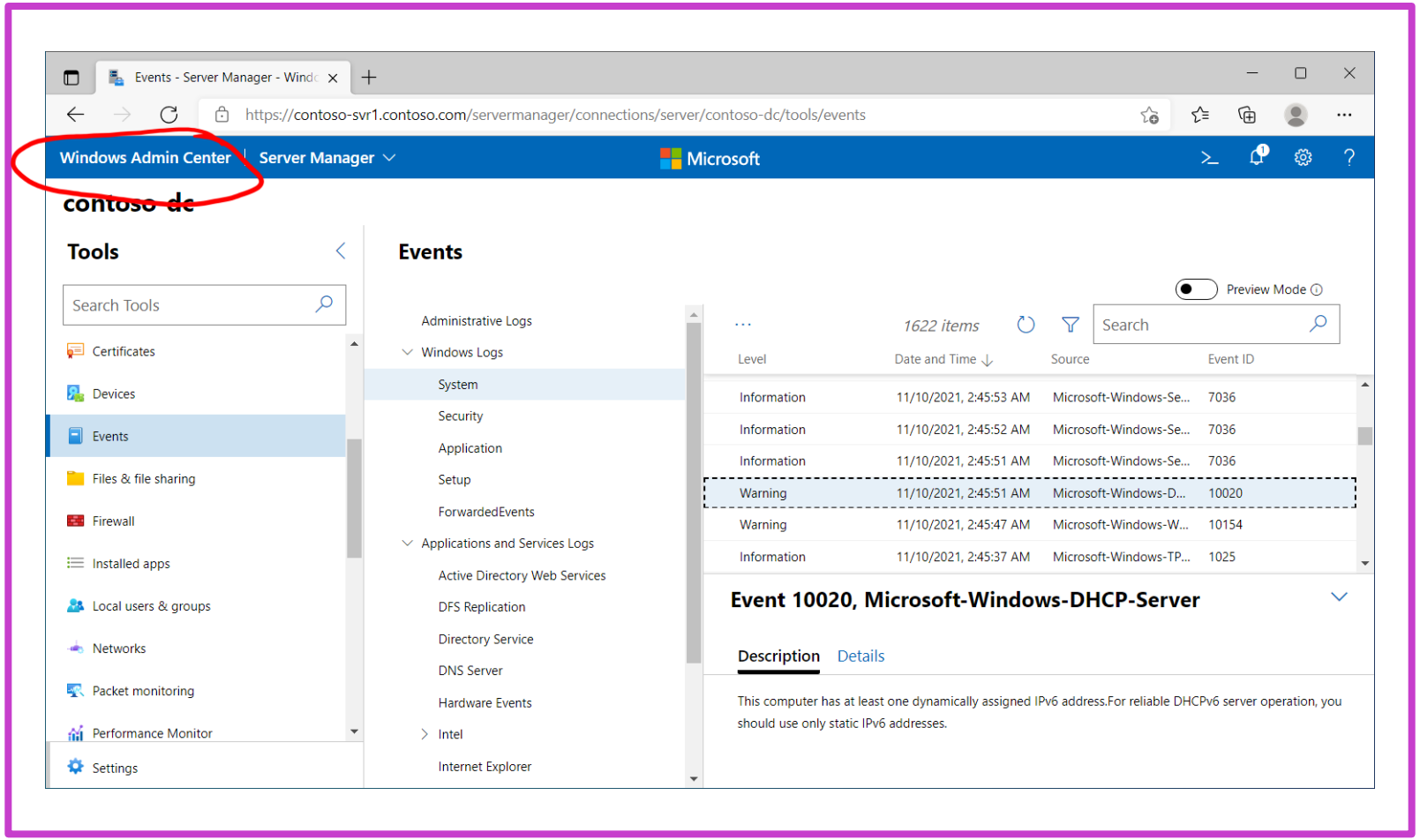
Use Windows Admin Center to review logs (1 of 2)

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.

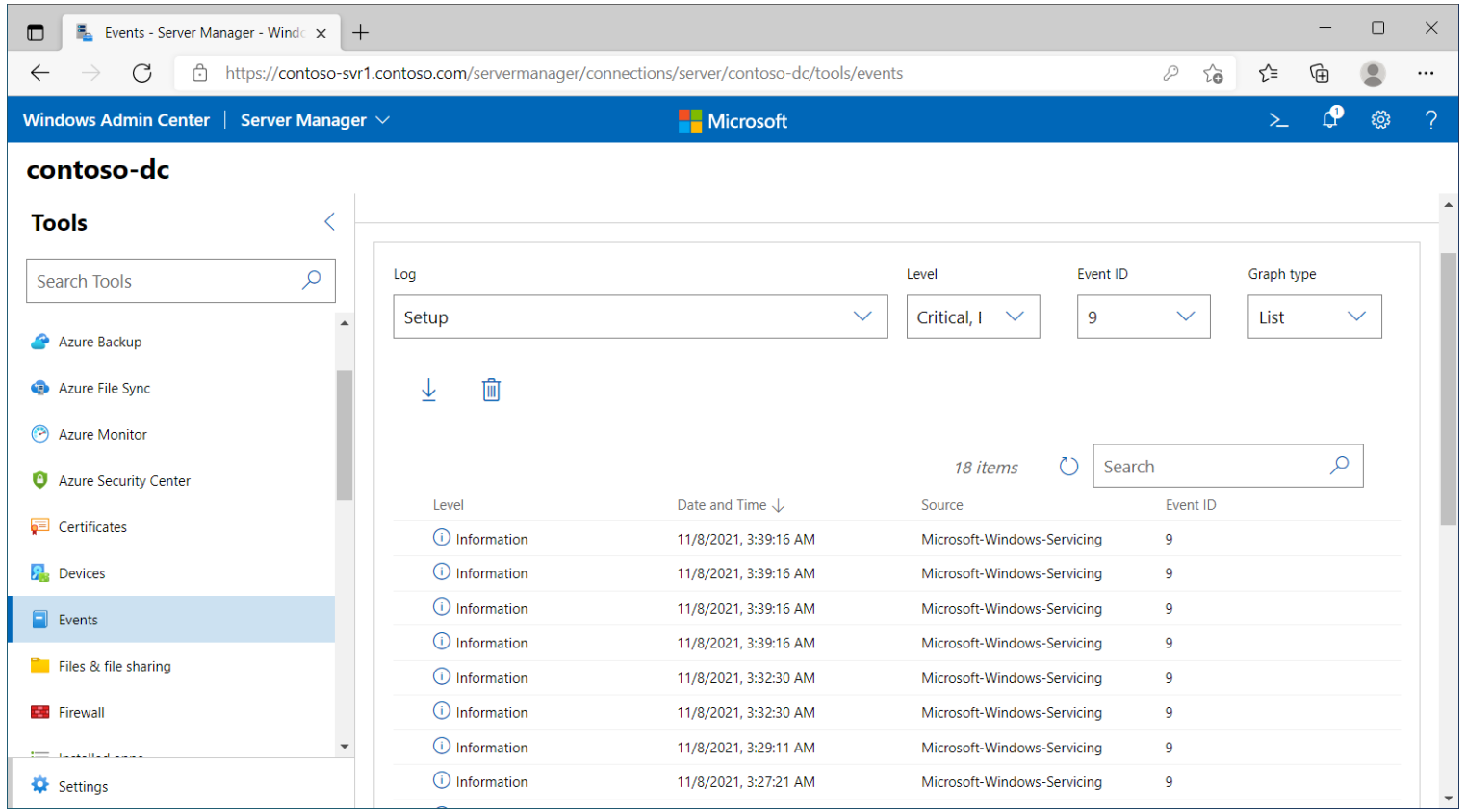


Use Windows Admin Center to review logs (2 of 2)

