Contents

- Failover Clustering
- What's New in Failover Clustering
- Understand
  - Scale-Out File Server for application data
  - Cluster and pool quorum
  - Fault domain awareness
  - Simplified SMB Multichannel and multi-NIC cluster networks
  - VM load balancing
  - Cluster sets
  - Cluster affinity
- Plan
  - Hardware requirements
  - Use Cluster Shared Volumes (CSVs
  - Using guest VM clusters
- Deploy
  - Create a failover cluster
  - Deploy a two-node file server
  - Deploy a cluster set
  - Prestage a cluster in AD DS
    - Configuring cluster accounts in Active Directory
  - Manage quorum and witnesses
  - Deploy a Cloud Witness
  - Deploy a file share witness
  - Cluster operating system rolling upgrades
  - Upgrading a failover cluster on the same hardware
- Manage
  - Cluster-Aware Updating
    - Requirements and best practices
    - Advanced options

FAQ
Plug-ins
Health Service reports
Health Service faults
Cluster-domain migration
Troubleshooting using Windows Error Reporting
Troubleshooting cluster issue with Event ID 1135
A problem with deleting a node
Remove node from active failover cluster membership
Adjust the failover baseline network threshold
Cluster system log events
Use BitLocker with Cluster Shared Volumes
Change history for Failover Clustering topics

Failover Clustering in Windows Server and Azure Stack HCI

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

A failover cluster is a group of independent computers that work together to increase the availability and scalability of clustered roles (formerly called clustered applications and services). The clustered servers (called nodes) are connected by physical cables and by software. If one or more of the cluster nodes fail, other nodes begin to provide service (a process known as failover). In addition, the clustered roles are proactively monitored to verify that they are working properly. If they are not working, they are restarted or moved to another node.

Failover clusters also provide Cluster Shared Volume (CSV) functionality that provides a consistent, distributed namespace that clustered roles can use to access shared storage from all nodes. With the Failover Clustering feature, users experience a minimum of disruptions in service.

Failover Clustering has many practical applications, including:

- Highly available or continuously available file share storage for applications such as Microsoft SQL Server and Hyper-V virtual machines
- Highly available clustered roles that run on physical servers or on virtual machines that are installed on servers running Hyper-V

To learn more about failover clustering in Azure Stack HCI, see Understanding cluster and pool quorum.

UNDERSTAND	PLANNING	DEPLOYMENT
What's new in Failover Clustering	Planning Failover Clustering Hardware Requirements and Storage Options	Creating a Failover Cluster
Scale-Out File Server for application data	Use Cluster Shared Volumes (CSVs)	Deploy a two-node file server
Cluster and pool quorum	Using guest virtual machine clusters with Storage Spaces Direct	Prestage cluster computer objects in Active Directory Domain Services
Fault domain awareness		Configuring cluster accounts in Active Directory
Simplified SMB Multichannel and multi-NIC cluster networks		Manage the quorum and witnesses
VM load balancing		Deploy a cloud witness
Cluster sets		Deploy a file share witness
Cluster affinity		Cluster operating system rolling upgrades

UNDERSTAND	PLANNING	DEPLOYMENT
		Upgrading a failover cluster on the same hardware
		Deploy an Active Directory Detached Cluster

MANAGE	TOOLS AND SETTINGS	COMMUNITY RESOURCES
Cluster-Aware Updating	Failover Clustering PowerShell Cmdlets	High Availability (Clustering) Forum
Health Service	Cluster Aware Updating PowerShell Cmdlets	Failover Clustering and Network Load Balancing Team Blog
Cluster-domain migration		
Troubleshooting using Windows Error Reporting		

What's new in Failover Clustering

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

This topic explains the new and changed functionality in Failover Clustering for Azure Stack HCI, Windows Server 2019, and Windows Server 2016.

What's new in Windows Server 2019 and Azure Stack HCI

- **Cluster sets**

  (Applies only to Windows Server 2019) Cluster sets enable you to increase the number of servers in a single software-defined datacenter (SDDC) solution beyond the current limits of a cluster. This is accomplished by grouping multiple clusters into a cluster set--a loosely-coupled grouping of multiple failover clusters: compute, storage and hyper-converged. With cluster sets, you can move online virtual machines (live migrate) between clusters within the cluster set.

  For more info, see Cluster sets.

- **Azure-aware clusters**

  Failover clusters now automatically detect when they're running in Azure IaaS virtual machines and optimize the configuration to provide proactive failover and logging of Azure planned maintenance events to achieve the highest levels of availability. Deployment is also simplified by removing the need to configure the load balancer with Distributed Network Name for cluster name.

- **Cross-domain cluster migration**

  Failover Clusters can now dynamically move from one Active Directory domain to another, simplifying domain consolidation and allowing clusters to be created by hardware partners and joined to the customer's domain later.

- **USB witness**

  You can now use a simple USB drive attached to a network switch as a witness in determining quorum for a cluster. This extends the File Share Witness to support any SMB2-compliant device.

- **Cluster infrastructure improvements**

  The CSV cache is now enabled by default to boost virtual machine performance. MSDTC now supports Cluster Shared Volumes, to allow deploying MSDTC workloads on Storage Spaces Direct such as with SQL Server. Enhanced logic to detect partitioned nodes with self-healing to return nodes to cluster membership. Enhanced cluster network route detection and self-healing.

- **Cluster Aware Updating supports Storage Spaces Direct**

  Cluster Aware Updating (CAU) is now integrated and aware of Storage Spaces Direct, validating and ensuring data resynchronization completes on each node. Cluster Aware Updating inspects updates to intelligently restart only if necessary. This enables orchestrating restarts of all servers in the cluster for planned maintenance.

- **File share witness enhancements**

We enabled the use of a file share witness in the following scenarios:

- Absent or extremely poor Internet access because of a remote location, preventing the use of a cloud witness.
- Lack of shared drives for a disk witness. This could be a Storage Spaces Direct hyperconverged configuration, a SQL Server Always On Availability Groups (AG), or an * Exchange Database Availability Group (DAG), none of which use shared disks.
- Lack of a domain controller connection due to the cluster being behind a DMZ.
- A workgroup or cross-domain cluster for which there is no Active Directory cluster name object (CNO). Find out more about these enhancements in the following post in Server & Management Blogs: Failover Cluster File Share Witness and DFS.

  We now also explicitly block the use of a DFS Namespaces share as a location. Adding a file share witness to a DFS share can cause stability issues for your cluster, and this configuration has never been supported. We added logic to detect if a share uses DFS Namespaces, and if DFS Namespaces is detected, Failover Cluster Manager blocks creation of the witness and displays an error message about not being supported.

- **Cluster hardening**

  Intra-cluster communication over Server Message Block (SMB) for Cluster Shared Volumes and Storage Spaces Direct now leverages certificates to provide the most secure platform. This allows Failover Clusters to operate with no dependencies on NTLM and enable security baselines.

- **Failover Cluster no longer uses NTLM authentication**

  Failover Clusters no longer use NTLM authentication. Instead Kerberos and certificate-based authentication is used exclusively. There are no changes required by the user, or deployment tools, to take advantage of this security enhancement. It also allows failover clusters to be deployed in environments where NTLM has been disabled.

What's new in Windows Server 2016

Cluster Operating System Rolling Upgrade

Cluster Operating System Rolling Upgrade enables an administrator to upgrade the operating system of the cluster nodes from Windows Server 2012 R2 to a newer version without stopping the Hyper-V or the Scale-Out File Server workloads. Using this feature, the downtime penalties against Service Level Agreements (SLA) can be avoided.

What value does this change add?

Upgrading a Hyper-V or Scale-Out File Server cluster from Windows Server 2012 R2 to Windows Server 2016 no longer requires downtime. The cluster will continue to function at a Windows Server 2012 R2 level until all of the nodes in the cluster are running Windows Server 2016. The cluster functional level is upgraded to Windows Server 2016 by using the Windows PowerShell cmdlet `Update-ClusterFunctionalLevel`.

> **WARNING**
>
> - After you update the cluster functional level, you cannot go back to a Windows Server 2012 R2 cluster functional level.
> - Until the `Update-ClusterFunctionalLevel` cmdlet is run, the process is reversible, and Windows Server 2012 R2 nodes can be added and Windows Server 2016 nodes can be removed.

What works differently?

A Hyper-V or Scale-Out File Server failover cluster can now easily be upgraded without any downtime or need to build a new cluster with nodes that are running the Windows Server 2016 operating system. Migrating clusters to Windows Server 2012 R2 involved taking the existing cluster offline and reinstalling the new operating system for each nodes, and then bringing the cluster back online. The old process was cumbersome and required downtime. However, in Windows Server 2016, the cluster does not need to go offline at any point.

The cluster operating systems for the upgrade in phases are as follows for each node in a cluster:

- The node is paused and drained of all virtual machines that are running on it.
- The virtual machines (or other cluster workload) are migrated to another node in the cluster.
- The existing operating system is removed and a clean installation of the Windows Server 2016 operating system on the node is performed.
- The node running the Windows Server 2016 operating system is added back to the cluster.
- At this point, the cluster is said to be running in mixed mode, because the cluster nodes are running either Windows Server 2012 R2 or Windows Server 2016.
- The cluster functional level stays at Windows Server 2012 R2. At this functional level, new features in Windows Server 2016 that affect compatibility with previous versions of the operating system will be unavailable.
- Eventually, all nodes are upgraded to Windows Server 2016.
- Cluster functional level is then changed to Windows Server 2016 using the Windows PowerShell cmdlet `Update-ClusterFunctionalLevel`. At this point, you can take advantage of the Windows Server 2016 features.

For more information, see Cluster Operating System Rolling Upgrade.

Storage Replica

Storage Replica is a new feature that enables storage-agnostic, block-level, synchronous replication between servers or clusters for disaster recovery, as well as stretching of a failover cluster between sites. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes to ensure zero data loss at the file-system level. Asynchronous replication allows site extension beyond metropolitan ranges with the possibility of data loss.

What value does this change add?

Storage Replica enables you to do the following:

- Provide a single vendor disaster recovery solution for planned and unplanned outages of mission critical workloads.
- Use SMB3 transport with proven reliability, scalability, and performance.
- Stretch Windows failover clusters to metropolitan distances.
- Use Microsoft software end to end for storage and clustering, such as Hyper-V, Storage Replica, Storage Spaces, Cluster, Scale-Out File Server, SMB3, Data Deduplication, and ReFS/NTFS.
- Help reduce cost and complexity as follows:
  - Is hardware agnostic, with no requirement for a specific storage configuration like DAS or SAN.
  - Allows commodity storage and networking technologies.
  - Features ease of graphical management for individual nodes and clusters through Failover Cluster Manager.
  - Includes comprehensive, large-scale scripting options through Windows PowerShell.

- Help reduce downtime, and increase reliability and productivity intrinsic to Windows.
- Provide supportability, performance metrics, and diagnostic capabilities.

For more information, see the Storage Replica in Windows Server 2016.

Cloud Witness

Cloud Witness is a new type of Failover Cluster quorum witness in Windows Server 2016 that leverages Microsoft Azure as the arbitration point. The Cloud Witness, like any other quorum witness, gets a vote and can participate in the quorum calculations. You can configure cloud witness as a quorum witness using the Configure a Cluster Quorum Wizard.

What value does this change add?

Using Cloud Witness as a Failover Cluster quorum witness provides the following advantages:

- Leverages Microsoft Azure and eliminates the need for a third separate datacenter.
- Uses the standard publicly available Microsoft Azure Blob Storage which eliminates the extra maintenance overhead of VMs hosted in a public cloud.
- Same Microsoft Azure Storage Account can be used for multiple clusters (one blob file per cluster; cluster unique ID used as blob file name).
- Provides a very low on-going cost to the Storage Account (very small data written per blob file, blob file updated only once when cluster nodes' state changes).

For more information, see Deploy a Cloud Witness For a Failover Cluster.

What works differently?

This capability is new in Windows Server 2016.

