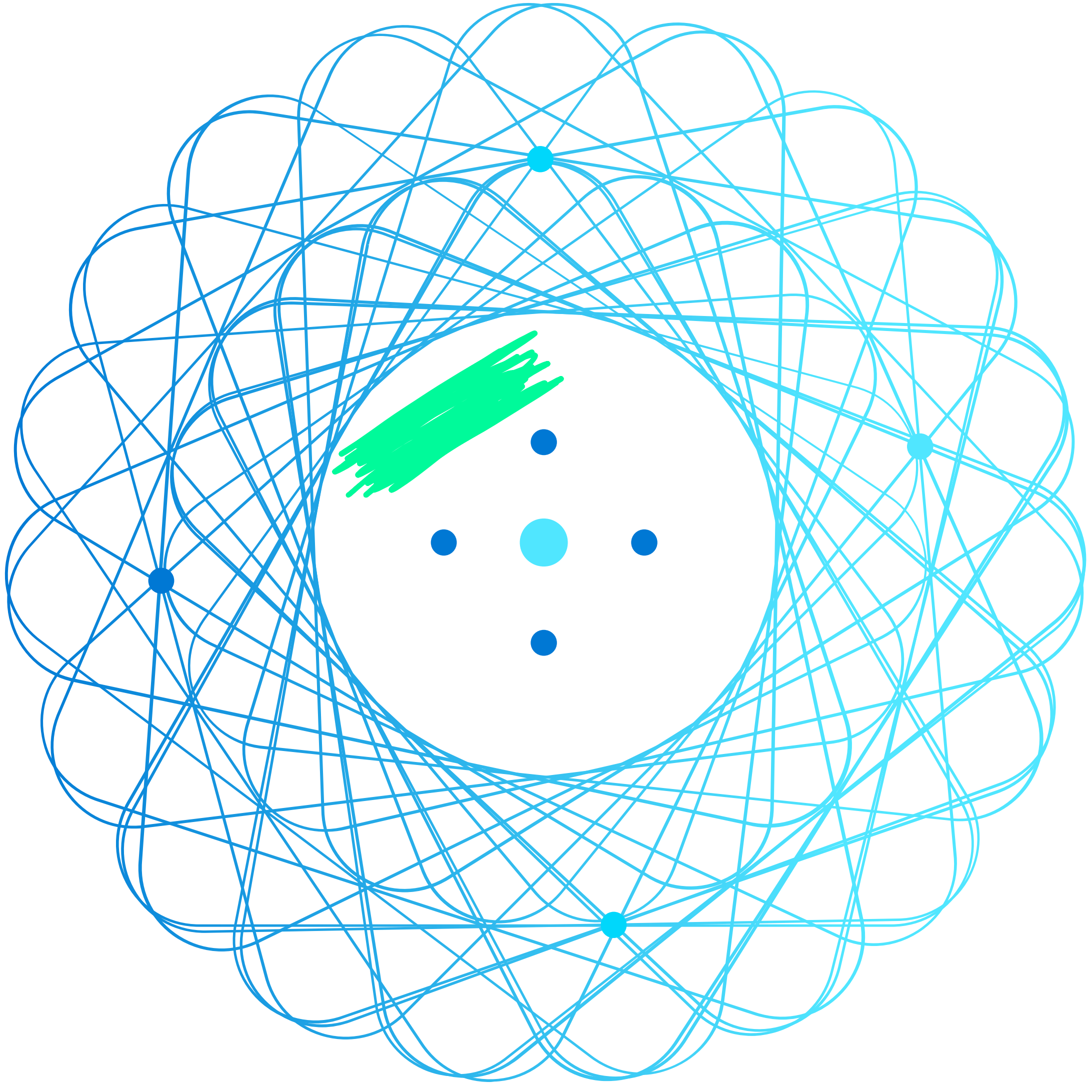
Microsoft Azure

Tag 4

AZ-801

Guten Morgen!

Configuring Windows Server Hybrid Advanced Services



AZ-800

AZ-801

Azure Pass ✗

Azure Pass ✓

Sub

26 Tage

LP 2

- Module 01: Windows Server security
- Module 02: Implementing security solutions in hybrid scenarios
- Module 03: Implementing Windows Server high availability
- Module 04: Disaster recovery in Windows Server
- Module 05: Implementing recovery services in hybrid scenarios
- Module 06: Upgrade and migrate in Windows Server
- Module 07: Implementing migration in hybrid scenarios
- Module 08: Server and performance monitoring in Windows Server
- Module 09: Implementing operational monitoring in hybrid scenarios

LP 5

Lift & shift

Quick Start

Size

Migration Project

Perfmon

Event Log

Event Sub

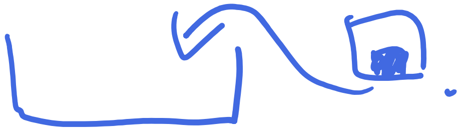
Bicep → ARM

Template json

Log Analytics

Data Lake

Blob



Azure Monitor

Learning Path 5: Monitor and troubleshoot Windows Server environment

(Server and performance monitoring in Windows Server)

- Monitor Windows Server performance ✓
- Manage and monitor Windows Server event logs ✓ SVR1 App Log → (SVR2)
- Implement Windows Server auditing and diagnostics
- Troubleshoot Active Directory ntdsutil
- Lab 08

Module 1: Monitor Windows Server performance

Monitor Windows Server performance

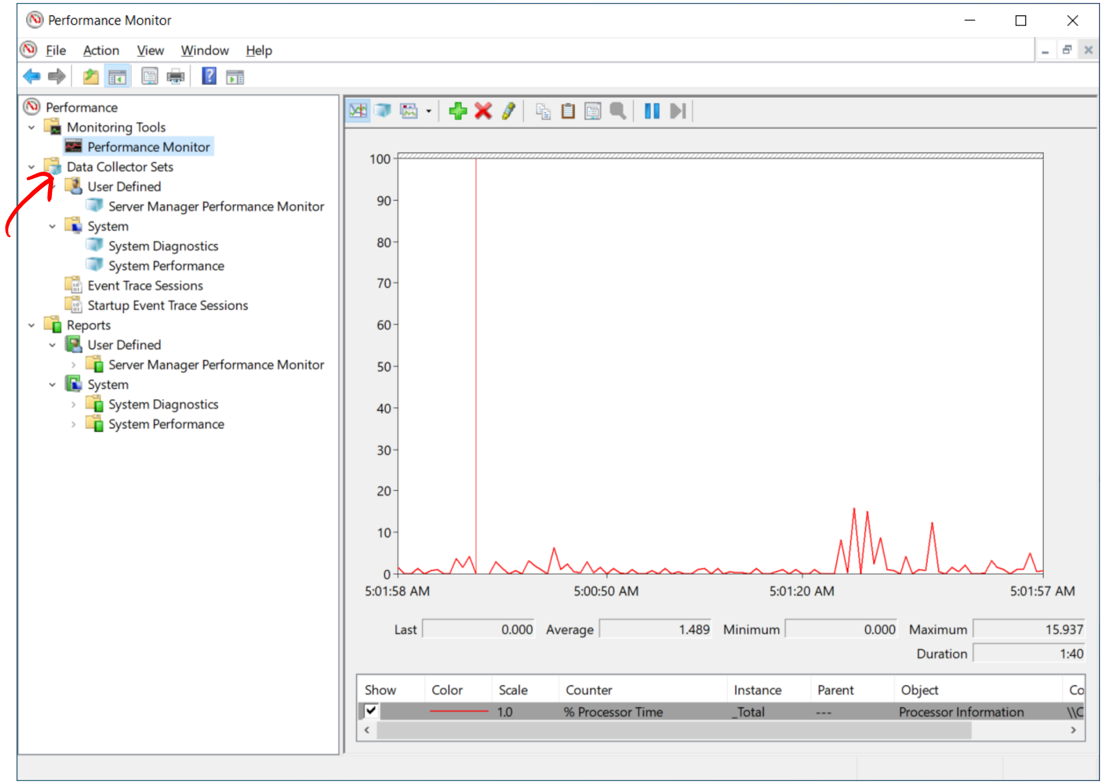
- Use Performance Monitor to identify performance problems
- Use Resource Monitor to review current resource usage
- Review reliability with Reliability Monitor
- Implement a performance monitoring methodology
- Use Data Collector Sets to analyze server performance

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



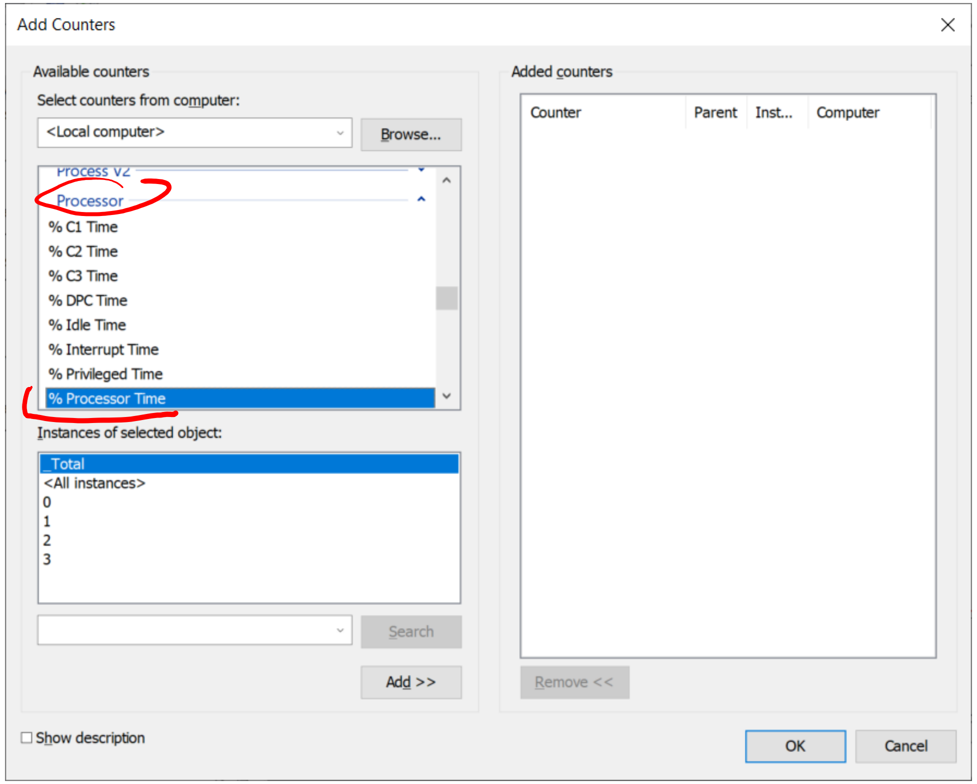
- Performance
  - Monitoring Tools
    - Performance Monitor
  - Data Collector Sets
    - User Defined
      - Server Manager Performance Monitor
    - System
      - System Diagnostics
      - System Performance
    - Event Trace Sessions
    - Startup Event Trace Sessions
  - Reports
    - User Defined
      - Server Manager Performance Monitor
    - System
      - System Diagnostics
      - System Performance