Use preview features

Use Events to perform the following functions:

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

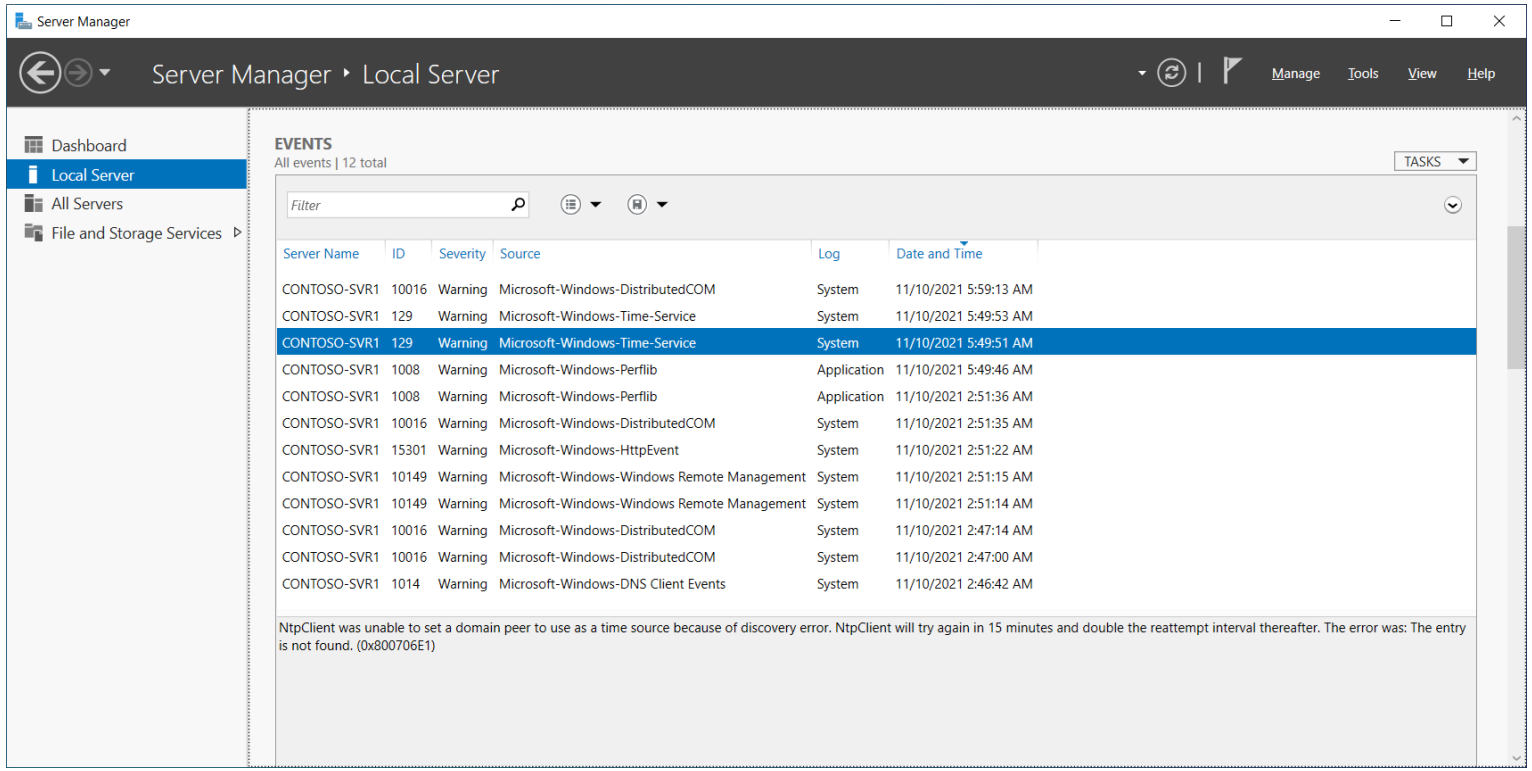


Use Server Manager to review logs (1 of 2)

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.

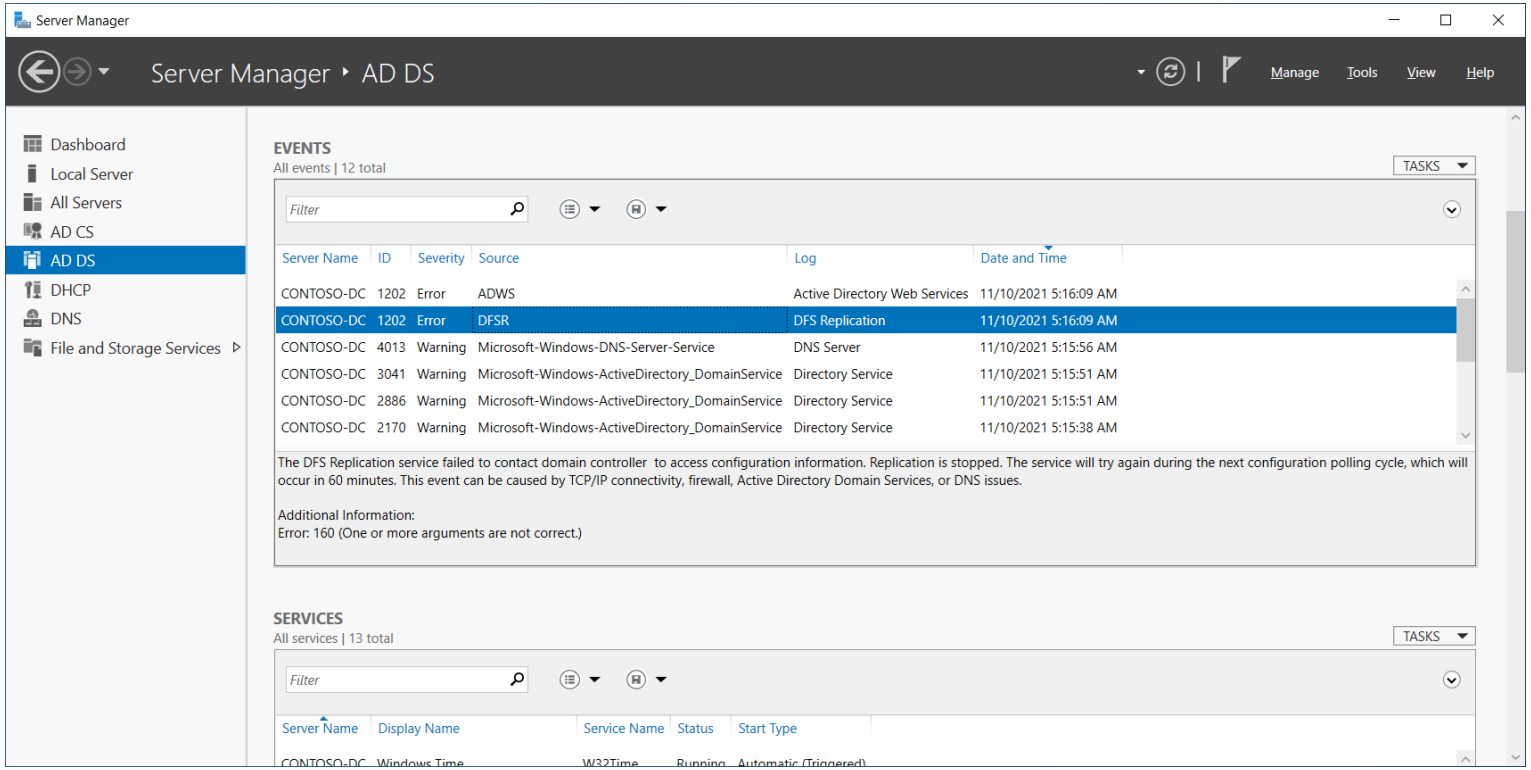
How can you use Server Manager to review logs?