Virtual Machine Resiliency

Compute Resiliency Windows Server 2016 includes increased virtual machines compute resiliency to help reduce intra-cluster communication issues in your compute cluster as follows:

- **Resiliency options available for virtual machines:** You can now configure virtual machine resiliency options that define behavior of the virtual machines during transient failures:
  - **Resiliency Level:** Helps you define how the transient failures are handled.
  - **Resiliency Period:** Helps you define how long all the virtual machines are allowed to run isolated.
- **Quarantine of unhealthy nodes:** Unhealthy nodes are quarantined and are no longer allowed to join the cluster. This prevents flapping nodes from negatively effecting other nodes and the overall cluster.

For more information virtual machine compute resiliency workflow and node quarantine settings that control how your node is placed in isolation or quarantine, see Virtual Machine Compute Resiliency in Windows Server 2016.

Storage Resiliency In Windows Server 2016, virtual machines are more resilient to transient storage failures. The improved virtual machine resiliency helps preserve tenant virtual machine session states in the event of a storage disruption. This is achieved by intelligent and quick virtual machine response to storage infrastructure issues.

When a virtual machine disconnects from its underlying storage, it pauses and waits for storage to recover. While paused, the virtual machine retains the context of applications that are running in it. When the virtual machine's connection to its storage is restored, the virtual machine returns to its running state. As a result, the

tenant machine's session state is retained on recovery.

In Windows Server 2016, virtual machine storage resiliency is aware and optimized for guest clusters too.

Diagnostic Improvements in Failover Clustering

To help diagnose issues with failover clusters, Windows Server 2016 includes the following:

- Several enhancements to cluster log files (such as Time Zone Information and DiagnosticVerbose log) that makes it easier to troubleshoot failover clustering issues. For more information, see Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Cluster Log.
- A new a dump type of **Active memory dump**, which filters out most memory pages allocated to virtual machines, and therefore makes the memory.dmp much smaller and easier to save or copy. For more information, see Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Active Dump.

Site-aware Failover Clusters

Windows Server 2016 includes site-aware failover clusters that enable group nodes in stretched clusters, based on their physical location (site). Cluster site-awareness enhances key operations during the cluster lifecycle, such as failover behavior, placement policies, heartbeat between the nodes, and quorum behavior. For more information, see Site-aware Failover Clusters in Windows Server 2016.

Workgroup and Multi-domain clusters

In Windows Server 2012 R2 and previous versions, a cluster can only be created between member nodes joined to the same domain. Windows Server 2016 breaks down these barriers and introduces the ability to create a Failover Cluster without Active Directory dependencies. You can now create failover clusters in the following configurations:

- **Single-domain Clusters.** Clusters with all nodes joined to the same domain.
- **Multi-domain Clusters.** Clusters with nodes which are members of different domains.
- **Workgroup Clusters.** Clusters with nodes which are member servers / workgroup (not domain joined).

For more information, see Workgroup and Multi-domain clusters in Windows Server 2016

Virtual Machine Load Balancing

Virtual machine Load Balancing is a new feature in Failover Clustering that facilitates the seamless load balancing of virtual machines across the nodes in a cluster. Over-committed nodes are identified based on virtual machine Memory and CPU utilization on the node. Virtual machines are then moved (live migrated) from an over-committed node to nodes with available bandwidth (if applicable). The aggressiveness of the balancing can be tuned to ensure optimal cluster performance and utilization. Load Balancing is enabled by default in Windows Server 2016 Technical Preview. However, Load Balancing is disabled when SCVMM Dynamic Optimization is enabled.

Virtual Machine Start Order

Virtual machine Start Order is a new feature in Failover Clustering that introduces start order orchestration for Virtual machines (and all groups) in a cluster. Virtual machines can now be grouped into tiers, and start order dependencies can be created between different tiers. This ensures that the most important virtual machines (such as Domain Controllers or Utility virtual machines) are started first. Virtual machines are not started until the virtual machines that they have a dependency on are also started.

Simplified SMB Multichannel and Multi-NIC Cluster Networks

Failover Cluster networks are no longer limited to a single NIC per subnet / network. With Simplified SMB Multichannel and Multi-NIC Cluster Networks, network configuration is automatic and every NIC on the subnet can be used for cluster and workload traffic. This enhancement allows customers to maximize network throughput for Hyper-V, SQL Server Failover Cluster Instance, and other SMB workloads.

For more information, see Simplified SMB Multichannel and Multi-NIC Cluster Networks.

See Also

- Storage
- What's New in Storage in Windows Server 2016

Scale-Out File Server for application data overview

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Scale-Out File Server is designed to provide scale-out file shares that are continuously available for file-based server application storage. Scale-out file shares provide the ability to share the same folder from multiple nodes of the same cluster. This scenario focuses on how to plan for and deploy Scale-Out File Server.

You can deploy and configure a clustered file server by using either of the following methods:

- **Scale-Out File Server for application data** This clustered file server feature was introduced in Windows Server 2012, and it lets you store server application data, such as Hyper-V virtual machine files, on file shares, and obtain a similar level of reliability, availability, manageability, and high performance that you would expect from a storage area network. All file shares are simultaneously online on all nodes. File shares associated with this type of clustered file server are called scale-out file shares. This is sometimes referred to as active-active. This is the recommended file server type when deploying either Hyper-V over Server Message Block (SMB) or Microsoft SQL Server over SMB.
- **File Server for general use** This is the continuation of the clustered file server that has been supported in Windows Server since the introduction of Failover Clustering. This type of clustered file server, and therefore all the shares associated with the clustered file server, is online on one node at a time. This is sometimes referred to as active-passive or dual-active. File shares associated with this type of clustered file server are called clustered file shares. This is the recommended file server type when deploying information worker scenarios.

Scenario description

With scale-out file shares, you can share the same folder from multiple nodes of a cluster. For instance, if you have a four-node file server cluster that is using Server Message Block (SMB) Scale-Out, a computer running Windows Server 2012 R2 or Windows Server 2012 can access file shares from any of the four nodes. This is achieved by applying new Windows Server Failover Clustering features and the capabilities of the Windows file server protocol, SMB 3.0. File server administrators can provide scale-out file shares and continuously available file services to server applications and respond to increased demands quickly by bringing more servers online. All of this can be done in a production environment, and it is completely transparent to the server application.

Key benefits provided by Scale-Out File Server in include:

- **Active-Active file shares**. All cluster nodes can accept and serve SMB client requests. By making the file share content accessible through all cluster nodes simultaneously, SMB 3.0 clusters and clients cooperate to provide transparent failover to alternative cluster nodes during planned maintenance and unplanned failures with service interruption.
- **Increased bandwidth**. The maximum share bandwidth is the total bandwidth of all file server cluster nodes. Unlike previous versions of Windows Server, the total bandwidth is no longer constrained to the bandwidth of a single cluster node; but rather, the capability of the backing storage system defines the constraints. You can increase the total bandwidth by adding nodes.
- **CHKDSK with zero downtime**. CHKDSK in Windows Server 2012 is enhanced to dramatically shorten the time a file system is offline for repair. Clustered shared volumes (CSVs) take this one step further by eliminating the offline phase. A CSV File System (CSVFS) can use CHKDSK without impacting applications with open handles on the file system.

- **Clustered Shared Volume cache**. CSVs in Windows Server 2012 introduces support for a Read cache, which can significantly improve performance in certain scenarios, such as in Virtual Desktop Infrastructure (VDI).
- **Simpler management**. With Scale-Out File Server, you create the scale-out file servers, and then add the necessary CSVs and file shares. It is no longer necessary to create multiple clustered file servers, each with separate cluster disks, and then develop placement policies to ensure activity on each cluster node.
- **Automatic rebalancing of Scale-Out File Server clients**. In Windows Server 2012 R2, automatic rebalancing improves scalability and manageability for scale-out file servers. SMB client connections are tracked per file share (instead of per server), and clients are then redirected to the cluster node with the best access to the volume used by the file share. This improves efficiency by reducing redirection traffic between file server nodes. Clients are redirected following an initial connection and when cluster storage is reconfigured.

In this scenario

The following articles are available to help you deploy a Scale-Out File Server:

- Plan for Scale-Out File Server
  - Step 1: Plan for Storage in Scale-Out File Server
  - Step 2: Plan for Networking in Scale-Out File Server
- Deploy Scale-Out File Server
  - Step 1: Install Prerequisites for Scale-Out File Server
  - Step 2: Configure Scale-Out File Server
  - Step 3: Configure Hyper-V to Use Scale-Out File Server
  - Step 4: Configure Microsoft SQL Server to Use Scale-Out File Server

When to use Scale-Out File Server

You should not use Scale-Out File Server if your workload generates a high number of metadata operations, such as opening files, closing files, creating new files, or renaming existing files. A typical information worker would generate several metadata operations. You should use a Scale-Out File Server if you are interested in the scalability and simplicity that it offers and if you only require technologies that are supported with Scale-Out File Server.

The following table lists the capabilities in SMB 3.0, the common Windows file systems, file server data management technologies, and common workloads. You can see whether the technology is supported with Scale-Out File Server, or if it requires a traditional clustered file server (also known as a file server for general use).

TECHNOLOGY AREA	FEATURE	GENERAL USE FILE SERVER CLUSTER	SCALE-OUT FILE SERVER
SMB	SMB Continuous Availability (*)	Yes	Yes
SMB	SMB Multichannel	Yes	Yes
SMB	SMB Direct	Yes	Yes
SMB	SMB Encryption	Yes	Yes

TECHNOLOGY AREA	FEATURE	GENERAL USE FILE SERVER CLUSTER	SCALE-OUT FILE SERVER
SMB	SMB Transparent failover	Yes (if continuous availability is enabled)	Yes
File System	NTFS	Yes	NA
File System	Resilient File System (ReFS)	Recommended with Storage Spaces Direct	Recommended with Storage Spaces Direct
File System	Cluster Shared Volume File System (CSV)	NA	Yes
File Management	BranchCache	Yes	No
File Management	Data Deduplication (Windows Server 2012)	Yes	No
File Management	Data Deduplication (Windows Server 2012 R2)	Yes	Yes (VDI only)
File Management	DFS Namespace (DFSN) root server root	Yes	No
File Management	DFS Namespace (DFSN) folder target server	Yes	Yes
File Management	DFS Replication (DFSR)	Yes	No
File Management	File Server Resource Manager (Screens and Quotas)	Yes	No
File Management	File Classification Infrastructure	Yes	No
File Management	Dynamic Access Control (claim-based access, CAP)	Yes	No
File Management	Folder Redirection	Yes	Not recommended
File Management	Offline Files (client side caching)	Yes	Not recommended
File Management	Roaming User Profiles	Yes	Not recommended
File Management	Home Directories	Yes	Not recommended
File Management	Work Folders	Yes	No
NFS	NFS Server	Yes	No
Applications	Hyper-V	Not recommended	Yes

TECHNOLOGY AREA	FEATURE	GENERAL USE FILE SERVER CLUSTER	SCALE-OUT FILE SERVER
Applications	Microsoft SQL Server	Not recommended	Yes

* SMB loopback Continuous Availability (CA) in hyper-converged configurations is available in Windows Server 2019.

> **NOTE**
> Folder Redirection, Offline Files, Roaming User Profiles, or Home Directories generate a large number of writes that must be immediately written to disk (without buffering) when using continuously available file shares, reducing performance as compared to general purpose file shares. Continuously available file shares are also incompatible with File Server Resource Manager and PCs running Windows XP. Additionally, Offline Files might not transition to offline mode for 3-6 minutes after a user loses access to a share, which could frustrate users who aren't yet using the Always Offline mode of Offline Files.

Practical applications

Scale-Out File Servers are ideal for server application storage. Some examples of server applications that can store their data on a scale-out file share are listed below:

- The Internet Information Services (IIS) Web server can store configuration and data for Web sites on a scale-out file share. For more information, see Shared Configuration.
- Hyper-V can store configuration and live virtual disks on a scale-out file share. For more information, see Deploy Hyper-V over SMB.
- SQL Server can store live database files on a scale-out file share. For more information, see Install SQL Server with SMB file share as a storage option.
- Virtual Machine Manager (VMM) can store a library share (which contains virtual machine templates and related files) on a scale-out file share. However, the library server itself can't be a Scale-Out File Server—it must be on a stand-alone server or a failover cluster that doesn't use the Scale-Out File Server cluster role.