Last 0.000 Average 1.489 Minimum 0.000 Maximum 15.937

Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Co
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\C

Common performance counters



Available counters

Select counters from computer:

<Local computer>

Process V2

Processor

% C1 Time

% C2 Time

% C3 Time

% DPC Time

% Idle Time

% Interrupt Time

% Privileged Time

% Processor Time

Instances of selected object:

_Total

<All instances>

0

1

2

3

Added counters

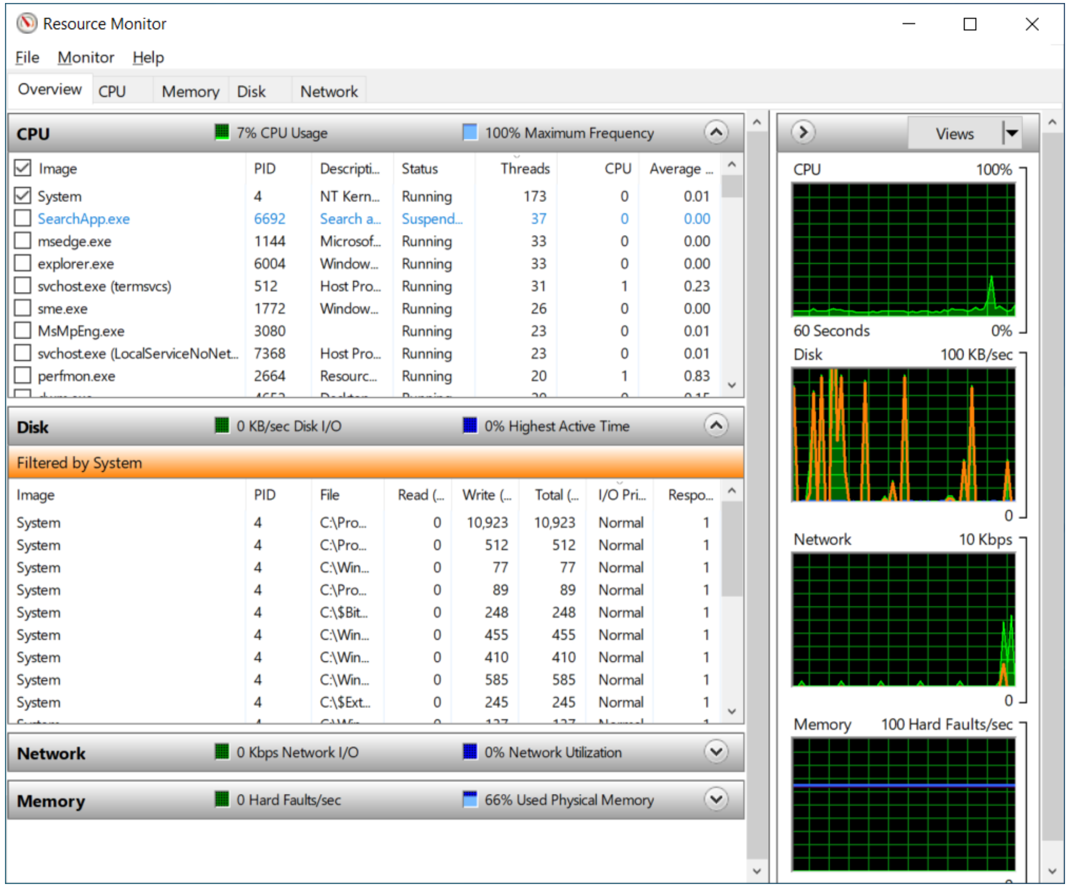
Counter	Parent	Inst...	Computer

□ Show description

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.



CPU 🟩 7% CPU Usage 🟦 100% Maximum Frequency

☑ Image	PID	Descripti...	Status	Threads	CPU	Average ...
☑ System	4	NT Kern...	Running	173	0	0.01
□ SearchApp.exe	6692	Search a...	Suspend...	37	0	0.00
□ msedge.exe	1144	Microsof...	Running	33	0	0.00
□ explorer.exe	6004	Window...	Running	33	0	0.00
□ svchost.exe (termsvcs)	512	Host Pro...	Running	31	1	0.23
□ sme.exe	1772	Window...	Running	26	0	0.00
□ MsMpEng.exe	3080		Running	23	0	0.01
□ svchost.exe (LocalServiceNoNet...	7368	Host Pro...	Running	23	0	0.01
□ perfmon.exe	2664	Resourc...	Running	20	1	0.83

Disk 🟩 0 KB/sec Disk I/O 🟦 0% Highest Active Time

Filtered by System

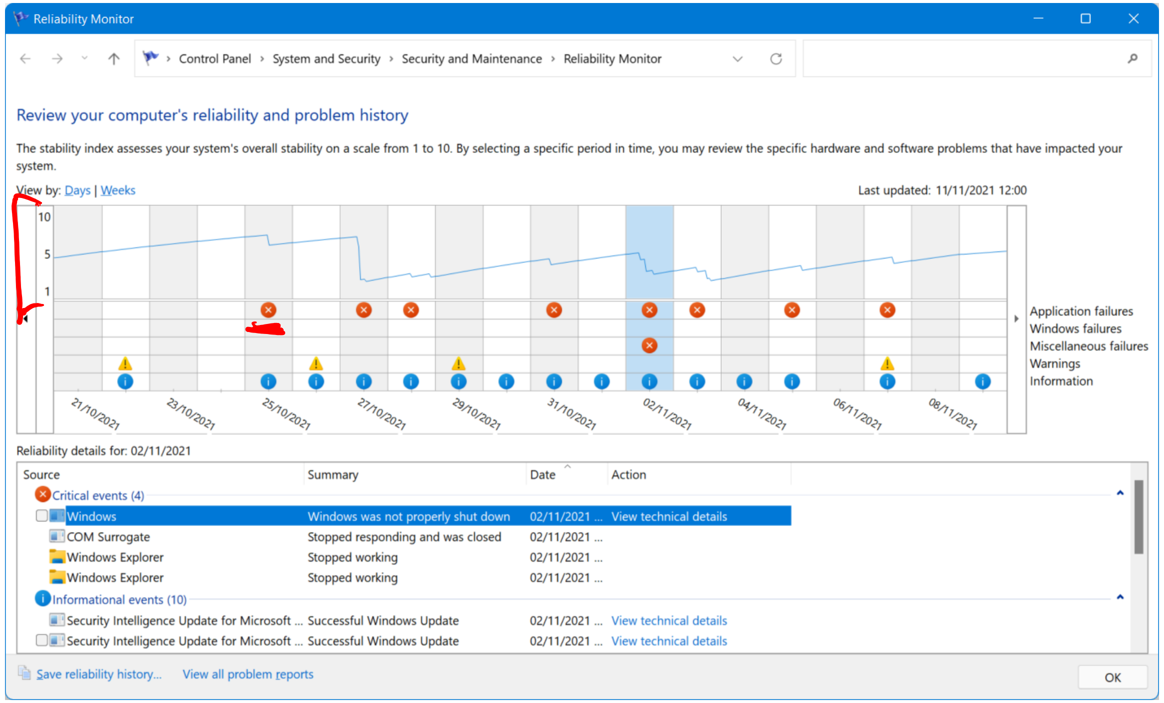
Image	PID	File	Read (...	Write (...	Total (...	I/O Pri...	Respo...
System	4	C:\Pro...	0	10,923	10,923	Normal	1
System	4	C:\Pro...	0	512	512	Normal	1
System	4	C:\Win...	0	77	77	Normal	1
System	4	C:\Pro...	0	89	89	Normal	1
System	4	C:\$Bit...	0	248	248	Normal	1
System	4	C:\Win...	0	455	455	Normal	1
System	4	C:\Win...	0	410	410	Normal	1
System	4	C:\Win...	0	585	585	Normal	1
System	4	C:\$Ext...	0	245	245	Normal	1

Network 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

Memory 🟩 0 Hard Faults/sec 🟦 66% Used Physical Memory

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**



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

Last updated: 11/11/2021 12:00

Reliability details for: 02/11/2021

Source	Summary	Date	Action
Critical events (4)			
Windows	Windows was not properly shut down	02/11/2021 ...	View technical details
COM Surrogate	Stopped responding and was closed	02/11/2021 ...	
Windows Explorer	Stopped working	02/11/2021 ...	
Windows Explorer	Stopped working	02/11/2021 ...	
Informational events (10)			
Security Intelligence Update for Microsoft ...	Successful Windows Update	02/11/2021 ...	View technical details
Security Intelligence Update for Microsoft ...	Successful Windows Update	02/11/2021 ...	View technical details

Implement a performance monitoring methodology

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.

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

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

Analyze key hardware components - The four key hardware components are processor, disk, memory, and network.

Use Data Collector Sets to analyze server performance

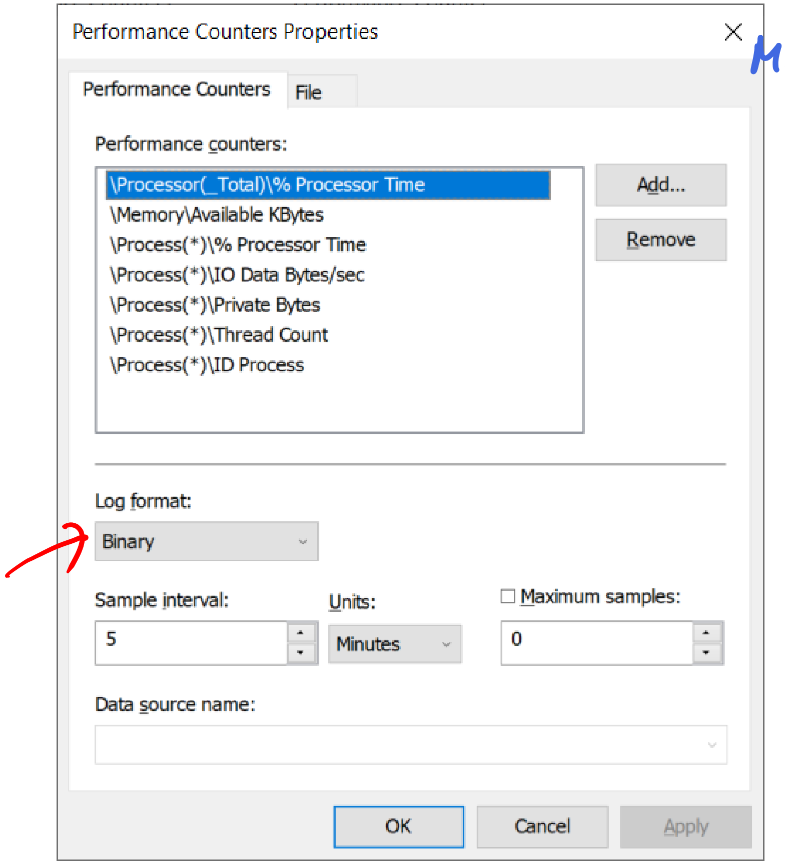
KQL LA

Provider
Microsoft.compute
VM Agent

win
Perf
conter

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



Performance counters:

\Processor(_Total)\% Processor Time
\Memory\Available KBytes
\Process(*)\% Processor Time
\Process(*)\IO Data Bytes/sec
\Process(*)\Private Bytes
\Process(*)\Thread Count
\Process(*)\ID Process

Log format: Binary

Sample interval: 5

Units: Minutes

□ Maximum samples: 0

Data source name:

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

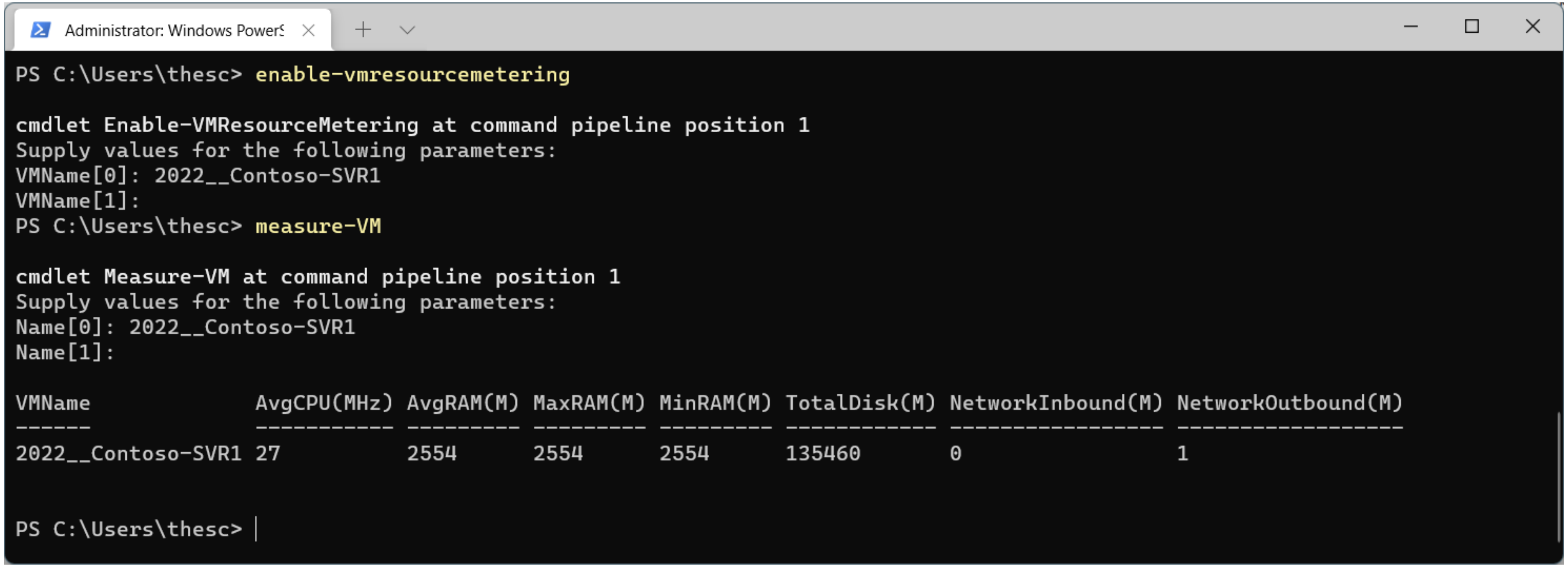
You can use Hyper-V Resource Metering to monitors VMs by measuring below parameters:

- 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



```
PS 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)
------             ----------- --------- --------- --------- ------------ ----------------- ------------------
2022__Contoso-SVR1 27          2554      2554      2554      135460       0                 1


PS C:\Users\thesc>
```

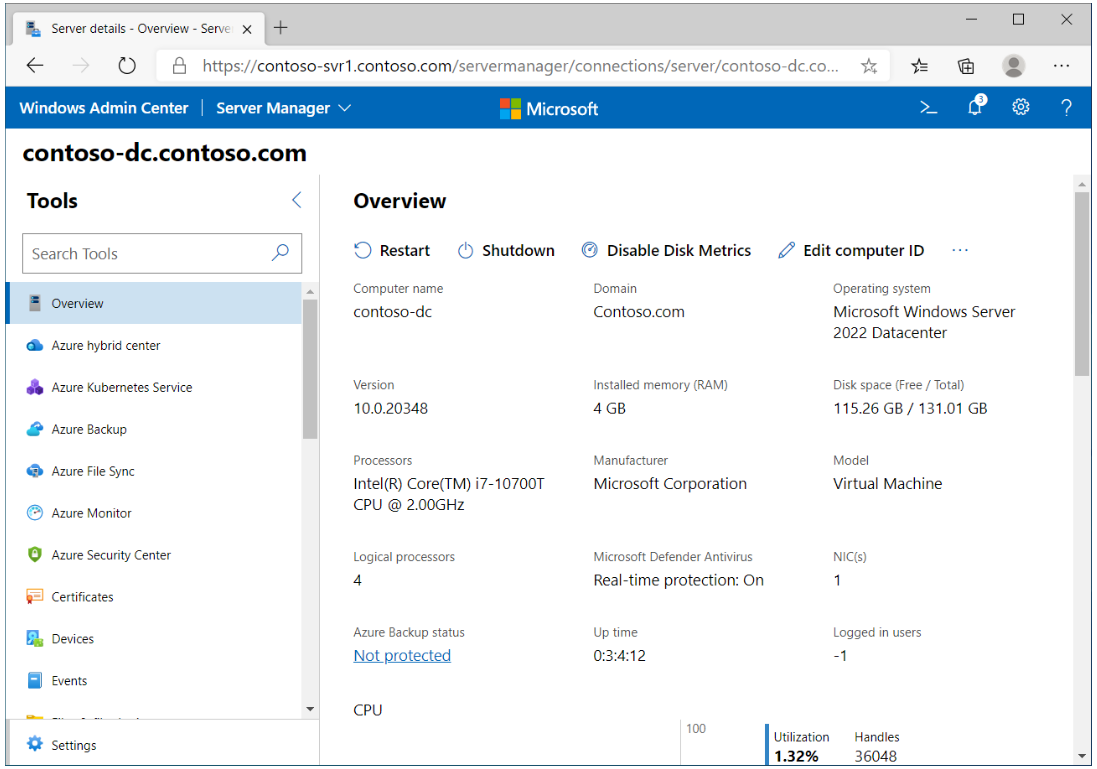
Typical output from the `measure-VM` cmdlet is displayed in the screenshot.

Monitor performance with Windows Admin Center

WAC

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



contoso-dc.contoso.com

Overview

Computer name: contoso-dc

Domain: Contoso.com

Operating system: Microsoft Windows Server 2022 Datacenter

Version: 10.0.20348

Installed memory (RAM): 4 GB

Disk space (Free / Total): 115.26 GB / 131.01 GB

Processors: Intel(R) Core(TM) i7-10700T CPU @ 2.00GHz

Manufacturer: Microsoft Corporation

Model: Virtual Machine

Logical processors: 4

Microsoft Defender Antivirus: Real-time protection: On

NIC(s): 1

Azure Backup status: Not protected

Up time: 0:3:4:12

Logged in users: -1

CPU

100

Utilization: 1.32%

Handles: 36048

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

SDN
Windows Server

Knowledge check and resources – Monitor Windows Server performance

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Monitor Windows Server performance

Module 2: Manage and monitor Windows Server event logs

Manage and monitor Windows Server event logs Introduction

- 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
- Knowledge check and resources

Describe Windows Server event logs

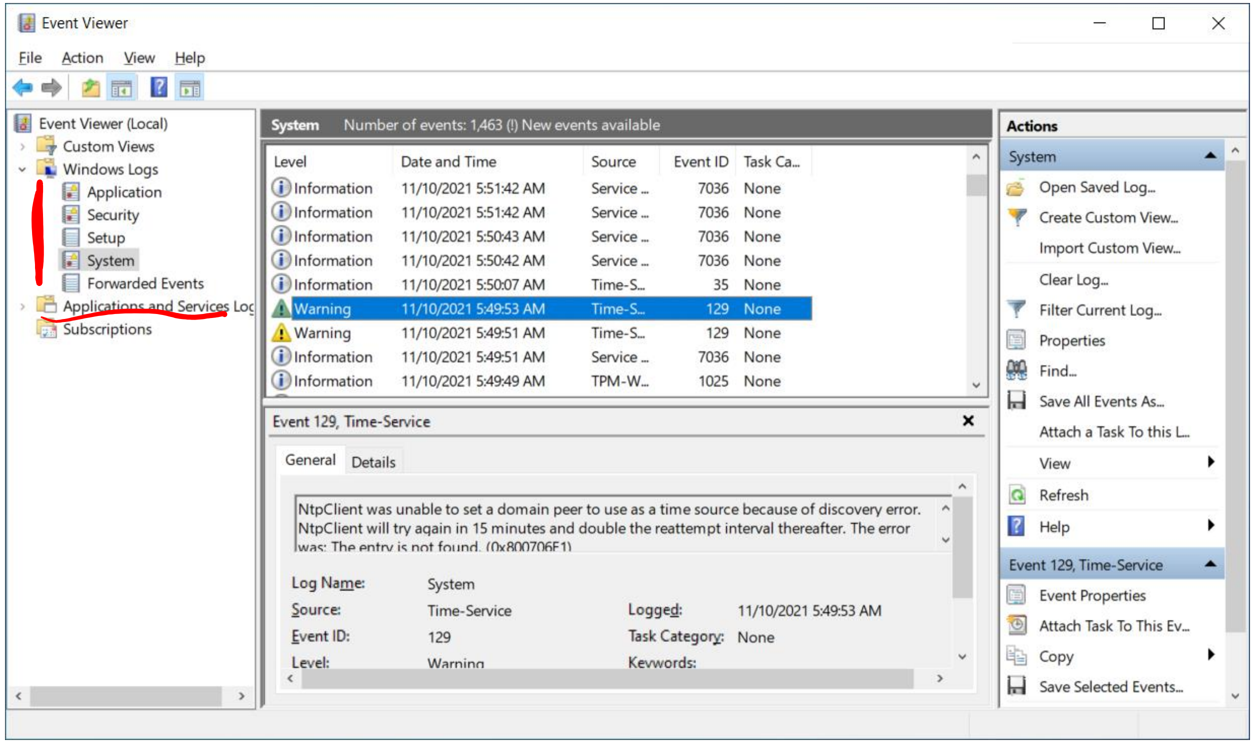
What is Event Viewer?