- 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



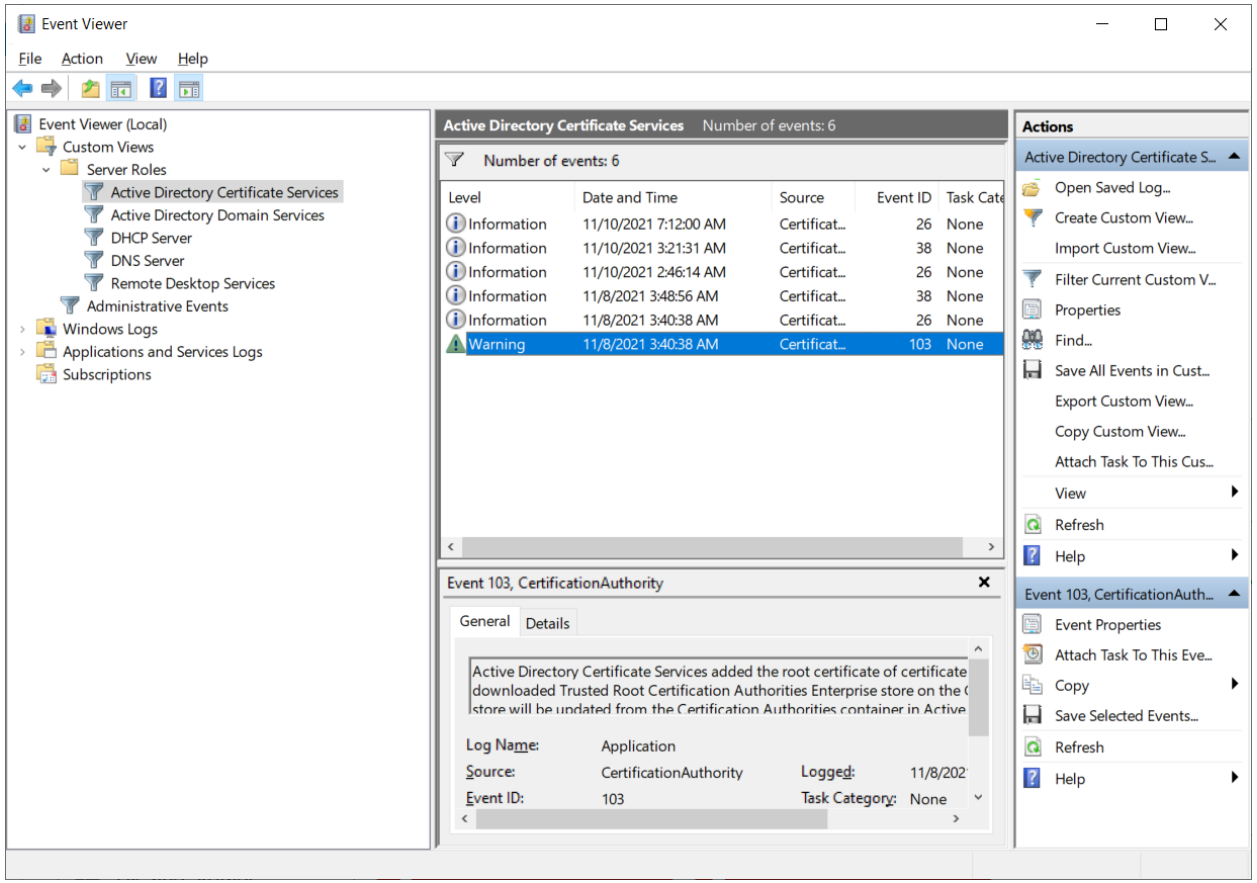
Use custom views

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 Wecsvc
- Both of these services must be running on computers that are participating in the forwarding and collecting process

Learning recap – Manage and Monitor Windows Server Event Logs

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Manage and monitor Windows Server event logs