If you use a scale-out file share as a library share, you can use only technologies that are compatible with Scale-Out File Server. For example, you can't use DFS Replication to replicate a library share hosted on a scale-out file share. It's also important that the scale-out file server has the latest software updates installed.

To use a scale-out file share as a library share, first add a library server (likely a virtual machine) with a local share or no shares at all. Then when you add a library share, choose a file share that's hosted on a scale-out file server. This share should be VMM-managed and created exclusively for use by the library server. Also make sure to install the latest updates on the scale-out file server. For more information about adding VMM library servers and library shares, see Add profiles to the VMM library. For a list of currently available hotfixes for File and Storage Services, see Microsoft Knowledge Base article 2899011.

> **NOTE**
> Some users, such as information workers, have workloads that have a greater impact on performance. For example, operations like opening and closing files, creating new files, and renaming existing files, when performed by multiple users, have an impact on performance. If a file share is enabled with continuous availability, it provides data integrity, but it also affects the overall performance. Continuous availability requires that data writes through to the disk to ensure integrity in the event of a failure of a cluster node in a Scale-Out File Server. Therefore, a user that copies several large files to a file server can expect significantly slower performance on continuously available file share.

Features included in this scenario

The following table lists the features that are part of this scenario and describes how they support it.

FEATURE	HOW IT SUPPORTS THIS SCENARIO
Failover Clustering	Failover clusters added the following features in Windows Server 2012 to support scale-Out file server: Distributed Network Name, the Scale-Out File Server resource type, Cluster Shared Volumes (CSV) 2, and the Scale-Out File Server High Availability role. For more information about these features, see What's New in Failover Clustering in Windows Server 2012 [redirected].
Server Message Block	SMB 3.0 added the following features in Windows Server 2012 to support scale-Out File Server: SMB Transparent Failover, SMB Multichannel, and SMB Direct. For more information on new and changed functionality for SMB in Windows Server 2012 R2, see What's New in SMB in Windows Server.

More information

- Software-Defined Storage Design Considerations Guide
- Increasing Server, Storage, and Network Availability
- Deploy Hyper-V over SMB
- Deploying Fast and Efficient File Servers for Server Applications
- To scale out or not to scale out, that is the question (blog post)
- Folder Redirection, Offline Files, and Roaming User Profiles

Fault domain awareness

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

Failover Clustering enables multiple servers to work together to provide high availability – or put another way, to provide node fault tolerance. But today's businesses demand ever-greater availability from their infrastructure. To achieve cloud-like uptime, even highly unlikely occurrences such as chassis failures, rack outages, or natural disasters must be protected against. That's why Failover Clustering in Windows Server 2016 introduced chassis, rack, and site fault tolerance as well.

Fault domains and fault tolerance

Fault domains and fault tolerance are closely related concepts. A fault domain is a set of hardware components that share a single point of failure. To be fault tolerant to a certain level, you need multiple fault domains at that level. For example, to be rack fault tolerant, your servers and your data must be distributed across multiple racks.

This short video presents an overview of fault domains in Windows Server 2016:

Fault domain awareness in Windows Server 2019

Fault domain awareness is available in Windows Server 2019 but it's disabled by default and must be enabled through the Windows Registry.

To enable fault domain awareness in Windows Server 2019, go to the Windows Registry and set the (Get-Cluster).AutoAssignNodeSite registry key to 1.

```
(Get-Cluster).AutoAssignNodeSite=1
```

To disable fault domain awareness in Windows 2019, go to the Windows Registry and set the (Get-

Cluster).AutoAssignNodeSite registry key to 0.

```
(Get-Cluster).AutoAssignNodeSite=0
```

Benefits

- **Storage Spaces, including Storage Spaces Direct, uses fault domains to maximize data safety.** Resiliency in Storage Spaces is conceptually like distributed, software-defined RAID. Multiple copies of all data are kept in sync, and if hardware fails and one copy is lost, others are recopied to restore resiliency. To achieve the best possible resiliency, copies should be kept in separate fault domains.
- **The Health Service uses fault domains to provide more helpful alerts.** Each fault domain can be associated with location metadata, which will automatically be included in any subsequent alerts. These descriptors can assist operations or maintenance personnel and reduce errors by disambiguating hardware.
- **Stretch clustering uses fault domains for storage affinity.** Stretch clustering allows faraway servers to join a common cluster. For the best performance, applications or virtual machines should be run on servers that are nearby to those providing their storage. Fault domain awareness enables this storage affinity.

Levels of fault domains

There are four canonical levels of fault domains - site, rack, chassis, and node. Nodes are discovered automatically; each additional level is optional. For example, if your deployment does not use blade servers, the chassis level may not make sense for you.

Usage

You can use PowerShell or XML markup to specify fault domains. Both approaches are equivalent and provide full functionality.

> **IMPORTANT**
> Specify fault domains before enabling Storage Spaces Direct, if possible. This enables the automatic configuration to prepare the pool, tiers, and settings like resiliency and column count, for chassis or rack fault tolerance. Once the pool and volumes have been created, data will not retroactively move in response to changes to the fault domain topology. To move nodes between chassis or racks after enabling Storage Spaces Direct, you should first evict the node and its drives from the pool using `Remove-ClusterNode -CleanUpDisks`.

Defining fault domains with PowerShell

Windows Server 2016 introduces the following cmdlets to work with fault domains:

- `Get-ClusterFaultDomain`
- `Set-ClusterFaultDomain`
- `New-ClusterFaultDomain`
- `Remove-ClusterFaultDomain`

This short video demonstrates the usage of these cmdlets.

Use `Get-ClusterFaultDomain` to see the current fault domain topology. This will list all nodes in the cluster, plus any chassis, racks, or sites you have created. You can filter using parameters like **-Type** or **-Name**, but these are not required.

```
Get-ClusterFaultDomain
Get-ClusterFaultDomain -Type Rack
Get-ClusterFaultDomain -Name "server01.contoso.com"
```

Use `New-ClusterFaultDomain` to create new chassis, racks, or sites. The `-Type` and `-Name` parameters are required. The possible values for `-Type` are `Chassis`, `Rack`, and `Site`. The `-Name` can be any string. (For `Node` type fault domains, the name must be the actual node name, as set automatically).

```
New-ClusterFaultDomain -Type Chassis -Name "Chassis 007"
New-ClusterFaultDomain -Type Rack -Name "Rack A"
New-ClusterFaultDomain -Type Site -Name "Shanghai"
```

> **IMPORTANT**
> Windows Server cannot and does not verify that any fault domains you create correspond to anything in the real, physical world. (This may sound obvious, but it's important to understand.) If, in the physical world, your nodes are all in one rack, then creating two `-Type Rack` fault domains in software does not magically provide rack fault tolerance. You are responsible for ensuring the topology you create using these cmdlets matches the actual arrangement of your hardware.

Use `Set-ClusterFaultDomain` to move one fault domain into another. The terms "parent" and "child" are commonly used to describe this nesting relationship. The `-Name` and `-Parent` parameters are required. In `-Name`, provide the name of the fault domain that is moving; in `-Parent`, provide the name of the destination. To move multiple fault domains at once, list their names.

```
Set-ClusterFaultDomain -Name "server01.contoso.com" -Parent "Rack A"
Set-ClusterFaultDomain -Name "Rack A", "Rack B", "Rack C", "Rack D" -Parent "Shanghai"
```

> **IMPORTANT**
> When fault domains move, their children move with them. In the above example, if Rack A is the parent of server01.contoso.com, the latter does not separately need to be moved to the Shanghai site – it is already there by virtue of its parent being there, just like in the physical world.

You can see parent-child relationships in the output of `Get-ClusterFaultDomain`, in the `ParentName` and `ChildrenNames` columns.

You can also use `Set-ClusterFaultDomain` to modify certain other properties of fault domains. For example, you can provide optional `-Location` or `-Description` metadata for any fault domain. If provided, this information will be included in hardware alerting from the Health Service. You can also rename fault domains using the `-NewName` parameter. Do not rename `Node` type fault domains.

```
Set-ClusterFaultDomain -Name "Rack A" -Location "Building 34, Room 4010"
Set-ClusterFaultDomain -Type Node -Description "Contoso XYZ Server"
Set-ClusterFaultDomain -Name "Shanghai" -NewName "China Region"
```

Use `Remove-ClusterFaultDomain` to remove chassis, racks, or sites you have created. The `-Name` parameter is required. You cannot remove a fault domain that contains children – first, either remove the children, or move them outside using `Set-ClusterFaultDomain`. To move a fault domain outside of all other fault domains, set its `-Parent` to the empty string ("). You cannot remove `Node` type fault domains. To remove multiple fault domains at once, list their names.

```
Set-ClusterFaultDomain -Name "server01.contoso.com" -Parent ""
Remove-ClusterFaultDomain -Name "Rack A"
```

Defining fault domains with XML markup

Fault domains can be specified using an XML-inspired syntax. We recommend using your favorite text editor, such as Visual Studio Code (available for free *here*) or Notepad, to create an XML document which you can save and reuse.

This short video demonstrates the usage of XML Markup to specify fault domains.

In PowerShell, run the following cmdlet: `Get-ClusterFaultDomainXML`. This returns the current fault domain specification for the cluster, as XML. This reflects every discovered `<Node>`, wrapped in opening and closing `<Topology>` tags.

Run the following to save this output to a file.

```
Get-ClusterFaultDomainXML | Out-File <Path>
```

Open the file, and add `<Site>`, `<Rack>`, and `<Chassis>` tags to specify how these nodes are distributed across sites, racks, and chassis. Every tag must be identified by a unique **Name**. For nodes, you must keep the node's name as populated by default.

> **IMPORTANT**
>
> While all additional tags are optional, they must adhere to the transitive Site > Rack > Chassis > Node hierarchy, and must be properly closed. In addition to name, freeform `Location="..."` and `Description="..."` descriptors can be added to any tag.

Example: Two sites, one rack each

```
<Topology>
  <Site Name="SEA" Location="Contoso HQ, 123 Example St, Room 4010, Seattle">
    <Rack Name="A01" Location="Aisle A, Rack 01">
      <Node Name="Server01" Location="Rack Unit 33" />
      <Node Name="Server02" Location="Rack Unit 35" />
      <Node Name="Server03" Location="Rack Unit 37" />
    </Rack>
  </Site>
  <Site Name="NYC" Location="Regional Datacenter, 456 Example Ave, New York City">
    <Rack Name="B07" Location="Aisle B, Rack 07">
      <Node Name="Server04" Location="Rack Unit 20" />
      <Node Name="Server05" Location="Rack Unit 22" />
      <Node Name="Server06" Location="Rack Unit 24" />
    </Rack>
  </Site>
</Topology>
```

Example: two chassis, blade servers

```
<Topology>
  <Rack Name="A01" Location="Contoso HQ, Room 4010, Aisle A, Rack 01">
    <Chassis Name="Chassis01" Location="Rack Unit 2 (Upper)" >
      <Node Name="Server01" Location="Left" />
      <Node Name="Server02" Location="Right" />
    </Chassis>
    <Chassis Name="Chassis02" Location="Rack Unit 6 (Lower)" >
      <Node Name="Server03" Location="Left" />
      <Node Name="Server04" Location="Right" />
    </Chassis>
  </Rack>
</Topology>
```

To set the new fault domain specification, save your XML and run the following in PowerShell.

```
$xml = Get-Content <Path> | Out-String
Set-ClusterFaultDomainXML -XML $xml
```

This guide presents just two examples, but the `<Site>`, `<Rack>`, `<Chassis>`, and `<Node>` tags can be mixed and

matched in many additional ways to reflect the physical topology of your deployment, whatever that may be. We hope these examples illustrate the flexibility of these tags and the value of freeform location descriptors to disambiguate them.