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



System Number of events: 1,463 (!) New events available

Level	Date and Time	Source	Event ID	Task Ca...
Information	11/10/2021 5:51:42 AM	Service ...	7036	None
Information	11/10/2021 5:51:42 AM	Service ...	7036	None
Information	11/10/2021 5:50:43 AM	Service ...	7036	None
Information	11/10/2021 5:50:42 AM	Service ...	7036	None
Information	11/10/2021 5:50:07 AM	Time-S...	35	None
Warning	11/10/2021 5:49:53 AM	Time-S...	129	None
Warning	11/10/2021 5:49:51 AM	Time-S...	129	None
Information	11/10/2021 5:49:51 AM	Service ...	7036	None
Information	11/10/2021 5:49:49 AM	TPM-W...	1025	None

Event 129, Time-Service

NtpClient was unable to set a domain peer to use as a time source because of discovery error. NtpClient will try again in 15 minutes and double the reattempt interval thereafter. The error was: The entry is not found. (0x800706E1)

Log Name: System
Source: Time-Service
Logged: 11/10/2021 5:49:53 AM
Event ID: 129
Task Category: None
Level: Warning
Keywords:

Describe Windows Server event logs

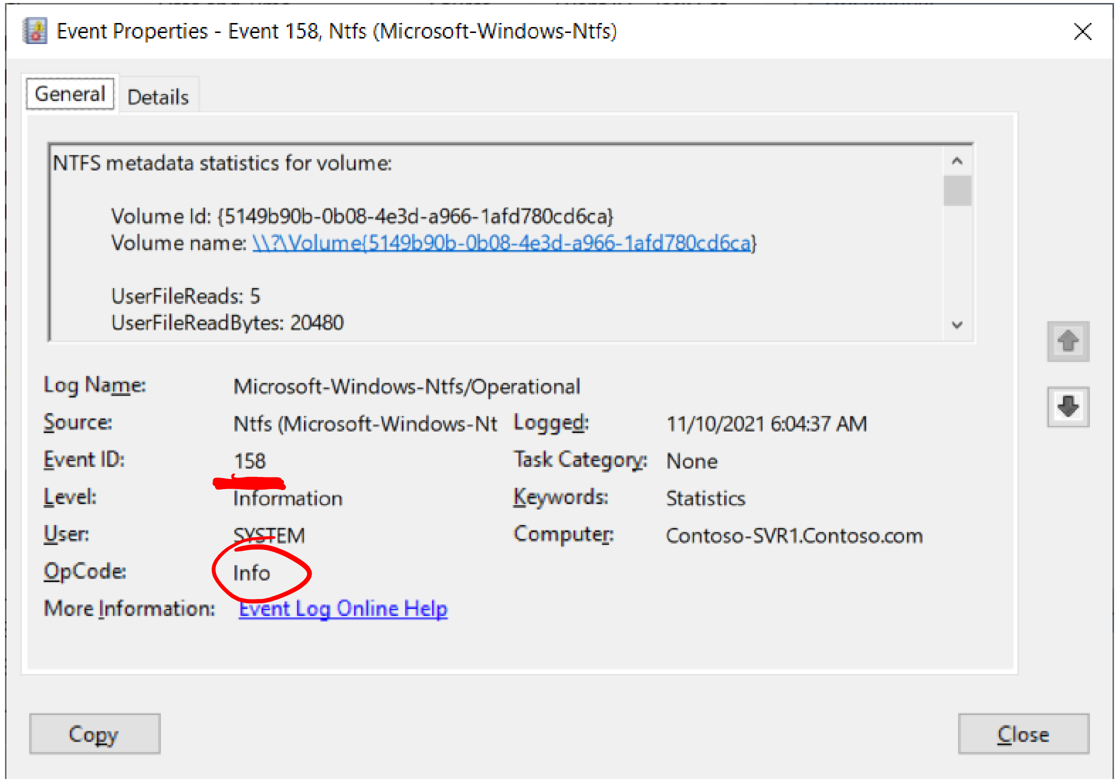
Get-EventLog

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



NTFS metadata statistics for volume:

Volume Id: {5149b90b-0b08-4e3d-a966-1afd780cd6ca}
Volume name: \\?\Volume{5149b90b-0b08-4e3d-a966-1afd780cd6ca}

UserFileReads: 5
UserFileReadBytes: 20480

Log Name: Microsoft-Windows-Ntfs/Operational
Source: Ntfs (Microsoft-Windows-Nt
Logged: 11/10/2021 6:04:37 AM
Event ID: 158
Task Category: None
Level: Information
Keywords: Statistics
User: SYSTEM
Computer: Contoso-SVR1.Contoso.com
OpCode: Info
More Information: Event Log Online Help

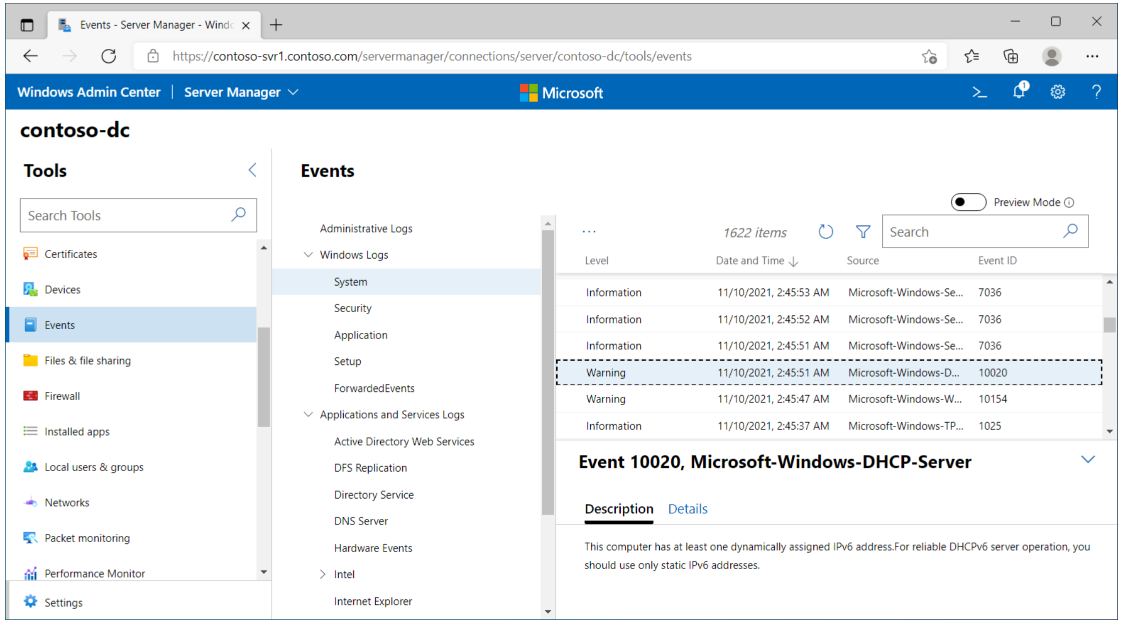
Use Windows Admin Center to review logs

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.



Level	Date and Time ↓	Source	Event ID
Information	11/10/2021, 2:45:53 AM	Microsoft-Windows-Se...	7036
Information	11/10/2021, 2:45:52 AM	Microsoft-Windows-Se...	7036
Information	11/10/2021, 2:45:51 AM	Microsoft-Windows-Se...	7036
Warning	11/10/2021, 2:45:51 AM	Microsoft-Windows-D...	10020
Warning	11/10/2021, 2:45:47 AM	Microsoft-Windows-W...	10154
Information	11/10/2021, 2:45:37 AM	Microsoft-Windows-TP...	1025

Event 10020, Microsoft-Windows-DHCP-Server

Description Details

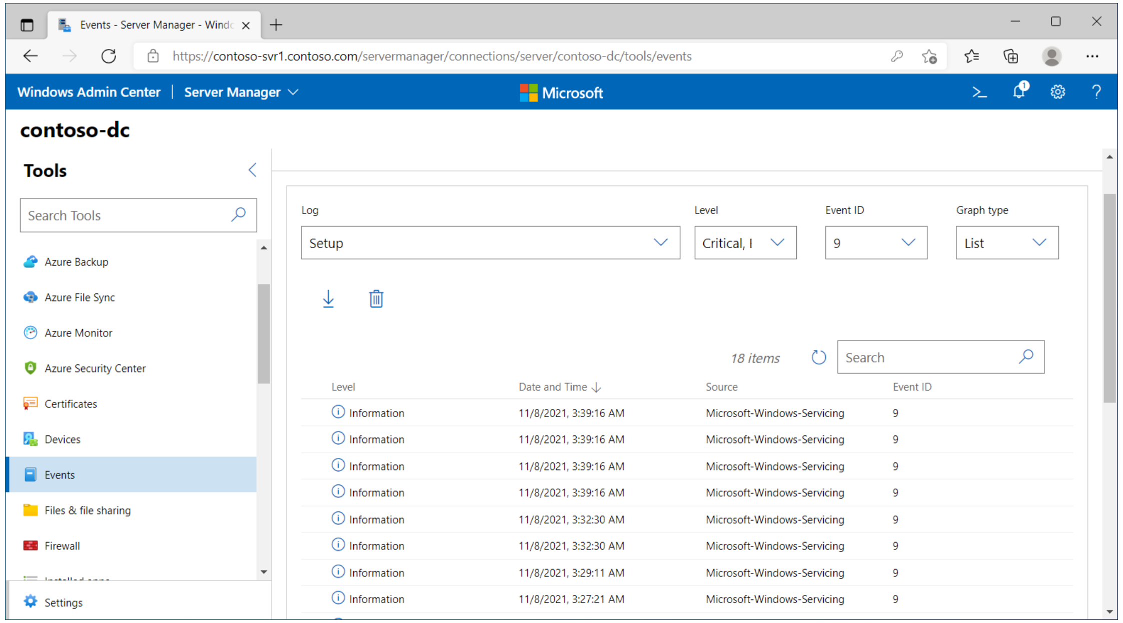
This computer has at least one dynamically assigned IPv6 address.For reliable DHCPv6 server operation, you should use only static IPv6 addresses.