Implement Windows Server Auditing and Diagnostics

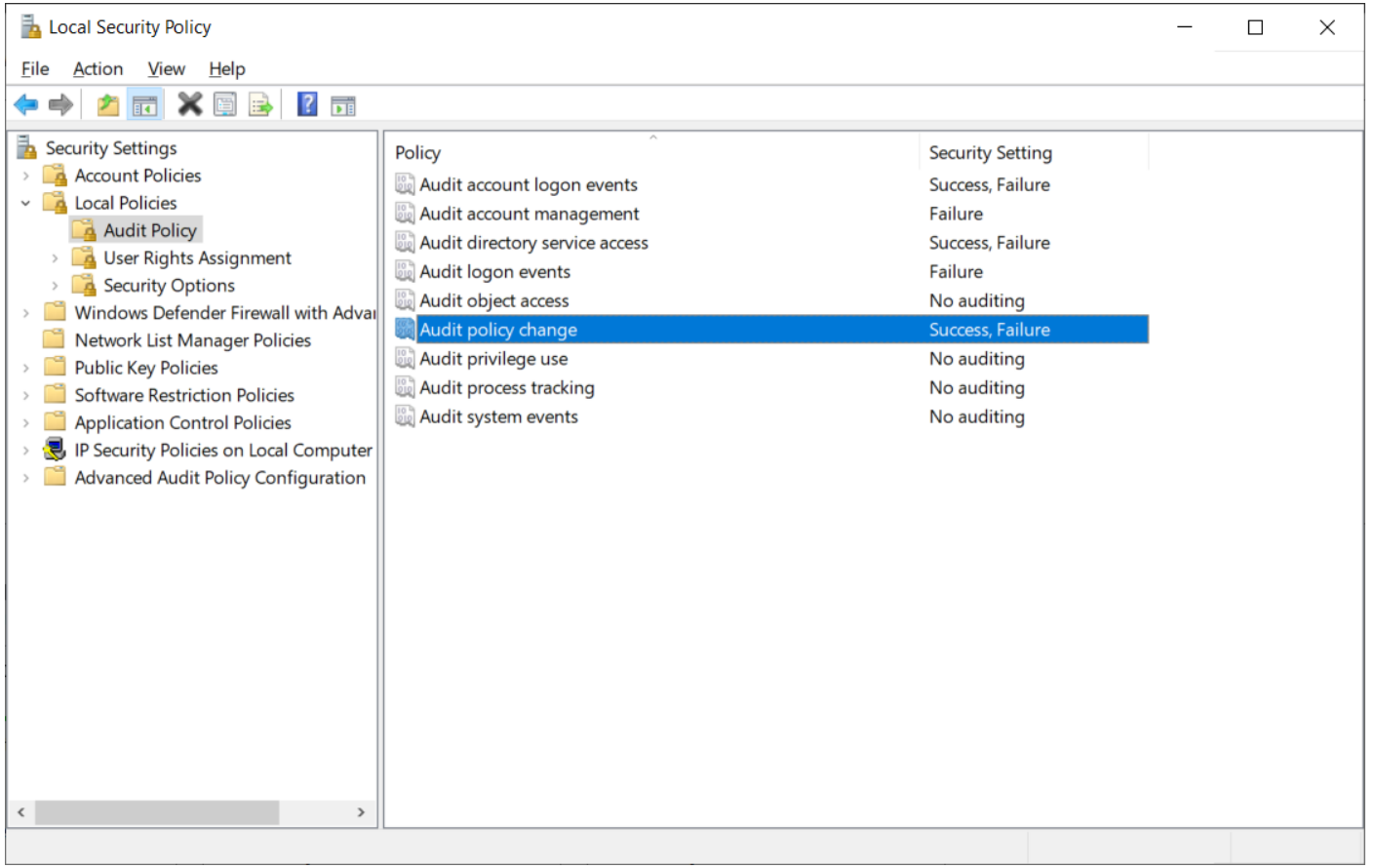
Learning Objectives – Implement Windows Server auditing and diagnostics

- Describe basic auditing categories
- Describe advanced auditing categories
- Log user access
- Enable setup and boot event collection
- Learning recap

Describe basic auditing categories (1 of 2)

Basic auditing values:

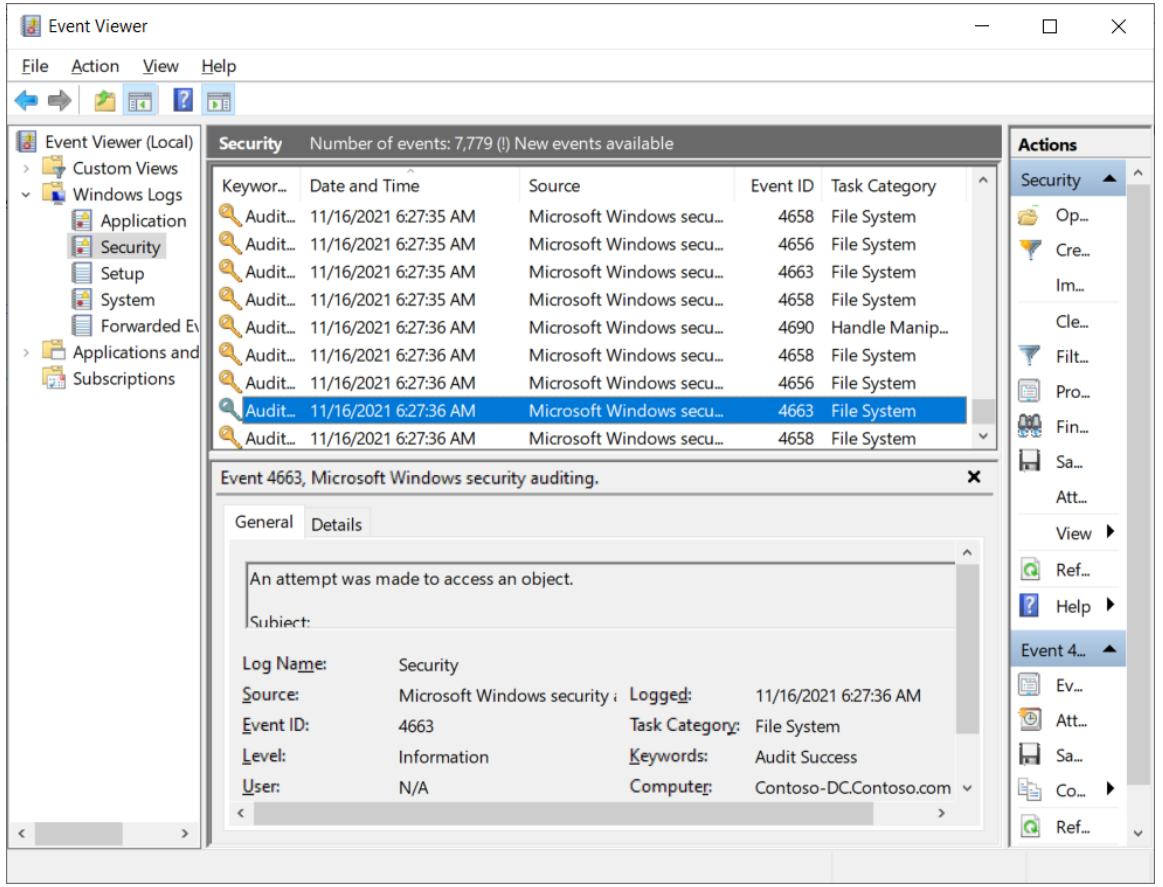
- Audit account logon events
- Audit logon events
- Audit account management
- Audit directory service access
- Audit policy change
- Audit privilege use
- Audit system events
- Audit process tracking
- Audit object access



Describe basic auditing categories (2 of 2)

Specify auditing settings on a file or folder:

- Typical usage
- Evaluate events in the security log

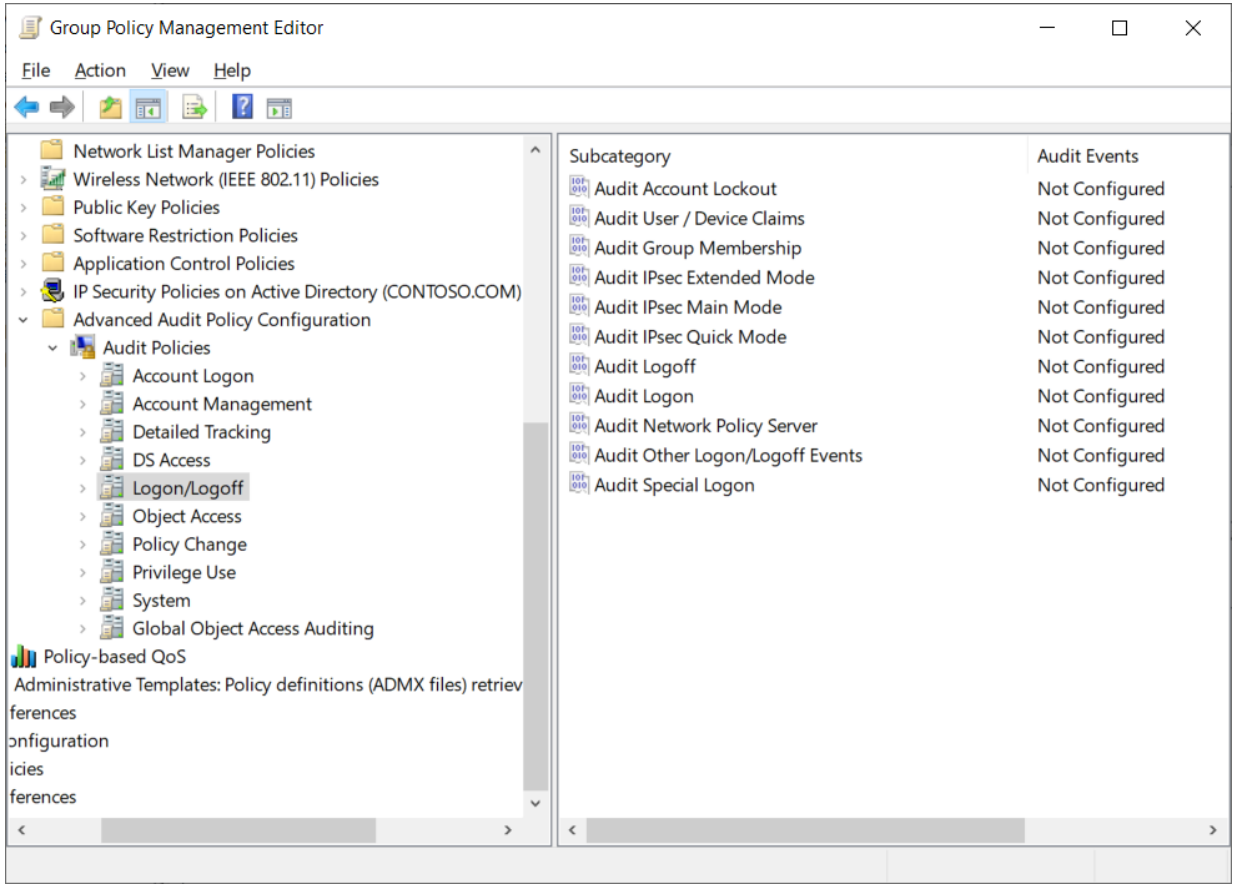


Describe advanced auditing categories

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.

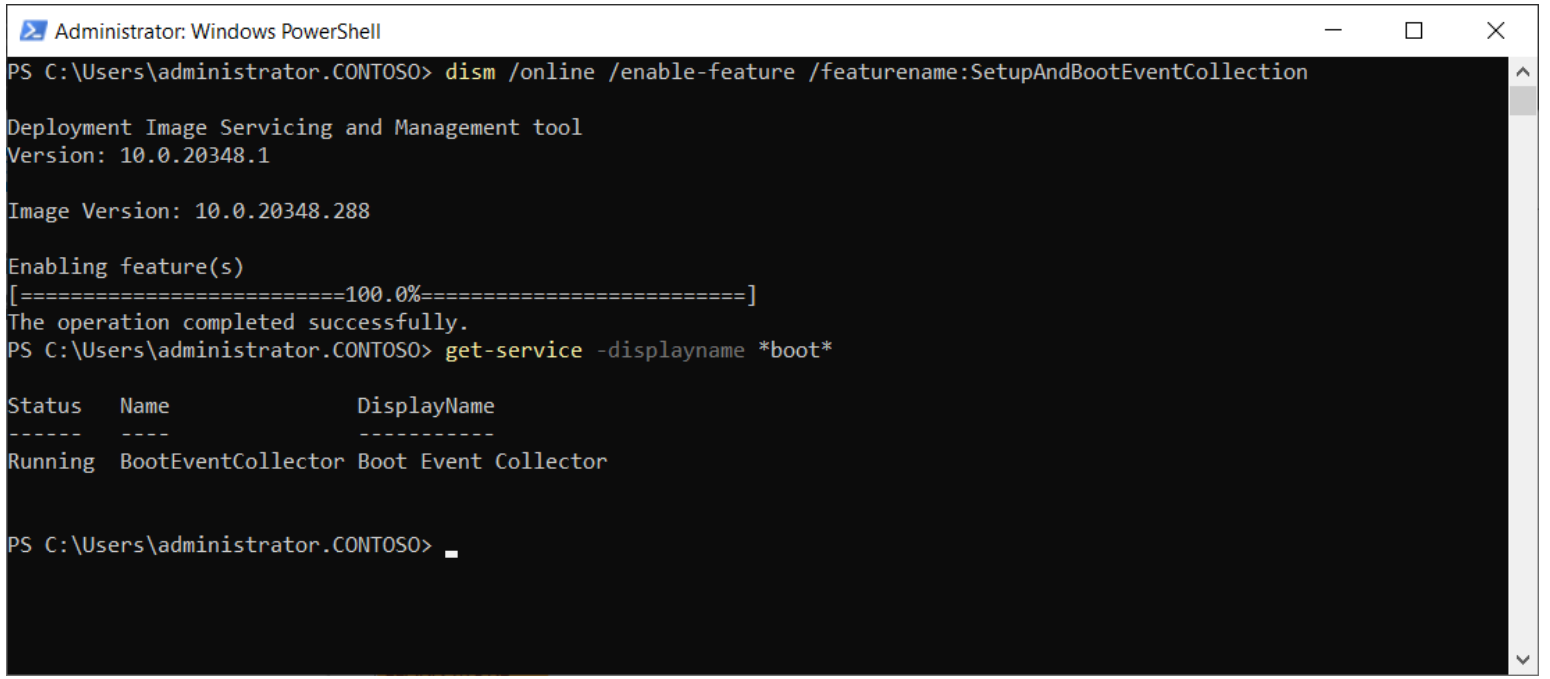
3. **Collect UAL data**
   You can use Windows PowerShell to collect UAL data.