Optional: Location and description metadata

You can provide optional **Location** or **Description** metadata for any fault domain. If provided, this information will be included in hardware alerting from the Health Service. This short video demonstrates the value of adding such descriptors.

Simplified SMB Multichannel and Multi-NIC Cluster Networks

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

Simplified SMB Multichannel and Multi-NIC Cluster Networks is a feature that enables the use of multiple NICs on the same cluster network subnet, and automatically enables SMB Multichannel.

Simplified SMB Multichannel and Multi-NIC Cluster Networks provides the following benefits:

- Failover Clustering automatically recognizes all NICs on nodes that are using the same switch / same subnet - no additional configuration needed.
- SMB Multichannel is enabled automatically.
- Networks that only have IPv6 Link Local (fe80) IP Addresses resources are recognized on cluster-only (private) networks.
- A single IP Address resource is configured on each Cluster Access Point (CAP) Network Name (NN) by default.
- Cluster validation no longer issues warning messages when multiple NICs are found on the same subnet.

Requirements

- Multiple NICs per server, using the same switch / subnet.

How to take advantage of multi-NIC clusters networks and simplified SMB multichannel

This section describes how to take advantage of the new multi-NIC clusters networks and simplified SMB multichannel features.

Use at least two networks for Failover Clustering

Although it is rare, network switches can fail - it is still best practice to use at least two networks for Failover Clustering. All networks that are found are used for cluster heartbeats. Avoid using a single network for your Failover Cluster in order to avoid a single point of failure. Ideally, there should be multiple physical communication paths between the nodes in the cluster, and no single point of failure.

Figure 1: Use at least two networks for Failover Clustering

Use Multiple NICs across clusters

Maximum benefit of the simplified SMB multichannel is achieved when multiple NICs are used across clusters - in both storage and storage workload clusters. This allows the workload clusters (Hyper-V, SQL Server Failover Cluster Instance, Storage Replica, etc.) to use SMB multichannel and results in more efficient use of the network. In a converged (also known as disaggregated) cluster configuration where a Scale-out File Server cluster is used for storing workload data for a Hyper-V or SQL Server Failover Cluster Instance cluster, this network is often called "the North-South subnet" / network. Many customers maximize throughput of this network by investing in RDMA capable NIC cards and switches.

Figure 2: To achieve maximum network throughput, use multiple NICs on both the Scale-out File Server cluster and the Hyper-V or SQL Server Failover Cluster Instance cluster - which share the North-South subnet

Figure 3: Two clusters (Scale-out File Server for storage, SQL Server FCI for workload) both use multiple NICs in the same subnet to leverage SMB Multichannel and achieve better network throughput.

Automatic recognition of IPv6 Link Local private networks

When private (cluster only) networks with multiple NICs are detected, the cluster will automatically recognize IPv6 Link Local (fe80) IP addresses for each NIC on each subnet. This saves administrators time since they no longer have to manually configure IPv6 Link Local (fe80) IP Address resources.

When using more than one private (cluster only) network, check the IPv6 routing configuration to ensure that routing is not configured to cross subnets, since this will reduce network performance.

Figure 4: Automatic IPv6 Link Local (fe80) Address resource configuration

Throughput and Fault Tolerance

Windows Server 2019 and Windows Server 2016 automatically detect NIC capabilities and will attempt to use each NIC in the fastest possible configuration. NICs that are teamed, NICs using RSS, and NICs with RDMA capability can all be used. The table below summarizes the trade-offs when using these technologies. Maximum throughput is achieved when using multiple RDMA capable NICs. For more information, see The basics of SMB multichannel.

	Throughput	Fault Tolerance for SMB	Fault Tolerance for non-SMB	Lower CPU utilization
Single NIC (no RSS)	▲			
Multiple NICs (no RSS)	▲▲	▲		
Multiple NICs (no RSS) + NIC Teaming	▲▲	▲▲	▲	
Single NIC (with RSS)	▲			
Multiple NICs (with RSS)	▲▲	▲		
Multiple NICs (with RSS) + NIC Teaming	▲▲	▲▲	▲	
Single NIC (with RDMA)	▲			▲
Multiple NICs (with RDMA)	▲▲	▲		▲

Figure 5: Throughput and fault tolerance for various NIC configurations

Frequently asked questions

Are all NICs in a multi-NIC network used for cluster heart beating? Yes.

Can a multi-NIC network be used for cluster communication only? Or can it only be used for client and cluster communication? Either configuration will work - all cluster network roles will work on a multi-NIC network.

Is SMB Multichannel also used for CSV and cluster traffic? Yes, by default all cluster and CSV traffic will use available multi-NIC networks. Administrators can use the Failover Clustering PowerShell cmdlets or Failover Cluster Manager UI to change the network role.

How can I see the SMB Multichannel settings? Use the **Get-SMBServerConfiguration** cmdlet, look for

the value of the **EnableMultiChannel** property.

Is the cluster common property PlumbAllCrossSubnetRoutes respected on a multi-NIC network?
Yes.

Additional References

- What's New in Failover Clustering in Windows Server

Cluster affinity

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

A failover cluster can hold many roles that can move between nodes and run. There are times when certain roles (that is, virtual machines, resource groups, and so on) should not run on the same node. This could be because of resource consumption, memory usage, and so on. For example, there are two virtual machines that are memory and CPU intensive and if the two virtual machines are running on the same node, one or both of the virtual machines could have performance impact issues. This article will explain cluster antiaffinity levels and how you can use them.

What is Affinity and AntiAffinity?

Affinity is a rule you would set up that establishes a relationship between two or more roles (i,e, virtual machines, resource groups, and so on) to keep them together. AntiAffinity is the same but is used to try to keep the specified roles apart from each other. Failover Clusters use AntiAffinity for its roles. More specifically, the AntiAffinityClassNames parameter defined on the roles so they do not run on the same node.

AntiAffinityClassnames

When looking at the properties of a group, the parameter AntiAffinityClassNames is blank as a default. In the examples below, Group1 and Group2 should be separated from running on the same node. To view the property, the PowerShell command and result would be:

```
Get-ClusterGroup Group1 | fl AntiAffinityClassNames
    AntiAffinityClassNames : {}

Get-ClusterGroup Group2 | fl AntiAffinityClassNames
    AntiAffinityClassNames : {}
```

Because AntiAffinityClassNames are not defined as a default, these roles can run together or apart. The goal is to keep them to be separated. The value for AntiAffinityClassNames can be whatever you want them to be, they just have to be the same. Say that Group1 and Group2 are domain controllers running in virtual machines and they would be best served running on different nodes. Because these are domain controllers, I will use DC for the class name. To set the value, the PowerShell command and results would be:

```
$AntiAffinity = New-Object System.Collections.Specialized.StringCollection
$AntiAffinity.Add("DC")
(Get-ClusterGroup -Name "Group1").AntiAffinityClassNames = $AntiAffinity
(Get-ClusterGroup -Name "Group2").AntiAffinityClassNames = $AntiAffinity

$AntiAffinity = New-Object System.Collections.Specialized.StringCollection
$AntiAffinity.Add("DC")
(Get-ClusterGroup -Name "Group1").AntiAffinityClassNames = $AntiAffinity
(Get-ClusterGroup -Name "Group2").AntiAffinityClassNames = $AntiAffinity

Get-ClusterGroup "Group1" | fl AntiAffinityClassNames
    AntiAffinityClassNames : {DC}

Get-ClusterGroup "Group2" | fl AntiAffinityClassNames
    AntiAffinityClassNames : {DC}
```

Now that they are set, failover clustering will attempt to keep them apart.

The AntiAffinityClassName parameter is a "soft" block. Meaning, it will try to keep them apart, but if it cannot, it will still allow them to run on the same node. For example, the groups are running on a two-node failover cluster. If one node needs to go down for maintenance, it would mean both groups would be up and running on the same node. In this case, it would be okay to have this. It may not be the most ideal, but both virtual machines will still run within acceptable performance ranges.

I need more

As mentioned, AntiAffinityClassNames is a soft block. But what if a hard block is needed? The virtual machines cannot be run on the same node; otherwise, performance impact will occur and cause some services to possibly go down.

For those cases, there is another cluster property of ClusterEnforcedAntiAffinity. This antiaffinity level will prevent at all costs any of the same AntiAffinityClassNames values from running on the same node.

To view the property and value, the PowerShell command (and result) would be:

```
Get-Cluster | fl ClusterEnforcedAntiAffinity
    ClusterEnforcedAntiAffinity : 0
```

The value of "0" means it is disabled and not to be enforced. The value of "1" enables it and is the hard block. To enable this hard block, the command (and result) is:

```
(Get-Cluster).ClusterEnforcedAntiAffinity = 1
    ClusterEnforcedAntiAffinity : 1
```

When both of these are set, the group will be prevented from coming online together. If they are on the same node, this is what you would see in Failover Cluster Manager.

In a PowerShell listing of the groups, you would see this:

```
Get-ClusterGroup

Name        State
----        -----
Group1      Offline(Anti-Affinity Conflict)
Group2      Online
```

Additional Comments

- Ensure you are using the proper AntiAffinity setting depending on the needs.
- Keep in mind that in a two-node scenario and ClusterEnforcedAntiAffinity, if one node is down, both groups will not run.
- The use of Preferred Owners on groups can be combined with AntiAffinity in a three or more node cluster.
- The AntiAffinityClassNames and ClusterEnforcedAntiAffinity settings will only take place after a recycling of the resources. That is, you can set them, but if both groups are online on the same node when set, they will both continue to remain online.

Failover clustering hardware requirements and storage options

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

You need the following hardware to create a failover cluster. To be supported by Microsoft, all hardware must be certified for the version of Windows Server that you are running, and the complete failover cluster solution must pass all tests in the Validate a Configuration Wizard. For more information about validating a failover cluster, see Validate Hardware for a Failover Cluster.

- **Servers**: We recommend that you use a set of matching computers that contain the same or similar components.

  > **NOTE**
  > If you've purchased Azure Stack HCI Integrated System solution hardware from the Azure Stack HCI Catalog through your preferred Microsoft hardware partner, the Azure Stack HCI operating system should be pre-installed.

- **Network adapters and cable (for network communication)**: If you use iSCSI, each network adapter should be dedicated to either network communication or iSCSI, not both.

  In the network infrastructure that connects your cluster nodes, avoid having single points of failure. For example, you can connect your cluster nodes by multiple, distinct networks. Alternatively, you can connect your cluster nodes with one network that's constructed with teamed network adapters, redundant switches, redundant routers, or similar hardware that removes single points of failure.

  > **NOTE**
  > If you connect cluster nodes with a single network, the network will pass the redundancy requirement in the Validate a Configuration Wizard. However, the report from the wizard will include a warning that the network should not have single points of failure.

- **Device controllers or appropriate adapters for the storage**:
  - **Serial Attached SCSI or Fibre Channel**: If you are using Serial Attached SCSI or Fibre Channel, in all clustered servers, all elements of the storage stack should be identical. It's required that the multipath I/O (MPIO) software be identical and that the Device Specific Module (DSM) software be identical. It's recommended that the mass-storage device controllers— the host bus adapter (HBA), HBA drivers, and HBA firmware—that are attached to cluster storage be identical. If you use dissimilar HBAs, you should verify with the storage vendor that you are following their supported or recommended configurations.
  - **iSCSI**: If you are using iSCSI, each clustered server should have one or more network adapters or HBAs that are dedicated to the cluster storage. The network you use for iSCSI should not be used for network communication. In all clustered servers, the network adapters you use to connect to the iSCSI storage target should be identical, and we recommend that you use Gigabit Ethernet or higher.

- **Storage**: You must use Storage Spaces Direct or shared storage that's compatible with Windows Server 2012 R2 or Windows Server 2012. You can use shared storage that's attached, and you can also use SMB 3.0 file shares as shared storage for servers that are running Hyper-V that are configured in a failover cluster. For more information, see Deploy Hyper-V over SMB.