Use Windows Admin Center to review logs

Use preview features

Use Events to perform the following functions:

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



Log: Setup

Level: Critical, I

Event ID: 9

Graph type: List

18 items

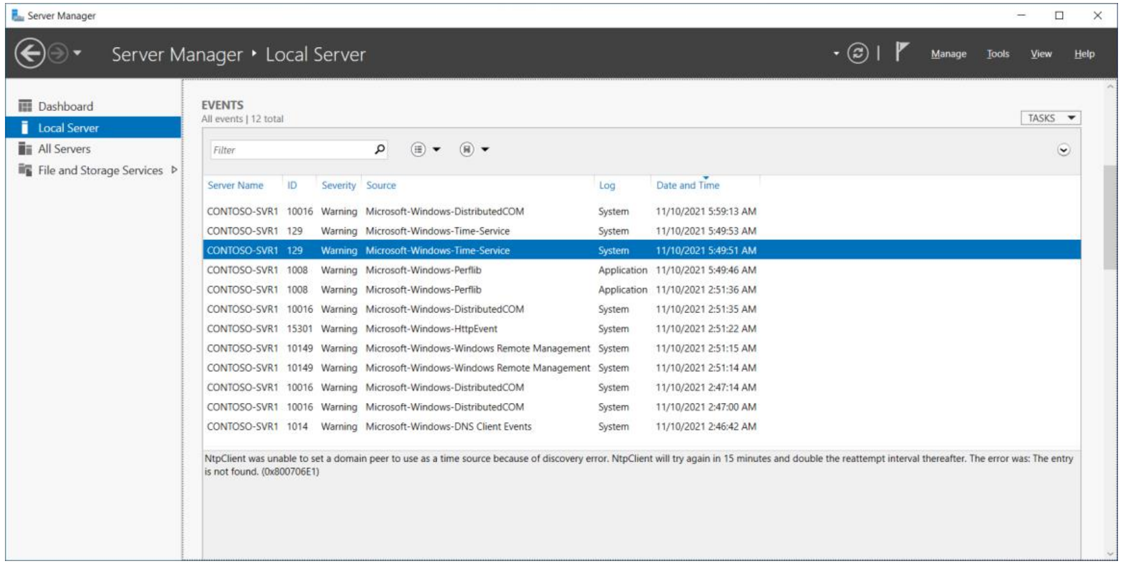
Level	Date and Time	Source	Event ID
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information	11/8/2021, 3:39:16 AM	Microsoft-Windows-Servicing	9
Information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

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



EVENTS
All events | 12 total

Server Name	ID	Severity	Source	Log	Date and Time
CONTOSO-SVR1	10016	Warning	Microsoft-Windows-DistributedCOM	System	11/10/2021 5:59:13 AM
CONTOSO-SVR1	129	Warning	Microsoft-Windows-Time-Service	System	11/10/2021 5:49:53 AM
CONTOSO-SVR1	129	Warning	Microsoft-Windows-Time-Service	System	11/10/2021 5:49:51 AM
CONTOSO-SVR1	1008	Warning	Microsoft-Windows-Perflib	Application	11/10/2021 5:49:46 AM
CONTOSO-SVR1	1008	Warning	Microsoft-Windows-Perflib	Application	11/10/2021 2:51:36 AM
CONTOSO-SVR1	10016	Warning	Microsoft-Windows-DistributedCOM	System	11/10/2021 2:51:35 AM
CONTOSO-SVR1	15301	Warning	Microsoft-Windows-HttpEvent	System	11/10/2021 2:51:22 AM
CONTOSO-SVR1	10149	Warning	Microsoft-Windows-Windows Remote Management	System	11/10/2021 2:51:15 AM
CONTOSO-SVR1	10149	Warning	Microsoft-Windows-Windows Remote Management	System	11/10/2021 2:51:14 AM
CONTOSO-SVR1	10016	Warning	Microsoft-Windows-DistributedCOM	System	11/10/2021 2:47:14 AM
CONTOSO-SVR1	10016	Warning	Microsoft-Windows-DistributedCOM	System	11/10/2021 2:47:00 AM
CONTOSO-SVR1	1014	Warning	Microsoft-Windows-DNS Client Events	System	11/10/2021 2:46:42 AM

```
NtpClient was unable to set a domain peer to use as a time source because of discovery error. NtpClient will try again in 15 minutes and double the reattempt interval thereafter. The error was: The entry is not found. (0x800706E1)
```

Use Server Manager to review logs

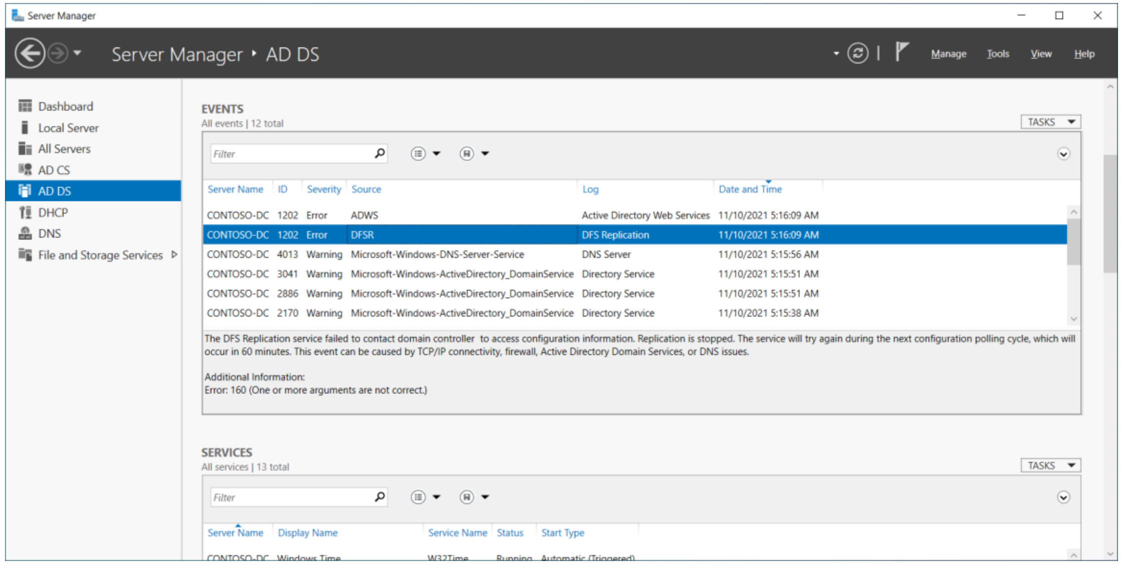
WinRM :5985

WS-Man :5986 SSL

● Perm

JEA

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



EVENTS
All events | 12 total

Server Name	ID	Severity	Source	Log	Date and Time
CONTOSO-DC	1202	Error	ADWS	Active Directory Web Services	11/10/2021 5:16:09 AM
CONTOSO-DC	1202	Error	DFSR	DFS Replication	11/10/2021 5:16:09 AM
CONTOSO-DC	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS Server	11/10/2021 5:15:56 AM
CONTOSO-DC	3041	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	11/10/2021 5:15:51 AM
CONTOSO-DC	2886	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	11/10/2021 5:15:51 AM
CONTOSO-DC	2170	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	11/10/2021 5:15:38 AM

The DFS Replication service failed to contact domain controller to access configuration information. Replication is stopped. The service will try again during the next configuration polling cycle, which will occur in 60 minutes. This event can be caused by TCP/IP connectivity, firewall, Active Directory Domain Services, or DNS issues.

Additional Information:
Error: 160 (One or more arguments are not correct.)

SERVICES
All services | 13 total

Server Name	Display Name	Service Name	Status	Start Type
CONTOSO-DC	Windows Time	W32Time	Running	Automatic (Triggered)

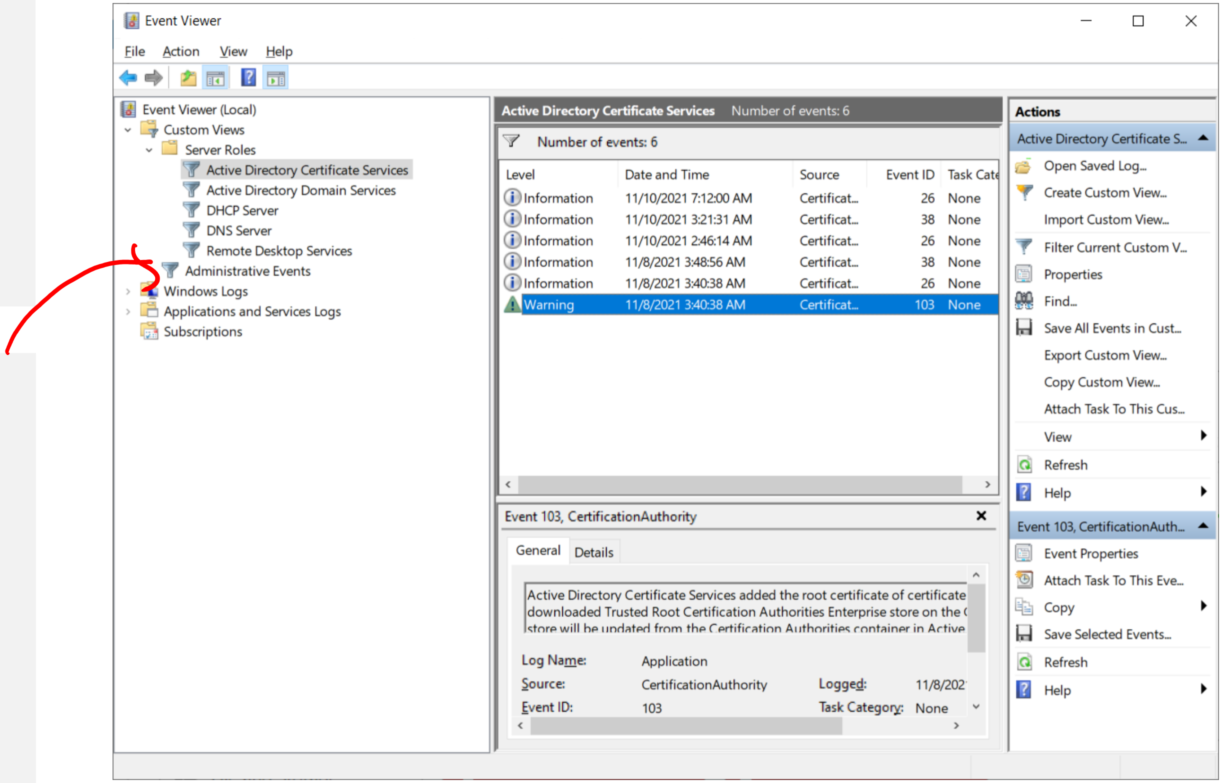
Use custom views

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



Active Directory Certificate Services   Number of events: 6

Number of events: 6

Level	Date and Time	Source	Event ID	Task Cate
Information	11/10/2021 7:12:00 AM	Certificat...	26	None
Information	11/10/2021 3:21:31 AM	Certificat...	38	None
Information	11/10/2021 2:46:14 AM	Certificat...	26	None
Information	11/8/2021 3:48:56 AM	Certificat...	38	None
Information	11/8/2021 3:40:38 AM	Certificat...	26	None
Warning	11/8/2021 3:40:38 AM	Certificat...	103	None

Event 103, CertificationAuthority

General   Details

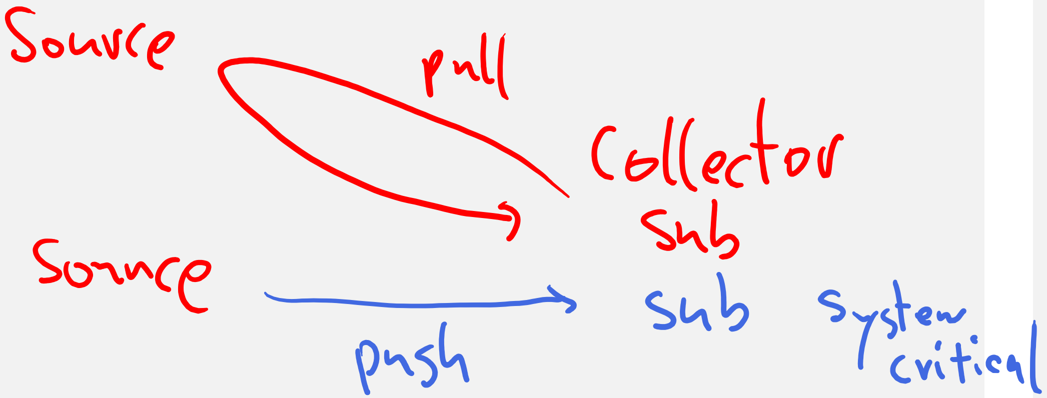
Active Directory Certificate Services added the root certificate of certificate
downloaded Trusted Root Certification Authorities Enterprise store on the
store will be updated from the Certification Authorities container in Active