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



Learning recap – Implement Windows Server auditing and diagnostics

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Implement Windows Server auditing and diagnostics

Troubleshoot Active Directory

Learning Objectives – Troubleshoot Active Directory

- Recover objects from the AD recycle bin
- Recover the AD DS database
- Recover SYSVOL
- Troubleshoot AD DS replication
- Troubleshoot hybrid authentication issues
- Learning recap

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

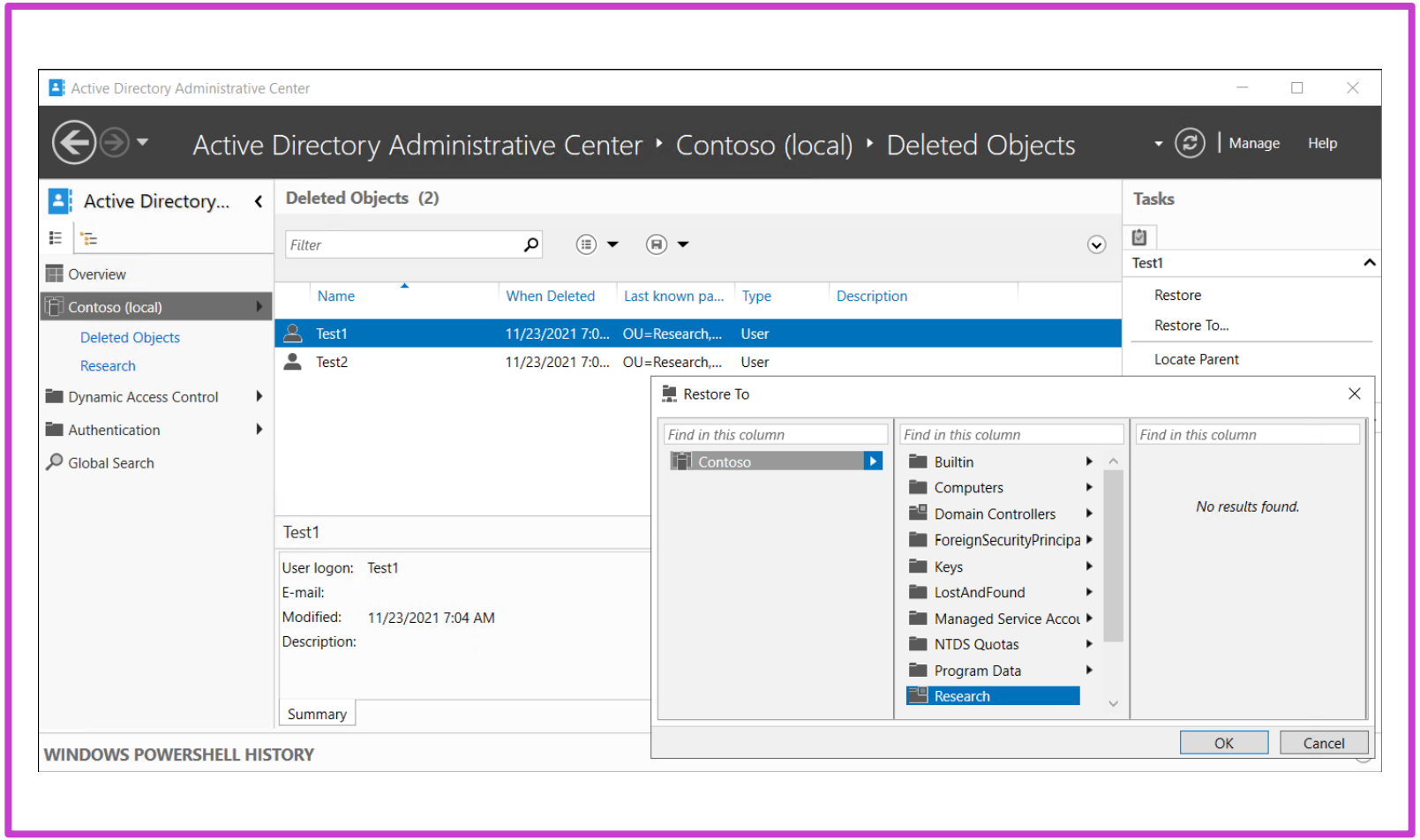
Recover Objects from the AD Recycle Bin

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)

ntds.dit
ntdsutil voles

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)

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

Recover SYSVOL

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 `msDFSR-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

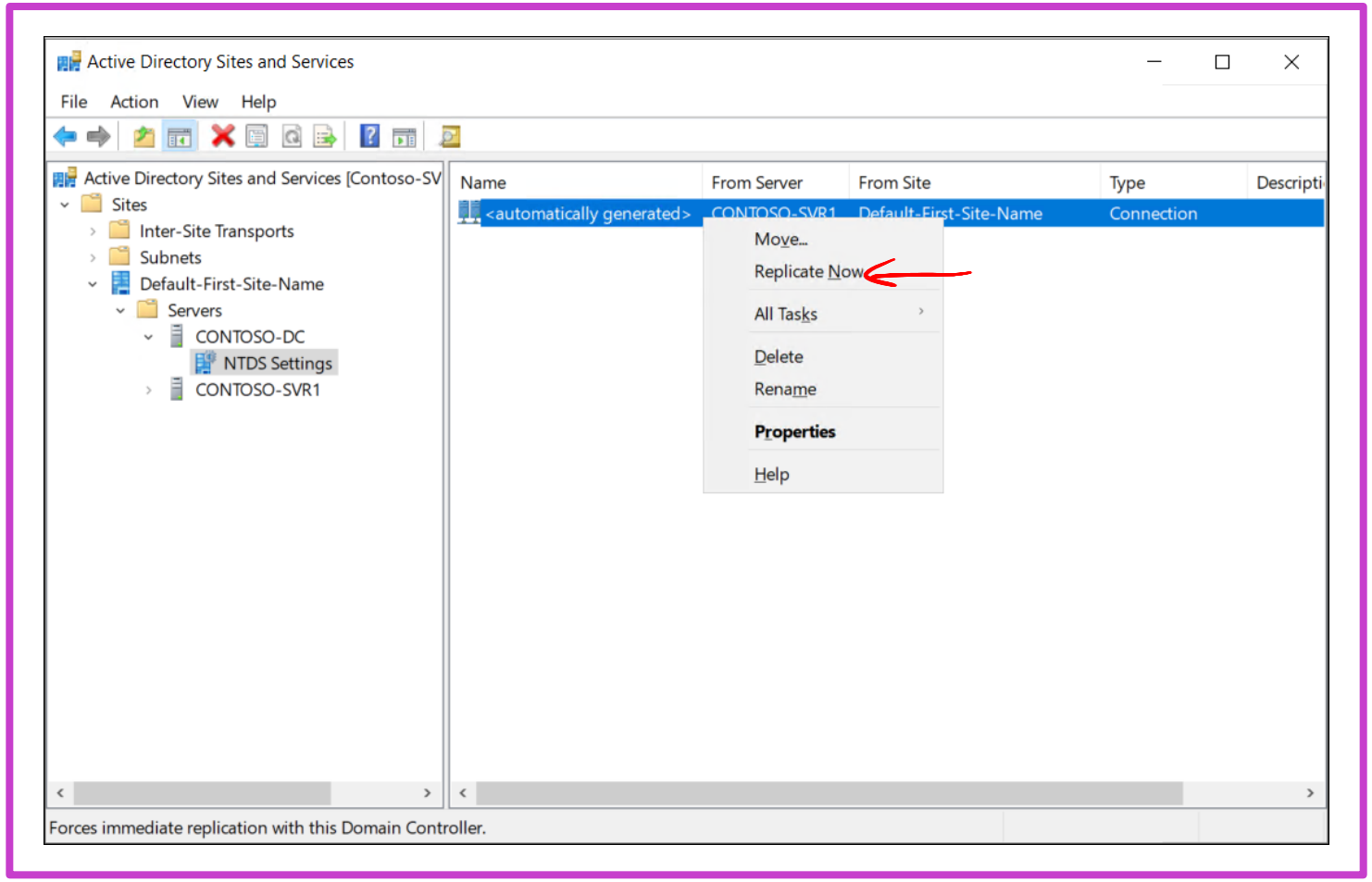
You can investigate and resolve most Active Directory replication using one of two tools:

- 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



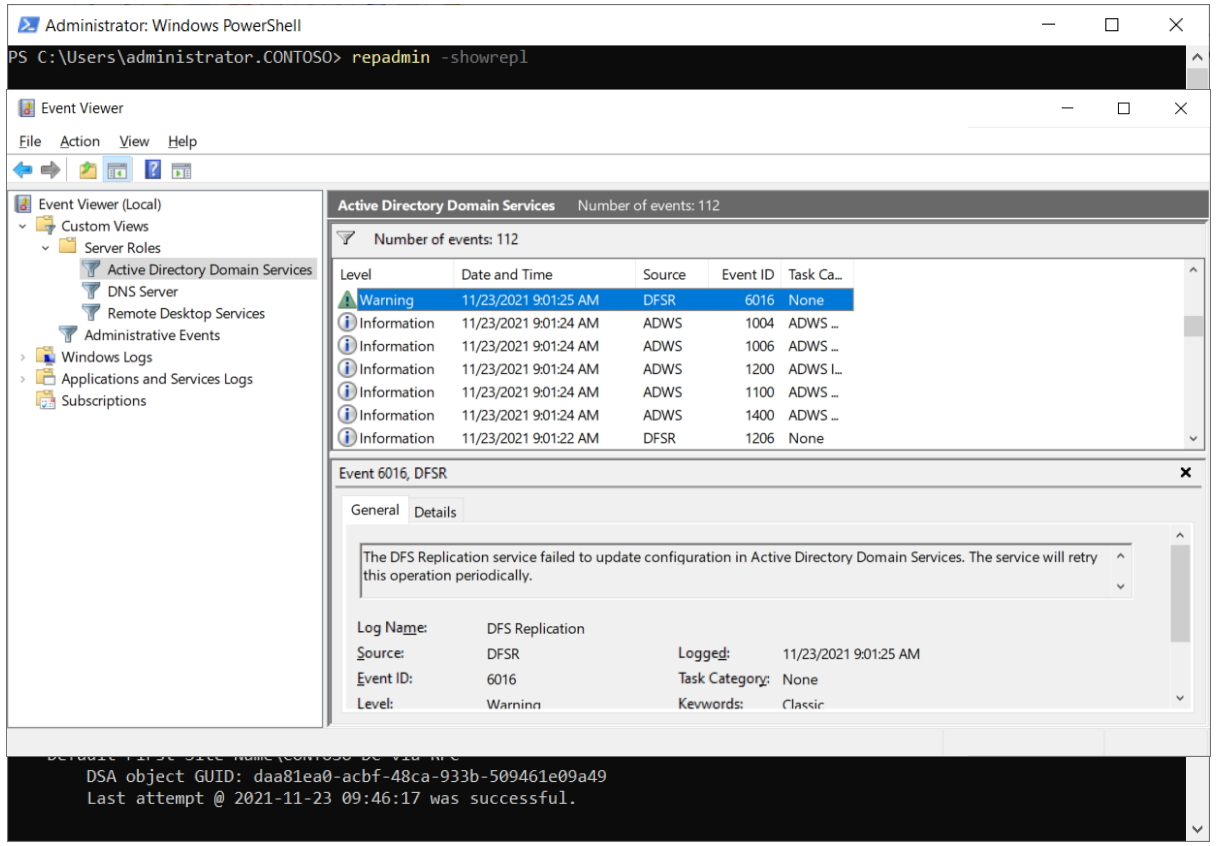
Troubleshoot AD DS replication (3 of 4)

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 Microsoft Entra ID
- Synchronizing AD DS with Microsoft Entra ID by using password hash synchronization
- Implementing SSO between on-premises AD DS and Microsoft Entra ID

What is Microsoft Entra 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 Microsoft Entra ID, and let it run

Troubleshoot hybrid authentication issues (2 of 3)