  In most cases, attached storage should contain multiple, separate disks (logical unit numbers, or LUNs) that are configured at the hardware level. For some clusters, one disk functions as the disk witness (described at the end of this subsection). Other disks contain the files required for the clustered roles (formerly called clustered services or applications). Storage requirements include the following:

  - To use the native disk support included in Failover Clustering, use basic disks, not dynamic disks.
  - We recommend that you format the partitions with NTFS. If you use Cluster Shared Volumes (CSV), the partition for each of those must be NTFS.

    > **NOTE**
    > If you have a disk witness for your quorum configuration, you can format the disk with either NTFS or Resilient File System (ReFS).

  - For the partition style of the disk, you can use either master boot record (MBR) or GUID partition table (GPT).

    A disk witness is a disk in the cluster storage that's designated to hold a copy of the cluster configuration database. A failover cluster has a disk witness only if this is specified as part of the quorum configuration. For more information, see Understanding Quorum in Storage Spaces Direct.

Hardware requirements for Hyper-V

If you are creating a failover cluster that includes clustered virtual machines, the cluster servers must support the hardware requirements for the Hyper-V role. Hyper-V requires a 64-bit processor that includes the following:

- Hardware-assisted virtualization. This is available in processors that include a virtualization option—specifically processors with Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) technology.
- Hardware-enforced Data Execution Prevention (DEP) must be available and enabled. Specifically, you must enable Intel XD bit (execute disable bit) or AMD NX bit (no execute bit).

For more information about the Hyper-V role, see Hyper-V Overview.

Deploying storage area networks with failover clusters

When deploying a storage area network (SAN) with a failover cluster, follow these guidelines:

- **Confirm compatibility of the storage**: Confirm with manufacturers and vendors that the storage, including drivers, firmware, and software used for the storage, are compatible with failover clusters in the version of Windows Server that you are running.

- **Isolate storage devices, one cluster per device**: Servers from different clusters must not be able to access the same storage devices. In most cases, a LUN used for one set of cluster servers should be isolated from all other servers through LUN masking or zoning.

- **Consider using multipath I/O software or teamed network adapters**: In a highly available storage fabric, you can deploy failover clusters with multiple host bus adapters by using multipath I/O

software or network adapter teaming (also called load balancing and failover, or LBFO). This provides the highest level of redundancy and availability. For Windows Server 2012 R2 or Windows Server 2012, your multipath solution must be based on Microsoft Multipath I/O (MPIO). Your hardware vendor will typically supply an MPIO device-specific module (DSM) for your hardware, although Windows Server includes one or more DSMs as part of the operating system.

> **IMPORTANT**
>
> Host bus adapters and multipath I/O software can be very version sensitive. If you are implementing a multipath solution for your cluster, work closely with your hardware vendor to choose the correct adapters, firmware, and software for the version of Windows Server that you are running.

- **Consider using Storage Spaces**: If you plan to deploy serial attached SCSI (SAS) clustered storage that's configured using Storage Spaces, see Deploy Clustered Storage Spaces for the requirements.

More information

- Failover Clustering
- Storage Spaces
- Using Guest Clustering for High Availability

Use Cluster Shared Volumes in a failover cluster

12/9/2022 • 21 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Azure Stack HCI, versions 21H2 and 20H2

Cluster Shared Volumes (CSV) enable multiple nodes in a Windows Server failover cluster or Azure Stack HCI to simultaneously have read-write access to the same LUN (disk) that is provisioned as an NTFS volume. The disk can be provisioned as Resilient File System (ReFS); however, the CSV drive will be in redirected mode meaning write access will be sent to the coordinator node. For more information, see About I/O synchronization and I/O redirection in CSV communication later in this document. With CSV, clustered roles can fail over quickly from one node to another node without requiring a change in drive ownership, or dismounting and remounting a volume. CSV also help simplify the management of a potentially large number of LUNs in a failover cluster.

CSV provides a general-purpose, clustered file system which is layered above NTFS or ReFS. CSV applications include:

- Clustered virtual hard disk (VHD/VHDX) files for clustered Hyper-V virtual machines
- Scale-out file shares to store application data for the Scale-Out File Server clustered role. Examples of the application data for this role include Hyper-V virtual machine files and Microsoft SQL Server data. Be aware that ReFS is not supported for a Scale-Out File Server in Windows Server 2012 R2 and below. For more information about Scale-Out File Server, see Scale-Out File Server for Application Data.
- Microsoft SQL Server 2014 (or higher) Failover Cluster Instance (FCI). Microsoft SQL Server clustered workload in SQL Server 2012 and earlier versions of SQL Server do not support the use of CSV.
- Windows Server 2019 or higher Microsoft Distributed Transaction Control (MSDTC)

> **NOTE**
>
> CSVs don't support the Microsoft SQL Server clustered workload in SQL Server 2012 and earlier versions of SQL Server.

In Windows Server 2012, CSV functionality was significantly enhanced. For example, dependencies on Active Directory Domain Services were removed. Support was added for the functional improvements in **chkdsk**, for interoperability with antivirus and backup applications, and for integration with general storage features such as BitLocker-encrypted volumes and Storage Spaces. For an overview of CSV functionality that was introduced in Windows Server 2012, see What's New in Failover Clustering in Windows Server 2012 [redirected].

Windows Server 2012 R2 introduces additional functionality, such as distributed CSV ownership, increased resiliency through availability of the Server service, greater flexibility in the amount of physical memory that you can allocate to CSV cache, better diagnosability, and enhanced interoperability that includes support for ReFS and deduplication. For more information, see What's New in Failover Clustering.

> **NOTE**
>
> For information about using data deduplication on CSV for Virtual Desktop Infrastructure (VDI) scenarios, see the blog posts Deploying Data Deduplication for VDI storage in Windows Server 2012 R2 and Extending Data Deduplication to new workloads in Windows Server 2012 R2.

Review requirements and considerations for using CSV in a failover

cluster

Before using CSV in a failover cluster, review the network, storage, and other requirements and considerations in this section.

Network configuration considerations

Consider the following when you configure the networks that support CSV.

- **Multiple networks and multiple network adapters**. To enable fault tolerance in the event of a network failure, we recommend that multiple cluster networks carry CSV traffic or that you configure teamed network adapters.

  If the cluster nodes are connected to networks that should not be used by the cluster, you should disable them. For example, we recommend that you disable iSCSI networks for cluster use to prevent CSV traffic on those networks. To disable a network, in Failover Cluster Manager, select **Networks**, select the network, select the **Properties** action, and then select **Do not allow cluster network communication on this network**. Alternatively, you can configure the **Role** property of the network by using the Get-ClusterNetwork Windows PowerShell cmdlet.

- **Network adapter properties**. In the properties for all adapters that carry cluster communication, make sure that the following settings are enabled:

  - **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks**. These settings support Server Message Block (SMB) 3.0, which is used by default to carry CSV traffic between nodes. To enable SMB, also ensure that the Server service and the Workstation service are running and that they are configured to start automatically on each cluster node.

    > **NOTE**
    >
    > In Windows Server 2012 R2 and later, there are multiple Server service instances per failover cluster node. There is the default instance that handles incoming traffic from SMB clients that access regular file shares, and a second CSV instance that handles only inter-node CSV traffic. Also, if the Server service on a node becomes unhealthy, CSV ownership automatically transitions to another node.

    SMB 3.0 includes the SMB Multichannel and SMB Direct features, which enable CSV traffic to stream across multiple networks in the cluster and to leverage network adapters that support Remote Direct Memory Access (RDMA). By default, SMB Multichannel is used for CSV traffic. For more information, see Server Message Block overview.

  - **Microsoft Failover Cluster Virtual Adapter Performance Filter**. This setting improves the ability of nodes to perform I/O redirection when it is required to reach CSV, for example, when a connectivity failure prevents a node from connecting directly to the CSV disk. The NetFT Virtual Adapter Performance Filter is disabled by default in all versions except Windows Server 2012 R2. The filter is disabled because it can cause issues with Hyper-V clusters which have a Guest Cluster running in VMs running on top of them. Issues have been seen where the NetFT Virtual Adapter Performance Filter in the host incorrectly routes NetFT traffic bound for a guest VM to the host. This can result in communication issues with the guest cluster in the VM. If you are deploying any workload **other** than Hyper-V with guest clusters, enabling the NetFT Virtual Adapter Performance Filter will optimize and improve cluster performance. For more information, see About I/O synchronization and I/O redirection in CSV communication later in this topic.

- **Cluster network prioritization**. We generally recommend that you do not change the cluster-configured preferences for the networks.

- **IP subnet configuration**. No specific subnet configuration is required for nodes in a network that use

CSV. CSV can support multi-subnet stretch clusters.

- **Policy-based Quality of Service (QoS)**. We recommend that you configure a QoS priority policy and a minimum bandwidth policy for network traffic to each node when you use CSV. For more information, see Quality of Service (QoS).

- **Storage network**. For storage network recommendations, review the guidelines that are provided by your storage vendor. For additional considerations about storage for CSV, see Storage and disk configuration requirements later in this topic.

For an overview of the hardware, network, and storage requirements for failover clusters, see Failover Clustering Hardware Requirements and Storage Options.

About I/O synchronization and I/O redirection in CSV communication

- **I/O synchronization**: CSV enables multiple nodes to have simultaneous read-write access to the same shared storage. When a node performs disk input/output (I/O) on a CSV volume, the node communicates directly with the storage, for example, through a storage area network (SAN). However, at any time, a single node (called the coordinator node) "owns" the physical disk resource that is associated with the LUN. The coordinator node for a CSV volume is displayed in Failover Cluster Manager as **Owner Node** under **Disks**. It also appears in the output of the Get-ClusterSharedVolume Windows PowerShell cmdlet.

  > **NOTE**
  >
  > Starting in Windows Server 2012 R2, CSV ownership is evenly distributed across the failover cluster nodes based on the number of CSV volumes that each node owns. Additionally, ownership is automatically rebalanced when there are conditions such as CSV failover, a node rejoins the cluster, you add a new node to the cluster, you restart a cluster node, or you start the failover cluster after it has been shut down.

  When certain small changes occur in the file system on a CSV volume, this metadata must be synchronized on each of the physical nodes that access the LUN, not only on the single coordinator node. For example, when a virtual machine on a CSV volume is started, created, or deleted, or when a virtual machine is migrated, this information needs to be synchronized on each of the physical nodes that access the virtual machine. These metadata update operations occur in parallel across the cluster networks by using SMB 3.0. These operations do not require all the physical nodes to communicate with the shared storage.

- **I/O redirection**: Storage connectivity failures and certain storage operations can prevent a given node from communicating directly with the storage. To maintain function while the node is not communicating with the storage, the node redirects the disk I/O through a cluster network to the coordinator node where the disk is currently mounted. If the current coordinator node experiences a storage connectivity failure, all disk I/O operations are queued temporarily while a new node is established as a coordinator node.

The server uses one of the following I/O redirection modes, depending on the situation:

- **File system redirection** Redirection is per volume—for example, when CSV snapshots are taken by a backup application when a CSV volume is manually placed in redirected I/O mode.
- **Block redirection** Redirection is at the file-block level—for example, when storage connectivity is lost to a volume. Block redirection is significantly faster than file system redirection.

In Windows Server 2012 R2 and higher, you can view the state of a CSV volume on a per node basis. For example, you can see whether I/O is direct or redirected, or whether the CSV volume is unavailable. If a CSV volume is in I/O redirected mode, you can also view the reason. Use the Windows PowerShell cmdlet Get-ClusterSharedVolumeState to view this information.

> **IMPORTANT**
>
> - Please note that CSVs pre-formatted with **ReFS used on top of SANs will NOT use Direct I/O**, regardless of all other requirements for Direct I/O being met.
> - If you plan to use CSV in junction with SAN(-FrontEnd) attached disks, format drives with NTFS before converting them to a CSV to leverage the performance benefits of Direct I/O.
> - This behavior is by design. Please consult the pages linked in the section **More information** below.