Log Name: Application
Source: CertificationAuthority   Logged: 11/8/202
Event ID: 103   Task Category: None

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

Knowledge check and resources – Manage and monitor Windows Server event logs

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage and monitor Windows Server event logs

Module 3: Implement Windows Server auditing and diagnostics

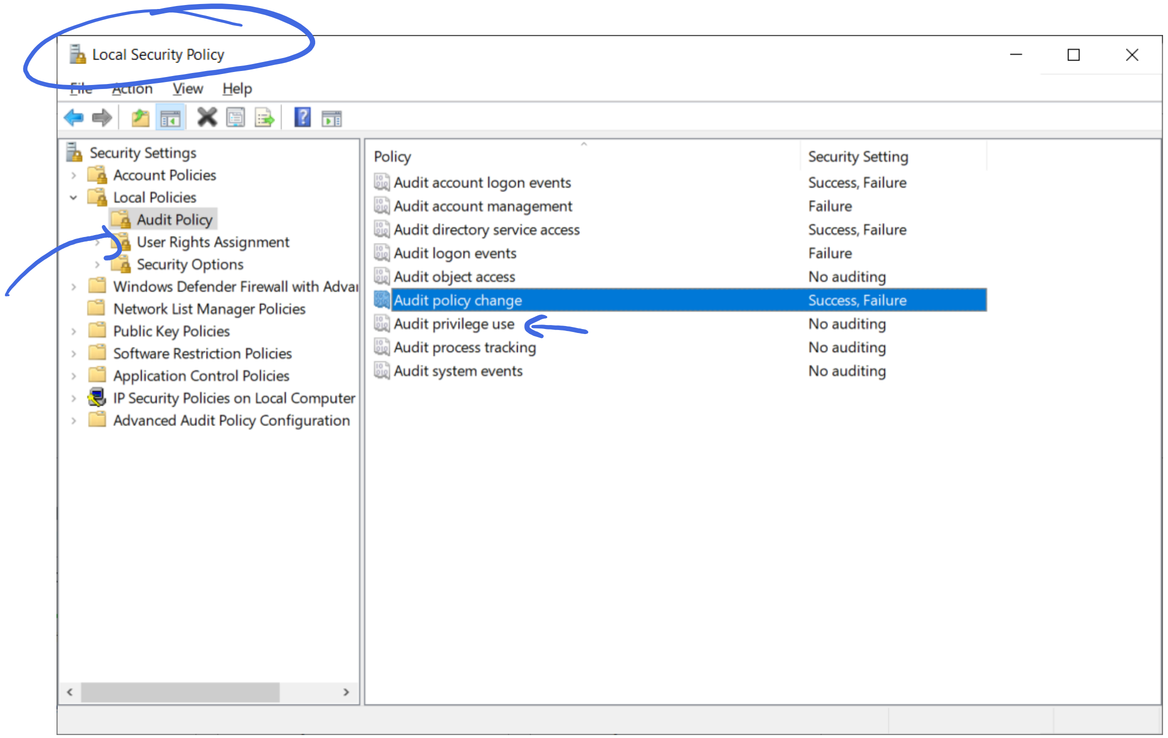
Implement Windows Server auditing and diagnostics Introduction

- Describe basic auditing categories
- Describe advanced categories
- Describe advanced categories
- Enable setup and boot event collection
- Knowledge check and resources

Describe basic auditing categories

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

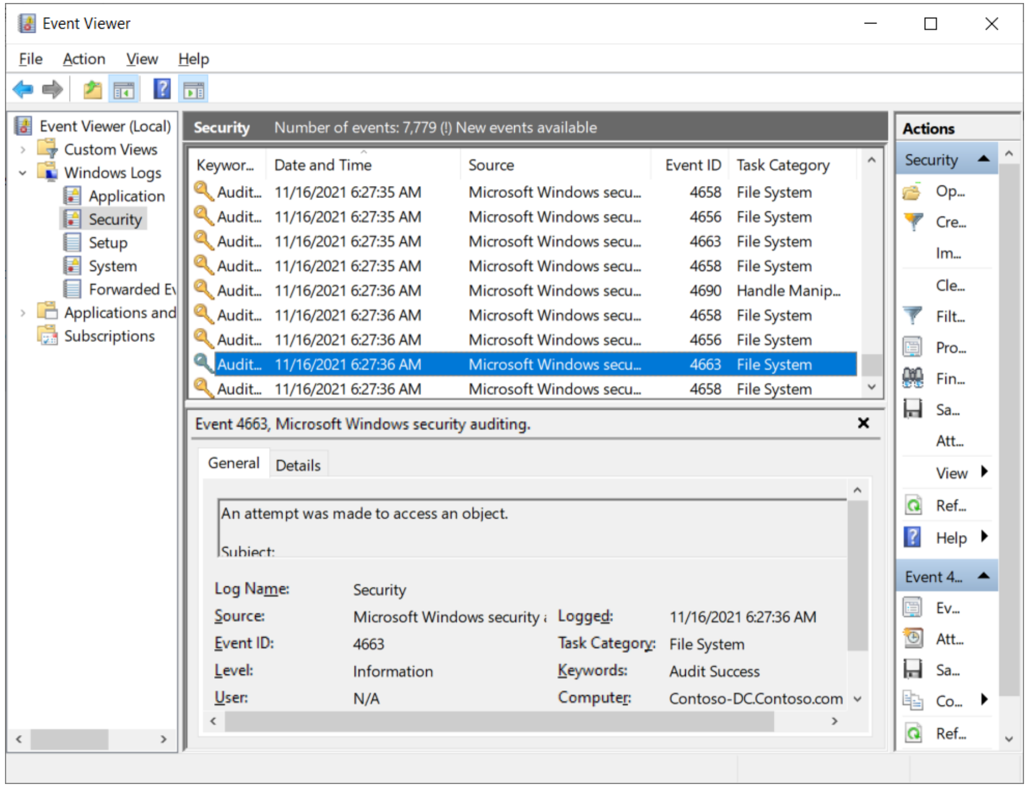

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Advai
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Failure
Audit directory service access	Success, Failure
Audit logon events	Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Describe basic auditing categories

Specify auditing settings on a file or folder:

- Typical usage
- Evaluate events in the security log



Security Number of events: 7,779 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task Category
Audit...	11/16/2021 6:27:35 AM	Microsoft Windows secu...	4658	File System
Audit...	11/16/2021 6:27:35 AM	Microsoft Windows secu...	4656	File System
Audit...	11/16/2021 6:27:35 AM	Microsoft Windows secu...	4663	File System
Audit...	11/16/2021 6:27:35 AM	Microsoft Windows secu...	4658	File System
Audit...	11/16/2021 6:27:36 AM	Microsoft Windows secu...	4690	Handle Manip...
Audit...	11/16/2021 6:27:36 AM	Microsoft Windows secu...	4658	File System
Audit...	11/16/2021 6:27:36 AM	Microsoft Windows secu...	4656	File System
Audit...	11/16/2021 6:27:36 AM	Microsoft Windows secu...	4663	File System
Audit...	11/16/2021 6:27:36 AM	Microsoft Windows secu...	4658	File System

Event 4663, Microsoft Windows security auditing.

An attempt was made to access an object.

Subject:

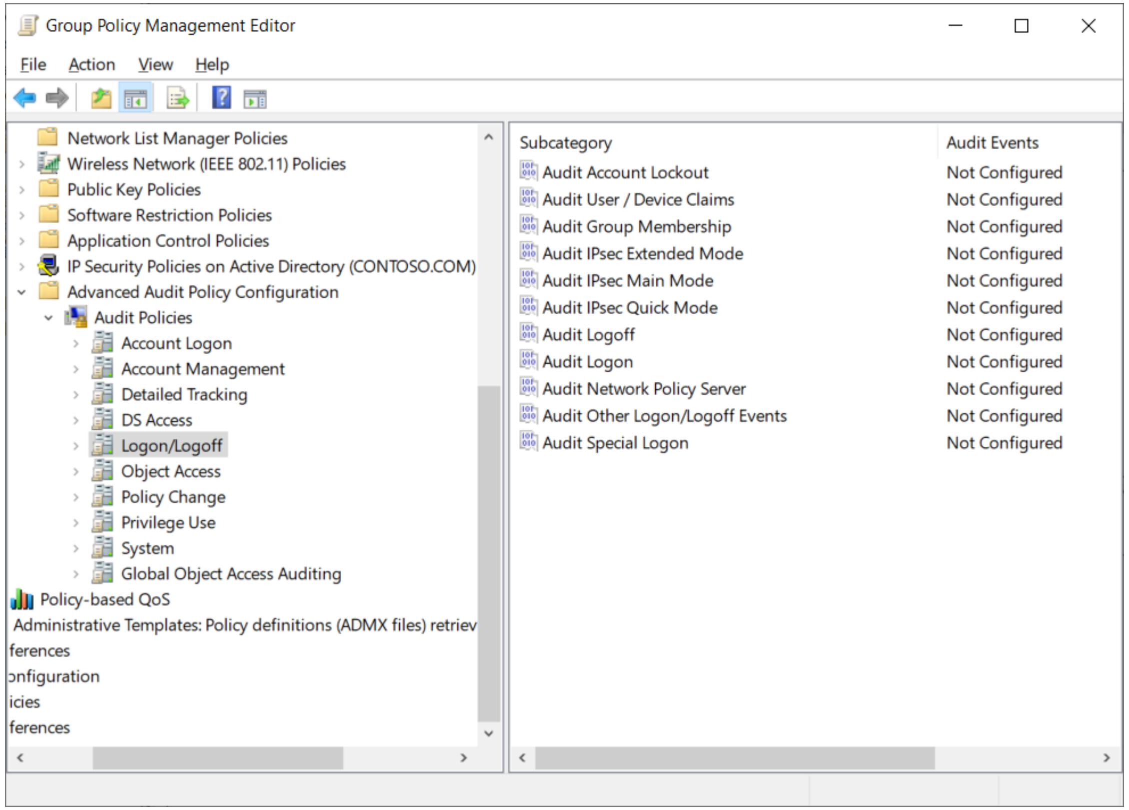
Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	11/16/2021 6:27:36 AM
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Contoso-DC.Contoso.com

Describe advanced 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



- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Active Directory (CONTOSO.COM)
- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing
- Policy-based QoS
- Administrative Templates: Policy definitions (ADMX files) retriev
- ferences
- onfiguration
- icies
- ferences

Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Not Configured
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

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.

What server roles and services are supported?

What data is logged?
UAL can log both user and device-related data.