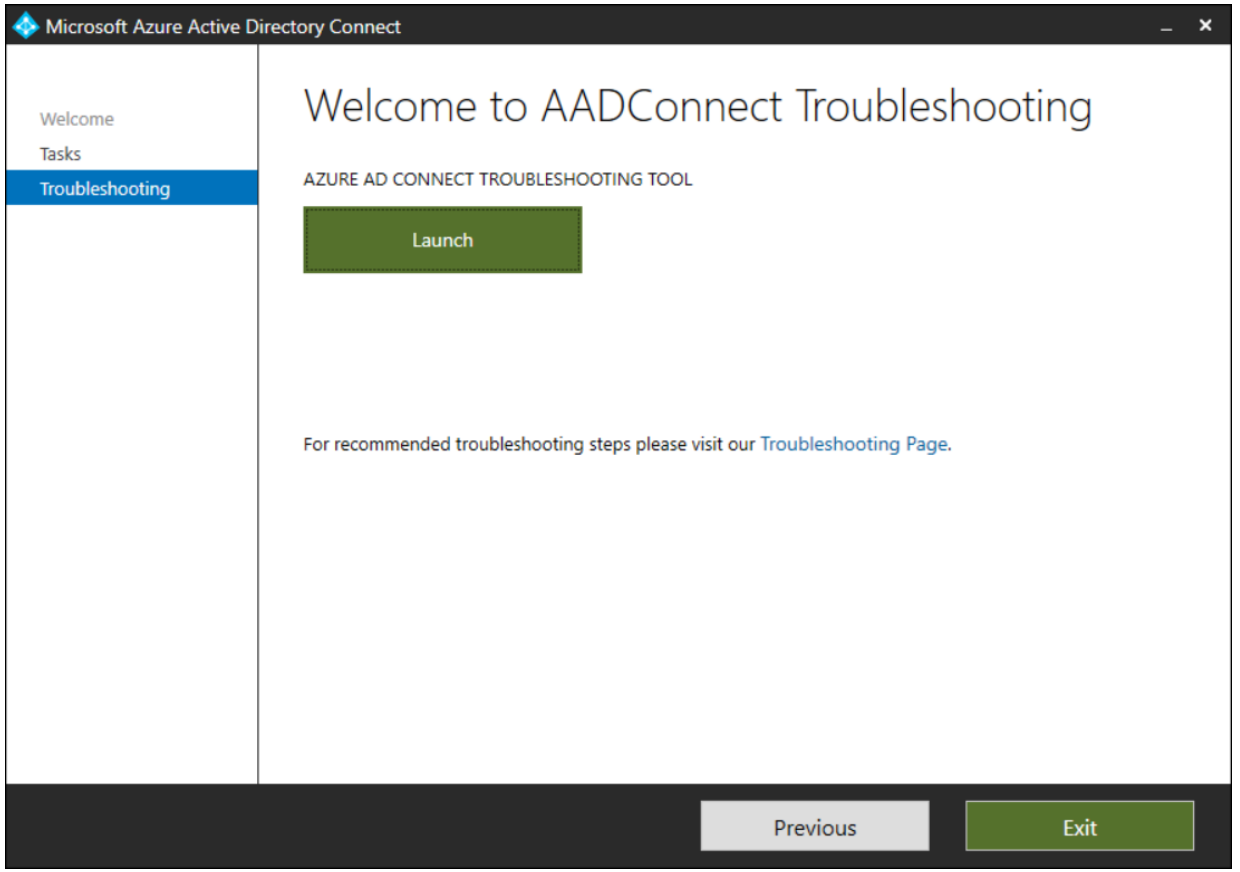
Prepare to synchronize

A very good way of avoiding problems with synchronizing identities.

Perform health checks of AD DS

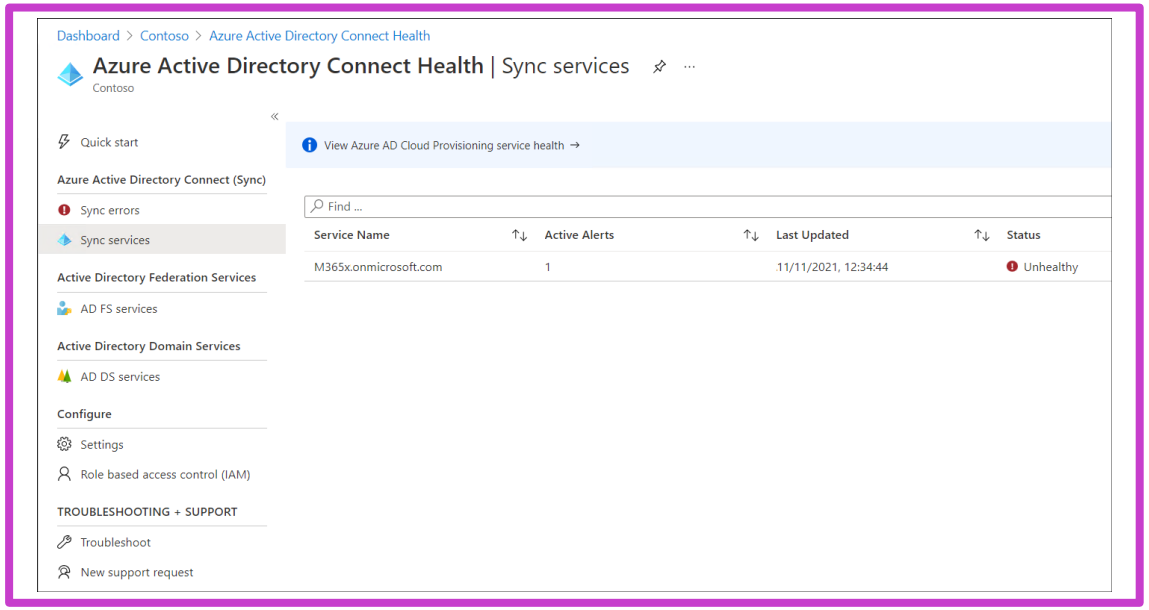
- IdFix tool
- ADModify.NET tool

Troubleshoot issues with Microsoft Entra Connect sync

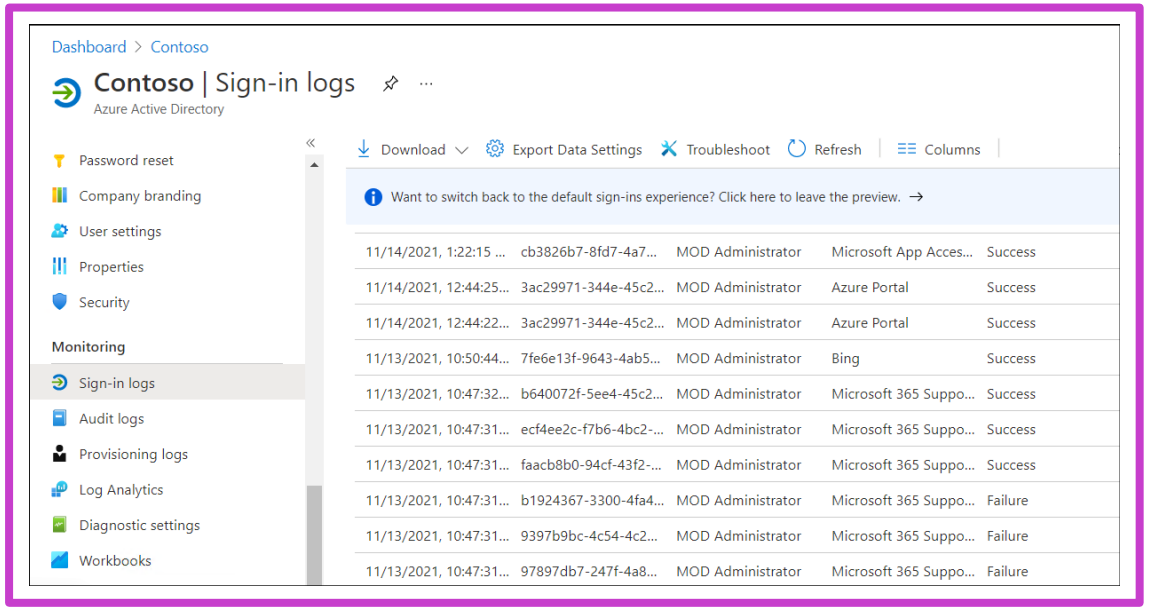


Troubleshoot hybrid authentication issues (3 of 3)

Monitor Microsoft Entra Connect



Review Microsoft Entra ID sign-in logs



Learning recap – Troubleshoot Active Directory

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Troubleshoot Active Directory

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.

End of presentation