- Because of the integration of CSV with SMB 3.0 features such as SMB Multichannel and SMB Direct, redirected I/O traffic can stream across multiple cluster networks.
- You should plan your cluster networks to allow for the potential increase in network traffic to the coordinator node during I/O redirection.

> **NOTE**
>
> - In Windows Server 2012, because of improvements in CSV design, CSV performs more operations in direct I/O mode than occurred in Windows Server 2008 R2.
> - Because of the integration of CSV with SMB 3.0 features such as SMB Multichannel and SMB Direct, redirected I/O traffic can stream across multiple cluster networks.
> - You should plan your cluster networks to allow for the potential increase in network traffic to the coordinator node during I/O redirection.

Storage and disk configuration requirements

To use CSV, your storage and disks must meet the following requirements:

- **File system format**. In Windows Server 2012, a disk or storage space for a CSV volume must be a basic disk that is partitioned with NTFS. In Windows Server 2012 R2, a disk or storage space for a CSV volume must be a basic disk that is partitioned with NTFS or ReFS. In Windows Server 2016 or higher and Azure Stack HCI, a disk or storage space for a CSV volume must be either a basic disk or GUID Partition Table (GPT) disk that is partitioned with NTFS or ReFS.

  A CSV has the following additional requirements:

  - In Windows Server 2012, you cannot use a disk for a CSV that is formatted with FAT, FAT32, or ReFS.
  - In Windows Server 2012 R2 and higher, you cannot use a disk for a CSV that is formatted with FAT or FAT32.
  - A CSV cannot be used as a quorum witness disk. For more information about the cluster quorum, see Understanding Quorum in Storage Spaces Direct.
  - After you add a disk as a CSV, it is designated in the CSVFS format (for CSV File System). This allows the cluster and other software to differentiate the CSV storage from other NTFS or ReFS storage. Generally, CSVFS supports the same functionality as NTFS or ReFS. However, certain features are not supported. For example, in Windows Server 2012 R2, you cannot enable compression on CSV. In Windows Server 2012, you cannot enable data deduplication or compression on CSV.
- **Resource type in the cluster**. For a CSV volume, you must use the Physical Disk resource type. By default, a disk or storage space that is added to cluster storage is automatically configured in this way.
- **Choice of CSV disks or other disks in cluster storage**. When choosing one or more disks for a clustered virtual machine, consider how each disk will be used. If a disk will be used to store files that are created by Hyper-V, such as VHD/VHDX files or configuration files, you can choose from the CSV disks or the other available disks in cluster storage. If a disk will be a physical disk that is directly attached to the virtual machine (also called a pass-through disk), you cannot choose a CSV disk, and you must choose from the other available disks in cluster storage.

- **Path name for identifying disks**. Disks in CSV are identified with a path name. Each path appears to be on the system drive of the node as a numbered volume under the **\ClusterStorage** folder. This path is the same when viewed from any node in the cluster. You can rename the volumes if needed but is recommended done before any virtual machine (if Hyper-V) or application such as SQL Server is installed. CSV cannot be renamed if there are any open handles (i.e. a virtual machine that is turned on or in a saved state).

For storage requirements for CSV, review the guidelines that are provided by your storage vendor. For additional storage planning considerations for CSV, see Plan to use CSV in a failover cluster later in this topic.

Node requirements

To use CSV, your nodes must meet the following requirements:

- **Drive letter of system disk**. On all nodes, the drive letter for the system disk must be the same.
- **Authentication protocol**. The NTLM protocol must be enabled on all nodes. This is enabled by default. Starting in Windows Server 2019 and Azure Stack HCI, NTLM dependencies have been removed as it uses certificates for authentication.

Plan to use CSV in a failover cluster

This section lists planning considerations and recommendations for using CSV in a failover cluster.

> **IMPORTANT**
>
> Ask your storage vendor for recommendations about how to configure your specific storage unit for CSV. If the recommendations from the storage vendor differ from information in this topic, use the recommendations from the storage vendor.

Arrangement of LUNs, volumes, and VHD files

To make the best use of CSV to provide storage for clustered virtual machines, it is helpful to review how you would arrange the LUNs (disks) when you configure physical servers. When you configure the corresponding virtual machines, try to arrange the VHD files in a similar way.

Consider a physical server for which you would organize the disks and files as follows:

- System files, including a page file, on one physical disk
- Data files on another physical disk

For an equivalent clustered virtual machine, you should organize the volumes and files in a similar way:

- System files, including a page file, in a VHD file on one CSV
- Data files in a VHD file on another CSV

If you add another virtual machine, where possible, you should keep the same arrangement for the VHDs on that virtual machine.

Number and size of LUNs and volumes

When you plan the storage configuration for a failover cluster that uses CSV, consider the following recommendations:

- To decide how many LUNs to configure, consult your storage vendor. For example, your storage vendor may recommend that you configure each LUN with one partition and place one CSV volume on it.

- Create at least one CSV per node.

- There are no limitations for the number of virtual machines that can be supported on a single CSV

volume. However, you should consider the number of virtual machines that you plan to have in the cluster and the workload (I/O operations per second) for each virtual machine. Consider the following examples:

  - One organization is deploying virtual machines that will support a virtual desktop infrastructure (VDI), which is a relatively light workload. The cluster uses high-performance storage. The cluster administrator, after consulting with the storage vendor, decides to place a relatively large number of virtual machines per CSV volume.
  - Another organization is deploying a large number of virtual machines that will support a heavily used database application, which is a heavier workload. The cluster uses lower-performing storage. The cluster administrator, after consulting with the storage vendor, decides to place a relatively small number of virtual machines per CSV volume.

- When you plan the storage configuration for a particular virtual machine, consider the disk requirements of the service, application, or role that the virtual machine will support. Understanding these requirements helps you avoid disk contention that can result in poor performance. The storage configuration for the virtual machine should closely resemble the storage configuration that you would use for a physical server that is running the same service, application, or role. For more information, see Arrangement of LUNs, volumes, and VHD files earlier in this topic.

  You can also mitigate disk contention by having storage with a large number of independent physical hard disks. Choose your storage hardware accordingly, and consult with your vendor to optimize the performance of your storage.

- Depending on your cluster workloads and their need for I/O operations, you can consider configuring only a percentage of the virtual machines to access each LUN, while other virtual machines do not have connectivity and are instead dedicated to compute operations.

Add a disk to CSV on a failover cluster

The CSV feature is enabled by default in Failover Clustering. To add a disk to CSV, you must add a disk to the **Available Storage** group of the cluster (if it is not already added), and then add the disk to CSV on the cluster. You can use Failover Cluster Manager or the Failover Clusters Windows PowerShell cmdlets to perform these procedures.

Add a disk to Available Storage

1. In Failover Cluster Manager, in the console tree, expand the name of the cluster, and then expand **Storage**.

2. Right-click **Disks**, and then select **Add Disk**. A list appears showing the disks that can be added for use in a failover cluster.

3. Select the disk or disks you want to add, and then select **OK**.

   The disks are now assigned to the **Available Storage** group.

Windows PowerShell equivalent commands (add a disk to Available Storage)

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

The following example identifies the disks that are ready to be added to the cluster, and then adds them to the **Available Storage** group.

```
Get-ClusterAvailableDisk | Add-ClusterDisk
```

Add a disk in Available Storage to CSV

1. In Failover Cluster Manager, in the console tree, expand the name of the cluster, expand **Storage**, and then select **Disks**.

2. Select one or more disks that are assigned to **Available Storage**, right-click the selection, and then select **Add to Cluster Shared Volumes**.

   The disks are now assigned to the **Cluster Shared Volume** group in the cluster. The disks are exposed to each cluster node as numbered volumes (mount points) under the %SystemDrive%ClusterStorage folder. The volumes appear in the CSVFS file system.

> **NOTE**
>
> You can rename CSV volumes in the %SystemDrive%ClusterStorage folder.

Windows PowerShell equivalent commands (add a disk to CSV)

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

The following example adds *Cluster Disk 1* in **Available Storage** to CSV on the local cluster.

```
Add-ClusterSharedVolume –Name "Cluster Disk 1"
```

Enable the CSV cache for read-intensive workloads (optional)

The CSV cache provides caching at the block level of read-only unbuffered I/O operations by allocating system memory (RAM) as a write-through cache. (Unbuffered I/O operations are not cached by the cache manager.) This can improve performance for applications such as Hyper-V, which conducts unbuffered I/O operations when accessing a VHD. The CSV cache can boost the performance of read requests without caching write requests. Enabling the CSV cache is also useful for Scale-Out File Server scenarios.

> **NOTE**
>
> We recommend that you enable the CSV cache for all clustered Hyper-V and Scale-Out File Server deployments.

In Windows Server 2019, the CSV cache is on by default with 1 gibibyte (GiB) allocated. In Windows Server 2016 and Windows Server 2012, it's off by default. In Windows Server 2012 R2, the CSV cache is enabled by default; however, you must still allocate the size of the block cache to reserve.

The following table describes the two configuration settings that control the CSV cache.

WINDOWS SERVER 2012 R2 AND LATER	WINDOWS SERVER 2012	DESCRIPTION
BlockCacheSize	SharedVolumeBlockCacheSizeInMB	This is a cluster common property that allows you to define how much memory (in megabytes) to reserve for the CSV cache on each node in the cluster. For example, if a value of 512 is defined, then 512 MB of system memory is reserved on each node. (In many clusters, 512 MB is a recommended value.) The default setting is 0 (for disabled).

WINDOWS SERVER 2012 R2 AND LATER	WINDOWS SERVER 2012	DESCRIPTION
EnableBlockCache	CsvEnableBlockCache	This is a private property of the cluster Physical Disk resource. It allows you to enable CSV cache on an individual disk that is added to CSV. In Windows Server 2012, the default setting is 0 (for disabled). To enable CSV cache on a disk, configure a value of 1. By default, in Windows Server 2012 R2, this setting is enabled.

You can monitor the CSV cache in Performance Monitor by adding the counters under **Cluster CSV Volume Cache**.

Configure the CSV cache

1. Start Windows PowerShell as an administrator.
2. To define a cache of *512* MB to be reserved on each node, type the following:
   - For Windows Server 2012 R2 and later:

     ```
     (Get-Cluster).BlockCacheSize = 512
     ```

   - For Windows Server 2012:

     ```
     (Get-Cluster).SharedVolumeBlockCacheSizeInMB = 512
     ```

3. In Windows Server 2012, to enable the CSV cache on a CSV named *Cluster Disk 1*, enter the following:

   ```
   Get-ClusterSharedVolume "Cluster Disk 1" | Set-ClusterParameter CsvEnableBlockCache 1
   ```

NOTE

- In Windows Server 2012, you can allocate only 20% of the total physical RAM to the CSV cache. In Windows Server 2012 R2 and later, you can allocate up to 80%. Because Scale-Out File Servers are not typically memory constrained, you can accomplish large performance gains by using the extra memory for the CSV cache.
- To avoid resource contention, you should restart each node in the cluster after you modify the memory that is allocated to the CSV cache. In Windows Server 2012 R2 and later, a restart is no longer required.
- After you enable or disable CSV cache on an individual disk, for the setting to take effect, you must take the Physical Disk resource offline and bring it back online. (By default, in Windows Server 2012 R2 and later, the CSV cache is enabled.)
- For more information about CSV cache that includes information about performance counters, see the blog post How to Enable CSV Cache.

Backing up CSVs

There are multiple methods to back up information that is stored on CSVs in a failover cluster. You can use a Microsoft backup application or a non-Microsoft application. In general, CSV do not impose special backup requirements beyond those for clustered storage formatted with NTFS or ReFS. CSV backups also do not disrupt other CSV storage operations.