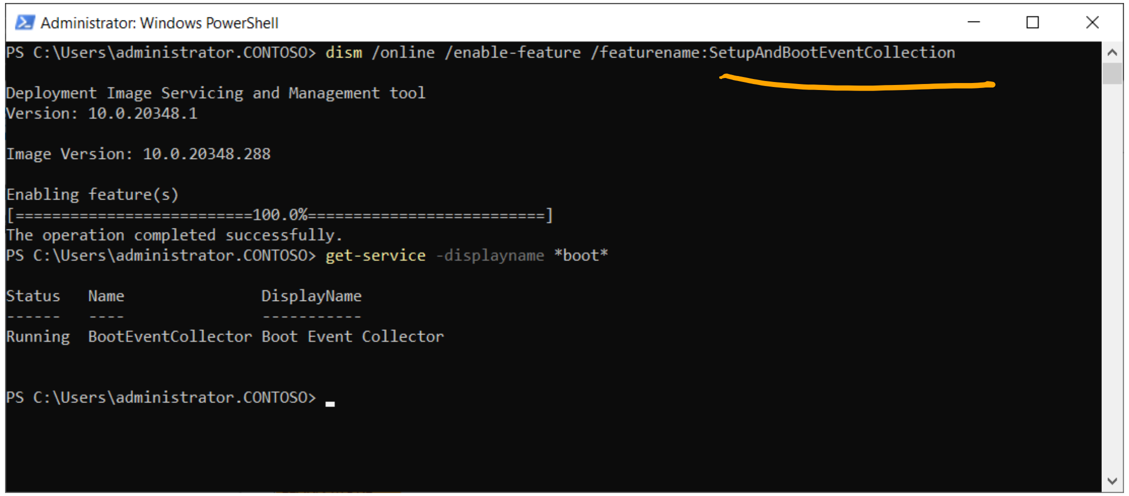
Collect UAL data
You can use Windows PowerShell to collect UAL data.

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



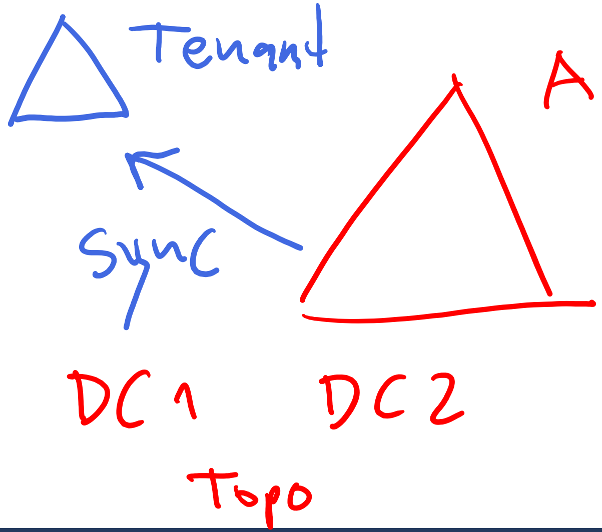
```
PS C:\Users\administrator.CONTOSO> dism /online /enable-feature /featurename:SetupAndBootEventCollection

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> _
```

Knowledge check and resources – Implement Windows Server auditing and diagnostics

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement Windows Server auditing and diagnostics



AD

LDAP

ntds.dit

ntdsutil

Sysvol

DFS

GPO

Module 4: Troubleshoot Active Directory

Troubleshoot Active Directory Introduction

- Recover objects from the AD recycle bin
- Recover the AD DS database
- Recover SYSVOL
- Troubleshoot AD DS replication
- Troubleshoot hybrid authentication issues
- Knowledge check and resources

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

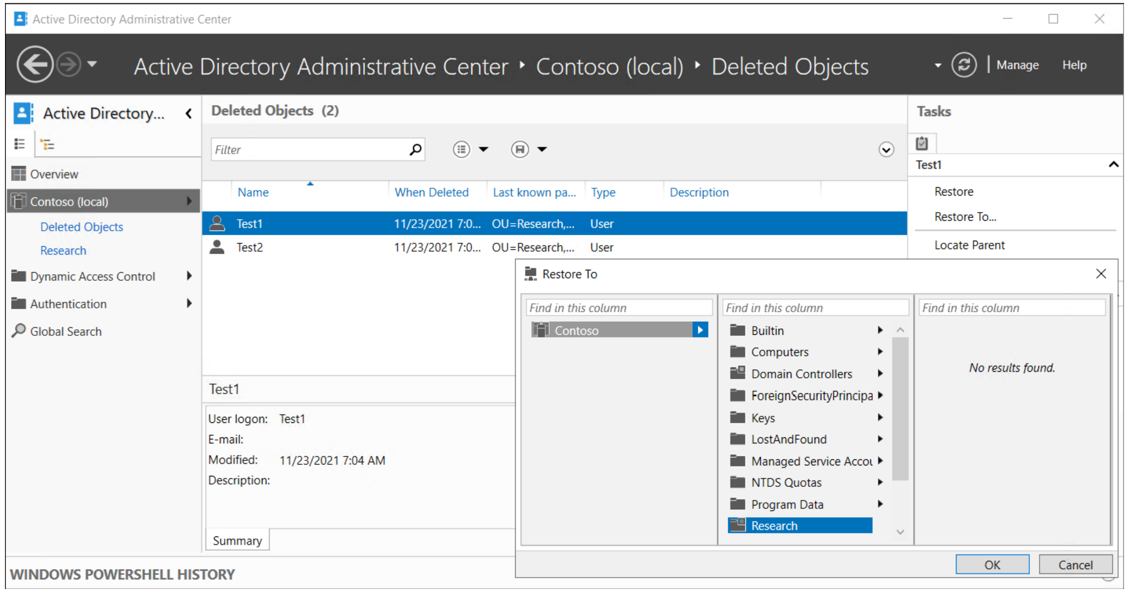
Recover objects from the AD recycle bin

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



Name	When Deleted	Last known pa...	Type	Description
Test1	11/23/2021 7:0...	OU=Research,...	User	
Test2	11/23/2021 7:0...	OU=Research,...	User	

Test1

User logon: Test1

E-mail:

Modified: 11/23/2021 7:04 AM

Description:

Recover the AD DS database

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

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

repadmin

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`

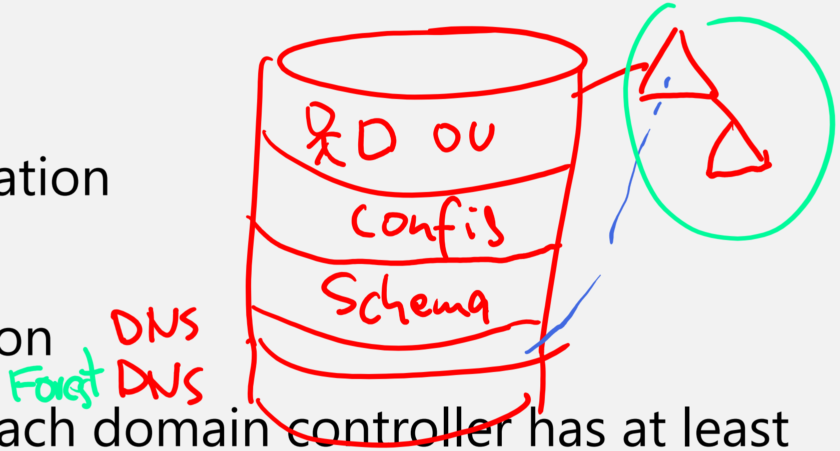
ntds .dit LDAP

Troubleshoot AD DS replication

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

Available tools for troubleshooting

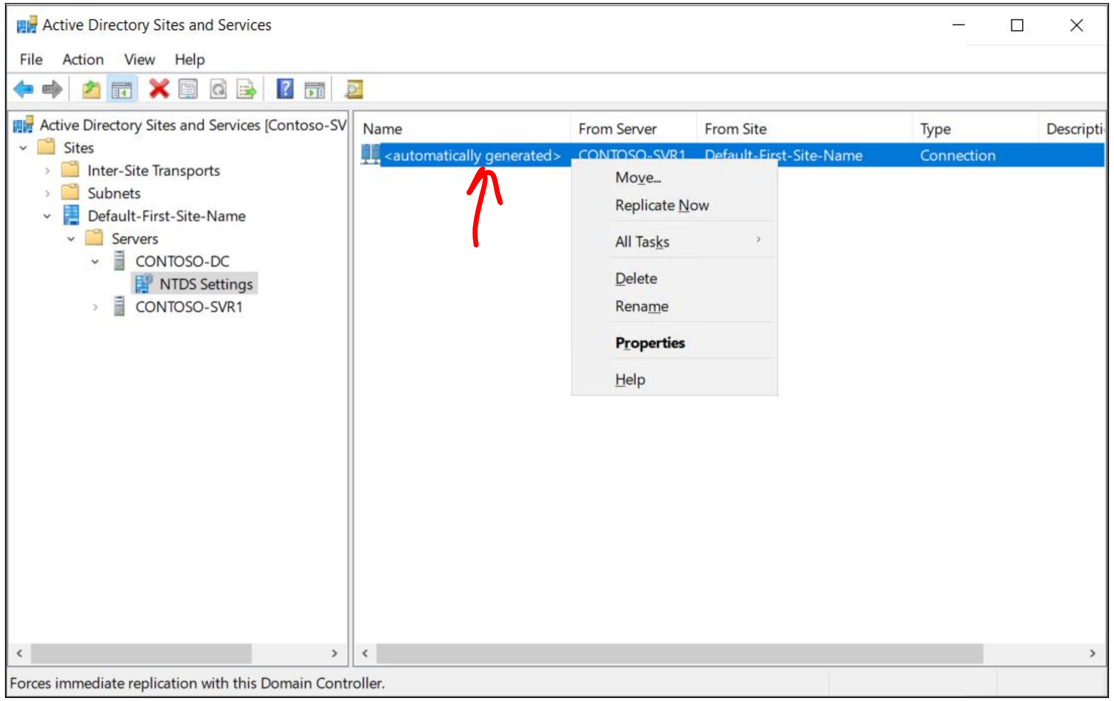
You can investigate and resolve most Active Directory replication using one of two tools:

- 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



Name	From Server	From Site	Type	Descripti
<automatically generated>	CONTOSO-SVR1	Default-First-Site-Name	Connection	

Forces immediate replication with this Domain Controller.

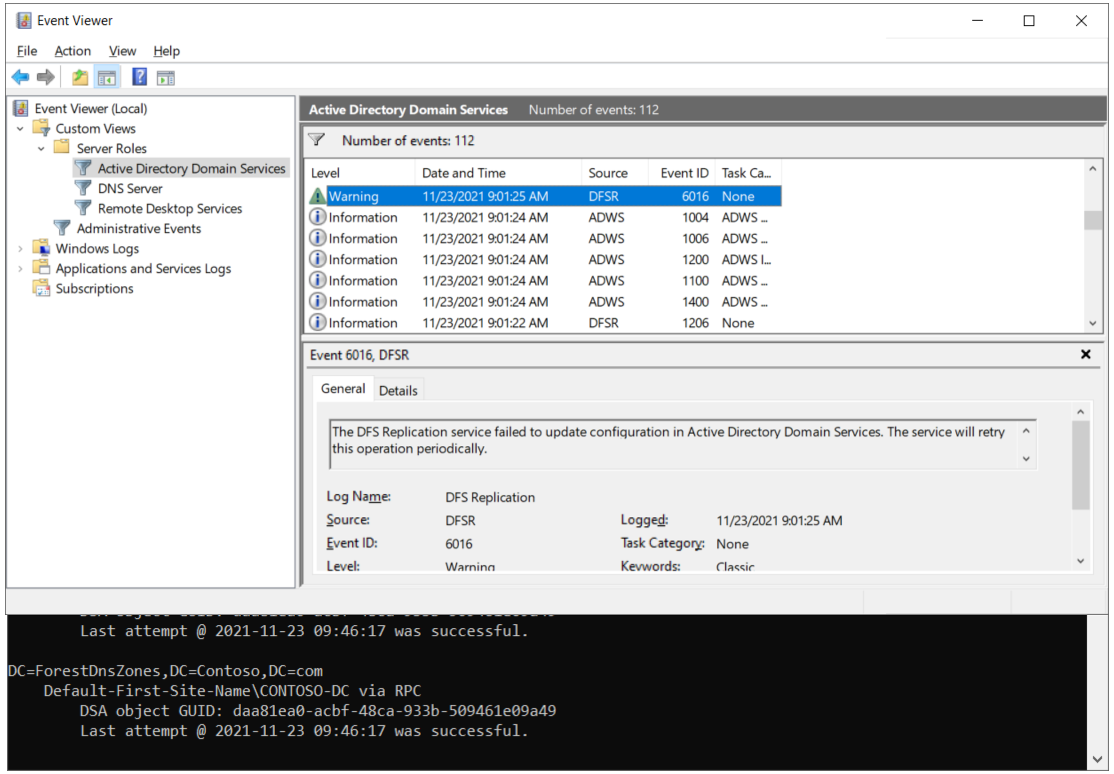
Troubleshoot AD DS replication

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.



Number of events: 112

Level	Date and Time	Source	Event ID	Task Ca...
Warning	11/23/2021 9:01:25 AM	DFSR	6016	None
Information	11/23/2021 9:01:24 AM	ADWS	1004	ADWS ...
Information	11/23/2021 9:01:24 AM	ADWS	1006	ADWS ...
Information	11/23/2021 9:01:24 AM	ADWS	1200	ADWS I...
Information	11/23/2021 9:01:24 AM	ADWS	1100	ADWS ...
Information	11/23/2021 9:01:24 AM	ADWS	1400	ADWS ...
Information	11/23/2021 9:01:22 AM	DFSR	1206	None

The DFS Replication service failed to update configuration in Active Directory Domain Services. The service will retry this operation periodically.

Log Name: DFS Replication
Source: DFSR
Logged: 11/23/2021 9:01:25 AM
Event ID: 6016
Task Category: None
Level: Warning
Keywords: Classic

```
        Last attempt @ 2021-11-23 09:46:17 was successful.

DC=ForestDnsZones,DC=Contoso,DC=com
    Default-First-Site-Name\CONTOSO-DC via RPC
        DSA object GUID: daa81ea0-acbf-48ca-933b-509461e09a49
        Last attempt @ 2021-11-23 09:46:17 was successful.
```

Troubleshoot AD DS replication

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

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

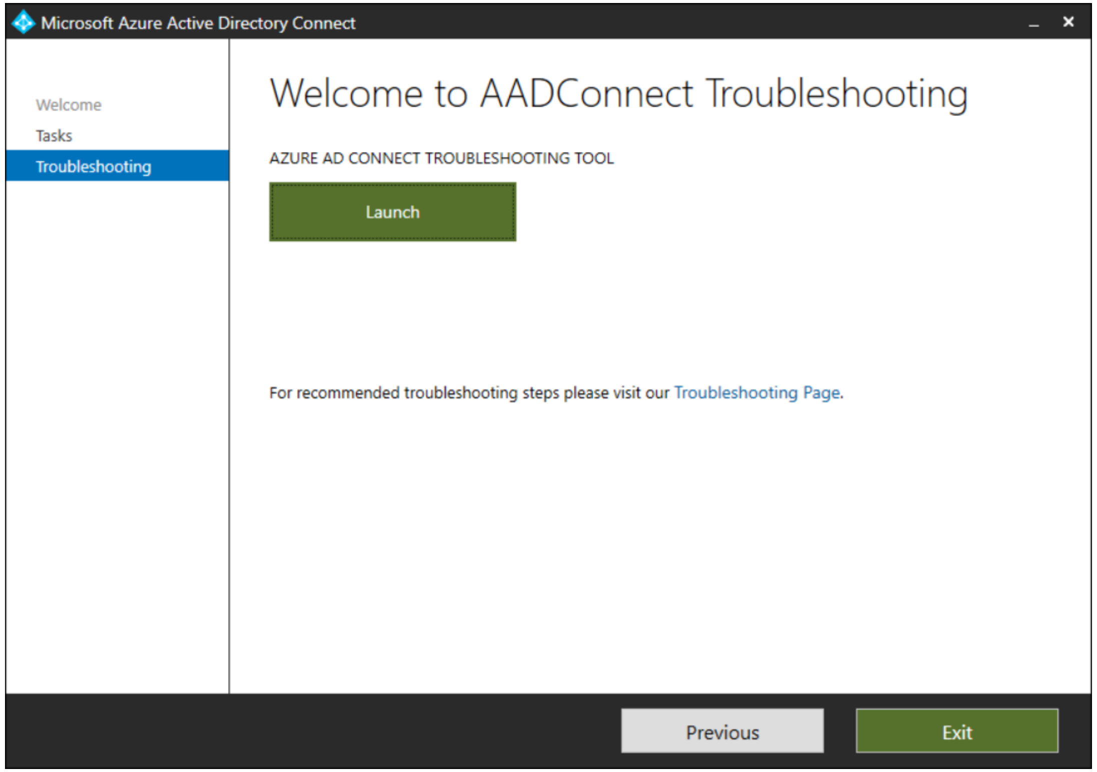
Prepare to synchronize

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



Microsoft Azure Active Directory Connect

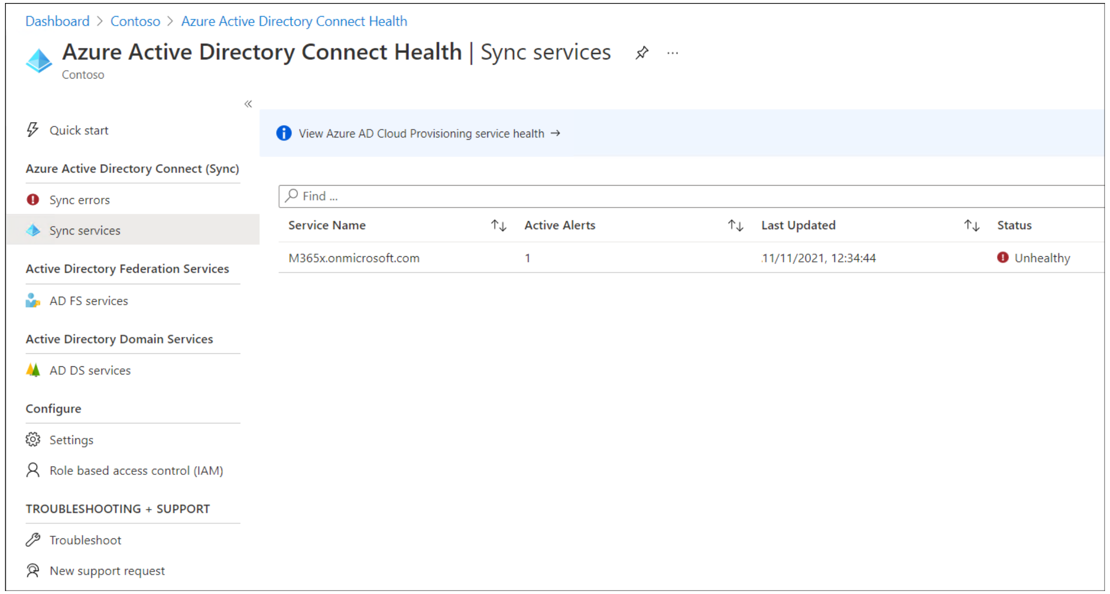
Welcome to AADConnect Troubleshooting

AZURE AD CONNECT TROUBLESHOOTING TOOL

For recommended troubleshooting steps please visit our Troubleshooting Page.

Troubleshoot hybrid authentication issues

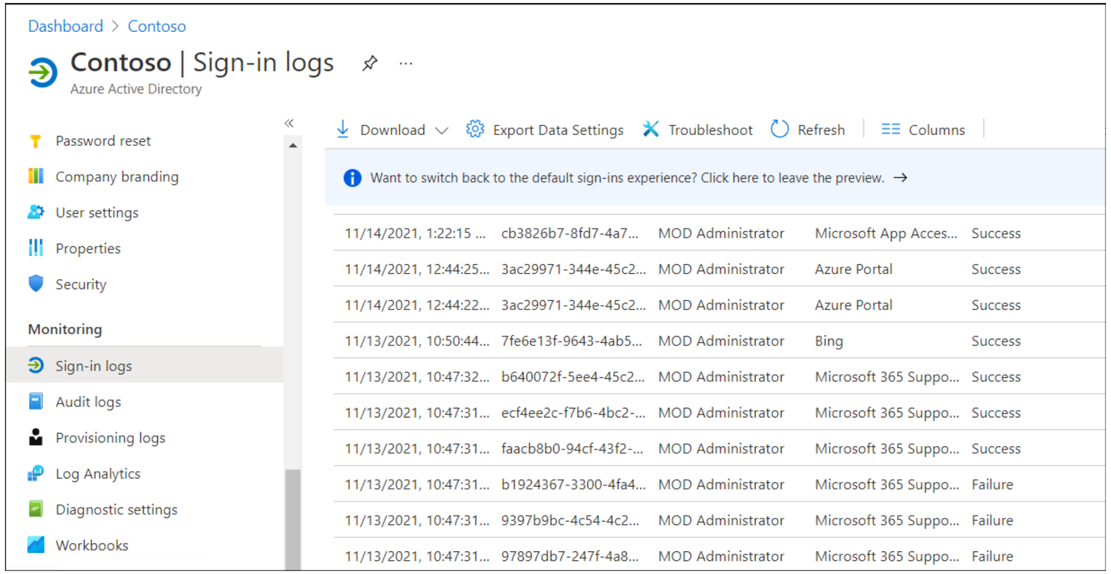
Monitor Azure AD Connect


Dashboard > Contoso > Azure Active Directory Connect Health
Azure Active Directory Connect Health | Sync services
Contoso
Quick start
Azure Active Directory Connect (Sync)
Sync errors
Sync services
Active Directory Federation Services
AD FS services
Active Directory Domain Services
AD DS services
Configure
Settings
Role based access control (IAM)
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
Find ...

View Azure AD Cloud Provisioning service health →

Service Name	Active Alerts	Last Updated	Status
M365x.onmicrosoft.com	1	11/11/2021, 12:34:44	Unhealthy

Review Azure AD sign-in logs



Want to switch back to the default sign-ins experience? Click here to leave the preview. →

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-5ee4-45c2...	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

Knowledge check and resources – Troubleshoot Active Directory

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Troubleshoot Active Directory

Lab 08

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