You should consider the following factors when you select a backup application and backup schedule for CSV:

- Volume-level backup of a CSV volume can be run from any node that connects to the CSV volume.
- Your backup application can use software snapshots or hardware snapshots. Depending on the ability of your backup application to support them, backups can use application-consistent and crash-consistent Volume Shadow Copy Service (VSS) snapshots.
- If you are backing up CSV that have multiple running virtual machines, you should generally choose a management operating system-based backup method. If your backup application supports it, multiple virtual machines can be backed up simultaneously.
- CSV support backup requestors running Windows Server Backup. However, Windows Server Backup generally provides only a basic backup solution that may not be suited for organizations with larger clusters. Windows Server Backup does not support application-consistent virtual machine backup on CSV. It supports crash-consistent volume-level backup only. (If you restore a crash-consistent backup, the virtual machine will be in the same state it was if the virtual machine had crashed at the exact moment that the backup was taken.) A backup of a virtual machine on a CSV volume will succeed, but an error event will be logged indicating that this is not supported.
- You may require administrative credentials when backing up a failover cluster.

> **IMPORTANT**
>
> Be sure to carefully review what data your backup application backs up and restores, which CSV features it supports, and the resource requirements for the application on each cluster node.

> **WARNING**
>
> If you need to restore the backup data onto a CSV volume, be aware of the capabilities and limitations of the backup application to maintain and restore application-consistent data across the cluster nodes. For example, with some applications, if the CSV is restored on a node that is different from the node where the CSV volume was backed up, you might inadvertently overwrite important data about the application state on the node where the restore is taking place.

More information

- Failover Clustering
- Deploy Clustered Storage Spaces
- Understanding the state of your Cluster Shared Volumes
- Cluster Shared Volume Diagnostics

Using Storage Spaces Direct in guest virtual machine clusters

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, versions 21H2 and 20H2

You can deploy Storage Spaces Direct on a cluster of physical servers or on virtual machine (VM) guest clusters as discussed in this topic. This type of deployment delivers virtual shared storage across a set of VMs on top of a private or public cloud. This allows you to use application high availability solutions.

To instead use Azure Shared Disks for guest virtual machines, see Azure Shared Disks.

Deploying in Azure Iaas VM guest clusters

Azure templates have been published to decrease complexity, configure best practices, and speed your Storage Spaces Direct deployments in an Azure Iaas VM. This is the recommended solution for deploying in Azure.

Requirements for guest clusters

The following considerations apply when deploying Storage Spaces Direct in a virtualized environment.

> **TIP**
> Azure templates will automatically configure the following considerations for you and they are the recommended solution when deploying in Azure IaaS VMs.

- Minimum of two nodes and maximum of three nodes
- Two-node deployments must configure a witness (Cloud Witness or File Share Witness)
- Three-node deployments can tolerate one node down and the loss of one or more disks on another node. If two nodes shut down, then the virtual disks will be offline until one of the nodes returns.
- Configure the VMs to be deployed across fault domains
  - Azure – Configure the Availability Set

  - Hyper-V – Configure AntiAffinityClassNames on the VMs to separate the VMs across nodes
  - VMware – Configure the VM-VM Anti-Affinity rule by creating a DRS Rule of type "Separate Virtual Machines" to separate the VMs across ESX hosts. Disks presented for use with Storage Spaces Direct should use the Paravirtual SCSI (PVSCSI) adapter. For PVSCSI support with Windows Server, consult https://kb.vmware.com/s/article/1010398.

- Use low latency / high performance storage such as Azure Premium SSD managed disks or faster
- Deploy a flat storage design with no caching devices configured
- Use a minimum of two virtual data disks presented to each VM (VHD / VHDX / VMDK)

  This number is different than bare-metal deployments because the virtual disks can be implemented as files that aren't susceptible to physical failures.

- Disable the automatic drive replacement capabilities in the Health Service by running the following PowerShell cmdlet:

  ```
  Get-storagesubsystem clus* | set-storagehealthsetting -name
  "System.Storage.PhysicalDisk.AutoReplace.Enabled" -value "False"
  ```

- To give greater resiliency to possible VHD / VHDX / VMDK storage latency in guest clusters, increase the Storage Spaces I/O timeout value:

  `HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\spaceport\\Parameters\\HwTimeout`

  `dword: 00007530`

  The decimal equivalent of Hexadecimal 7530 is 30000, which is 30 seconds. The default value is 1770 Hexadecimal, or 6000 Decimal, which is 6 seconds.

Not supported

- Host level virtual disk snapshot/restore

  Instead use traditional guest level backup solutions to back up and restore the data on the Storage Spaces Direct volumes.

- Host level virtual disk size change

  The virtual disks exposed through the VM must retain the same size and characteristics. Adding more capacity to the storage pool can be accomplished by adding more virtual disks to each of the VMs, and then adding them to the pool. It's highly recommended to use virtual disks of the same size and characteristics as the current virtual disks.

More references

- Additional Azure Iaas VM templates for deploying Storage Spaces Direct, videos, and step-by-step guides.
- Additional Storage Spaces Direct Overview

Create a failover cluster

12/9/2022 • 13 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This topic shows how to create a failover cluster by using either the Failover Cluster Manager snap-in or Windows PowerShell. The topic covers a typical deployment, where computer objects for the cluster and its associated clustered roles are created in Active Directory Domain Services (AD DS). If you're deploying a Storage Spaces Direct cluster, instead see Deploy Storage Spaces Direct. For information about using a failover cluster in Azure Stack HCI, see Create an Azure Stack HCI.

You can also deploy an Active Directory-detached cluster. This deployment method enables you to create a failover cluster without permissions to create computer objects in AD DS or the need to request that computer objects are prestaged in AD DS. This option is only available through Windows PowerShell, and is only recommended for specific scenarios. For more information, see Deploy an Active Directory-Detached Cluster.

Checklist: Create a failover cluster

STATUS	TASK	REFERENCE
☐	Verify the prerequisites	Verify the prerequisites
☐	Install the Failover Clustering feature on every server that you want to add as a cluster node	Install the Failover Clustering feature
☐	Run the Cluster Validation Wizard to validate the configuration	Validate the configuration
☐	Run the Create Cluster Wizard to create the failover cluster	Create the failover cluster
☐	Create clustered roles to host cluster workloads	Create clustered roles

Verify the prerequisites

Before you begin, verify the following prerequisites:

- Make sure that all servers that you want to add as cluster nodes are running the same version of Windows Server.
- Review the hardware requirements to make sure that your configuration is supported. For more information, see Failover Clustering Hardware Requirements and Storage Options. If you're creating a Storage Spaces Direct cluster, see Storage Spaces Direct hardware requirements.
- To add clustered storage during cluster creation, make sure that all servers can access the storage. (You can also add clustered storage after you create the cluster.)
- Make sure that all servers that you want to add as cluster nodes are joined to the same Active Directory domain.
- (Optional) Create an organizational unit (OU) and move the computer accounts for the servers that you want

to add as cluster nodes into the OU. As a best practice, we recommend that you place failover clusters in their own OU in AD DS. This can help you better control which Group Policy settings or security template settings affect the cluster nodes. By isolating clusters in their own OU, it also helps prevent against accidental deletion of cluster computer objects.

Additionally, verify the following account requirements:

- Make sure that the account you want to use to create the cluster is a domain user who has administrator rights on all servers that you want to add as cluster nodes.
- Make sure that either of the following is true:
  - The user who creates the cluster has the **Create Computer objects** permission to the OU or the container where the servers that will form the cluster reside.
  - If the user does not have the **Create Computer objects** permission, ask a domain administrator to prestage a cluster computer object for the cluster. For more information, see Prestage Cluster Computer Objects in Active Directory Domain Services.

> **NOTE**
> This requirement does not apply if you want to create an Active Directory-detached cluster in Windows Server 2012 R2. For more information, see Deploy an Active Directory-Detached Cluster.

Install the Failover Clustering feature

You must install the Failover Clustering feature on every server that you want to add as a failover cluster node.

Install the Failover Clustering feature

1. Start Server Manager.
2. On the **Manage** menu, select **Add Roles and Features**.
3. On the **Before you begin** page, select **Next**.
4. On the **Select installation type** page, select **Role-based or feature-based installation**, and then select **Next**.
5. On the **Select destination server** page, select the server where you want to install the feature, and then select **Next**.
6. On the **Select server roles** page, select **Next**.
7. On the **Select features** page, select the **Failover Clustering** check box.
8. To install the failover cluster management tools, select **Add Features**, and then select **Next**.
9. On the **Confirm installation selections** page, select **Install**.
   A server restart is not required for the Failover Clustering feature.
10. When the installation is completed, select **Close**.
11. Repeat this procedure on every server that you want to add as a failover cluster node.

> **NOTE**
> After you install the Failover Clustering feature, we recommend that you apply the latest updates from Windows Update. Also, for a Windows Server 2012-based failover cluster, review the Recommended hotfixes and updates for Windows Server 2012-based failover clusters Microsoft Support article and install any updates that apply.

Validate the configuration

Before you create the failover cluster, we strongly recommend that you validate the configuration to make sure that the hardware and hardware settings are compatible with failover clustering. Microsoft supports a cluster solution only if the complete configuration passes all validation tests and if all hardware is certified for the version of Windows Server that the cluster nodes are running.

> **NOTE**
> You must have at least two nodes to run all tests. If you have only one node, many of the critical storage tests do not run.

Run cluster validation tests

1. On a computer that has the Failover Cluster Management Tools installed from the Remote Server Administration Tools, or on a server where you installed the Failover Clustering feature, start Failover Cluster Manager. To do this on a server, start Server Manager, and then on the **Tools** menu, select **Failover Cluster Manager**.
2. In the **Failover Cluster Manager** pane, under **Management**, select **Validate Configuration**.
3. On the **Before You Begin** page, select **Next**.
4. On the **Select Servers or a Cluster** page, in the **Enter name** box, enter the NetBIOS name or the fully qualified domain name of a server that you plan to add as a failover cluster node, and then select **Add**. Repeat this step for each server that you want to add. To add multiple servers at the same time, separate the names by a comma or by a semicolon. For example, enter the names in the format `server1.contoso.com, server2.contoso.com`. When you are finished, select **Next**.
5. On the **Testing Options** page, select **Run all tests (recommended)**, and then select **Next**.
6. On the **Confirmation** page, select **Next**.

   The Validating page displays the status of the running tests.
7. On the **Summary** page, do either of the following:
   - If the results indicate that the tests completed successfully and the configuration is suited for clustering, and you want to create the cluster immediately, make sure that the **Create the cluster now using the validated nodes** check box is selected, and then select **Finish**. Then, continue to step 4 of the Create the failover cluster procedure.
   - If the results indicate that there were warnings or failures, select **View Report** to view the details and determine which issues must be corrected. Realize that a warning for a particular validation test indicates that this aspect of the failover cluster can be supported, but might not meet the recommended best practices.

     > **NOTE**
     > If you receive a warning for the Validate Storage Spaces Persistent Reservation test, see the blog post Windows Failover Cluster validation warning indicates your disks don't support the persistent reservations for Storage Spaces for more information.

For more information about hardware validation tests, see Validate Hardware for a Failover Cluster.

Create the failover cluster

To complete this step, make sure that the user account that you log on as meets the requirements that are

outlined in the Verify the prerequisites section of this topic.

1. Start Server Manager.
2. On the **Tools** menu, select **Failover Cluster Manager**.
3. In the **Failover Cluster Manager** pane, under **Management**, select **Create Cluster**.

   The Create Cluster Wizard opens.
4. On the **Before You Begin** page, select **Next**.
5. If the **Select Servers** page appears, in the **Enter name** box, enter the NetBIOS name or the fully qualified domain name of a server that you plan to add as a failover cluster node, and then select **Add**. Repeat this step for each server that you want to add. To add multiple servers at the same time, separate the names by a comma or a semicolon. For example, enter the names in the format *server1.contoso.com; server2.contoso.com*. When you are finished, select **Next**.

   > **NOTE**
   > If you chose to create the cluster immediately after running validation in the configuration validating procedure, you will not see the **Select Servers** page. The nodes that were validated are automatically added to the Create Cluster Wizard so that you do not have to enter them again.

6. If you skipped validation earlier, the **Validation Warning** page appears. We strongly recommend that you run cluster validation. Only clusters that pass all validation tests are supported by Microsoft. To run the validation tests, select **Yes**, and then select **Next**. Complete the Validate a Configuration Wizard as described in Validate the configuration.
7. On the **Access Point for Administering the Cluster** page, do the following:

   a. In the **Cluster Name** box, enter the name that you want to use to administer the cluster. Before you do, review the following information:

      - During cluster creation, this name is registered as the cluster computer object (also known as the *cluster name object* or *CNO*) in AD DS. If you specify a NetBIOS name for the cluster, the CNO is created in the same location where the computer objects for the cluster nodes reside. This can be either the default Computers container or an OU.
      - To specify a different location for the CNO, you can enter the distinguished name of an OU in the **Cluster Name** box. For example: *CN=ClusterName, OU=Clusters, DC=Contoso, DC=com*.
      - If a domain administrator has prestaged the CNO in a different OU than where the cluster nodes reside, specify the distinguished name that the domain administrator provides.

   b. If the server does not have a network adapter that is configured to use DHCP, you must configure one or more static IP addresses for the failover cluster. Select the check box next to each network that you want to use for cluster management. Select the **Address** field next to a selected network, and then enter the IP address that you want to assign to the cluster. This IP address (or addresses) will be associated with the cluster name in Domain Name System (DNS).

   > **NOTE**
   > If you're using Windows Server 2019, you have the option to use a distributed network name for the cluster. A distributed network name uses the IP addresses of the member servers instead of requiring a dedicated IP address for the cluster. By default, Windows uses a distributed network name if it detects that you're creating the cluster in Azure (so you don't have to create an internal load balancer for the cluster), or a normal static or IP address if you're running on-premises. For more info, see Distributed Network Name.

c. When you are finished, select **Next**.

8. On the **Confirmation** page, review the settings. By default, the **Add all eligible storage to the cluster** check box is selected. Clear this check box if you want to do either of the following:

   - You want to configure storage later.
   - You plan to create clustered storage spaces through Failover Cluster Manager or through the Failover Clustering Windows PowerShell cmdlets, and have not yet created storage spaces in File and Storage Services. For more information, see Deploy Clustered Storage Spaces.

9. Select **Next** to create the failover cluster.

10. On the **Summary** page, confirm that the failover cluster was successfully created. If there were any warnings or errors, view the summary output or select **View Report** to view the full report. Select **Finish**.

11. To confirm that the cluster was created, verify that the cluster name is listed under **Failover Cluster Manager** in the navigation tree. You can expand the cluster name, and then select items under **Nodes**, **Storage** or **Networks** to view the associated resources.

    Realize that it may take some time for the cluster name to successfully replicate in DNS. After successful DNS registration and replication, if you select **All Servers** in Server Manager, the cluster name should be listed as a server with a **Manageability** status of **Online**.

After the cluster is created, you can do things such as verify cluster quorum configuration, and optionally, create Cluster Shared Volumes (CSV). For more information, see Understanding Quorum in Storage Spaces Direct and Use Cluster Shared Volumes in a failover cluster.

Create clustered roles

After you create the failover cluster, you can create clustered roles to host cluster workloads.

> **NOTE**
>
> For clustered roles that require a client access point, a virtual computer object (VCO) is created in AD DS. By default, all VCOs for the cluster are created in the same container or OU as the CNO. Realize that after you create a cluster, you can move the CNO to any OU.

Here's how to create a clustered role:

1. Use Server Manager or Windows PowerShell to install the role or feature that is required for a clustered role on each failover cluster node. For example, if you want to create a clustered file server, install the File Server role on all cluster nodes.

   The following table shows the clustered roles that you can configure in the High Availability Wizard and the associated server role or feature that you must install as a prerequisite.

CLUSTERED ROLE	ROLE OR FEATURE PREREQUISITE
Namespace Server	Namespaces (part of File Server role)
DFS Namespace Server	DHCP Server role
Distributed Transaction Coordinator (DTC)	None
File Server	File Server role

CLUSTERED ROLE	ROLE OR FEATURE PREREQUISITE
Generic Application	Not applicable
Generic Script	Not applicable
Generic Service	Not applicable
Hyper-V Replica Broker	Hyper-V role
iSCSI Target Server	iSCSI Target Server (part of File Server role)
iSNS Server	iSNS Server Service feature
Message Queuing	Message Queuing Services feature
Other Server	None
Virtual Machine	Hyper-V role
WINS Server	WINS Server feature

2. In Failover Cluster Manager, expand the cluster name, right-click **Roles**, and then select **Configure Role**.
3. Follow the steps in the High Availability Wizard to create the clustered role.
4. To verify that the clustered role was created, in the **Roles** pane, make sure that the role has a status of **Running**. The Roles pane also indicates the owner node. To test failover, right-click the role, point to **Move**, and then select **Select Node**. In the **Move Clustered Role** dialog box, select the desired cluster node, and then select **OK**. In the **Owner Node** column, verify that the owner node changed.

Create a failover cluster by using Windows PowerShell

The following Windows PowerShell cmdlets perform the same functions as the preceding procedures in this topic. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines because of formatting constraints.

> **NOTE**
> You must use Windows PowerShell to create an Active Directory-detached cluster in Windows Server 2012 R2. For information about the syntax, see Deploy an Active Directory-Detached Cluster.

The following example installs the Failover Clustering feature.

```
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

The following example runs all cluster validation tests on computers that are named *Server1* and *Server2*.

```
Test-Cluster -Node Server1, Server2
```

> **NOTE**
> The **Test-Cluster** cmdlet outputs the results to a log file in the current working directory. For example: C:\Users<username>\AppData\Local\Temp.

The following example creates a failover cluster that is named *MyCluster* with nodes *Server1* and *Server2*, assigns the static IP address *192.168.1.12*, and adds all eligible storage to the failover cluster.

```
New-Cluster –Name MyCluster –Node Server1, Server2 –StaticAddress 192.168.1.12
```

The following example creates the same failover cluster as in the previous example, but it does not add eligible storage to the failover cluster.

```
New-Cluster –Name MyCluster –Node Server1, Server2 –StaticAddress 192.168.1.12 -NoStorage
```

The following example creates a cluster that is named *MyCluster* in the *Cluster* OU of the domain *Contoso.com*.

```
New-Cluster -Name CN=MyCluster,OU=Cluster,DC=Contoso,DC=com -Node Server1, Server2
```

For examples of how to add clustered roles, see topics such as Add-ClusterFileServerRole and Add-ClusterGenericApplicationRole.

After the AD Detached failover Cluster is created backup the certificate with private key exportable option. Open MMC ==>File ==>Add remove Snap in ==>Certificates==>Services Accounts==>Next==>Local Computer==>Cluster Service==>Certificates==>Clussvc\Personal==>Select Certificate right click==>export ==>Next==>Yes export the Private Key ==>PfX Format==>Choose Password or you can add group ==>Next==>Select path where you want to store certificate==>Next ==>Finish.

More information

- Failover Clustering
- Deploy a Hyper-V Cluster
- Scale-Out File Server for Application Data
- Deploy an Active Directory-Detached Cluster
- Using Guest Clustering for High Availability
- Cluster-Aware Updating
- New-Cluster
- Test-Cluster

Deploying a two-node clustered file server

12/9/2022 • 20 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service. For information about using a failover cluster in Azure Stack HCI, see Create an Azure Stack HCI cluster using Windows Admin Center.

This guide describes the steps for installing and configuring a general purpose file server failover cluster that has two nodes. By creating the configuration in this guide, you can learn about failover clusters and familiarize yourself with the Failover Cluster Management snap-in interface in Windows Server 2019 or Windows Server 2016.

Overview for a two-node file server cluster

Servers in a failover cluster can function in a variety of roles, including the roles of file server, Hyper-V server, or database server, and can provide high availability for a variety of other services and applications. This guide describes how to configure a two-node file server cluster.

A failover cluster usually includes a storage unit that is physically connected to all the servers in the cluster, although any given volume in the storage is only accessed by one server at a time. The following diagram shows a two-node failover cluster connected to a storage unit.

Storage volumes or logical unit numbers (LUNs) exposed to the nodes in a cluster must not be exposed to other servers, including servers in another cluster. The following diagram illustrates this.

Note that for the maximum availability of any server, it is important to follow best practices for server management—for example, carefully managing the physical environment of the servers, testing software changes before fully implementing them, and carefully keeping track of software updates and configuration changes on all clustered servers.

The following scenario describes how a file server failover cluster can be configured. The files being shared are on the cluster storage, and either clustered server can act as the file server that shares them.

Shared folders in a failover cluster

The following list describes shared folder configuration functionality that is integrated into failover clustering:

- Display is scoped to clustered shared folders only (no mixing with non-clustered shared folders): When a user views shared folders by specifying the path of a clustered file server, the display will include only the shared folders that are part of the specific file server role. It will exclude non-clustered shared folders and shares part of separate file server roles that happen to be on a node of the cluster.
- Access-based enumeration: You can use access-based enumeration to hide a specified folder from users' view. Instead of allowing users to see the folder but not access anything on it, you can choose to prevent them from seeing the folder at all. You can configure access-based enumeration for a clustered shared folder in the same way as for a non-clustered shared folder.
- Offline access: You can configure offline access (caching) for a clustered shared folder in the same way as for a nonclustered shared folder.
- Clustered disks are always recognized as part of the cluster: Whether you use the failover cluster interface, Windows Explorer, or the Share and Storage Management snap-in, Windows recognizes whether a disk has been designated as being in the cluster storage. If such a disk has already been configured in Failover Cluster Management as part of a clustered file server, you can then use any of the previously mentioned interfaces to create a share on the disk. If such a disk has not been configured as part of a clustered file server, you cannot mistakenly create a share on it. Instead, an error indicates that the disk must first be configured as part of a clustered file server before it can be shared.
- Integration of Services for Network File System: The File Server role in Windows Server includes the optional role service called Services for Network File System (NFS). By installing the role service and configuring shared folders with Services for NFS, you can create a clustered file server that supports UNIX-based clients.

Requirements for a two-node failover cluster

For a failover cluster in Windows Server 2016 or Windows Server 2019 to be considered an officially supported solution by Microsoft, the solution must meet the following criteria.

- All hardware and software components must meet the qualifications for the appropriate logo. For Windows Server 2016, this is the "Certified for Windows Server 2016" logo. For Windows Server 2019, this is the "Certified for Windows Server 2019" logo. For more information about what hardware and software systems have been certified, please visit the Microsoft Windows Server Catalog site.
- The fully configured solution (servers, network, and storage) must pass all tests in the validation wizard, which is part of the failover cluster snap-in.

The following will be needed for a two-node failover cluster.

- **Servers:** We recommend using matching computers with the same or similar components. The servers for a two-node failover cluster must run the same version of Windows Server. They should also have the same software updates (patches).
- **Network Adapters and cable:** The network hardware, like other components in the failover cluster solution, must be compatible with Windows Server 2016 or Windows Server 2019. If you use iSCSI, the network adapters must be dedicated to either network communication or iSCSI, not both. In the network infrastructure that connects your cluster nodes, avoid having single points of failure. There are multiple ways of accomplishing this. You can connect your cluster nodes by multiple, distinct networks. Alternatively, you can connect your cluster nodes with one network that is constructed with teamed network adapters, redundant switches, redundant routers, or similar hardware that removes single points of failure.

  > **NOTE**
  > If the cluster nodes are connected with a single network, the network will pass the redundancy requirement in the Validate a Configuration wizard. However, the report will include a warning that the network should not have a single point of failure.

- **Device Controllers or appropriate adapters for storage:**
  - **Serial Attached SCSI or Fibre Channel:** If you are using Serial Attached SCSI or Fibre Channel, in all clustered servers, all components of the storage stack should be identical. It is required that the multipath I/O (MPIO) software and Device Specific Module (DSM) software components be identical. It is recommended that the mass-storage device controllers—that is, the host bus adapter (HBA), HBA drivers, and HBA firmware—that are attached to cluster storage be identical. If you use dissimilar HBAs, you should verify with the storage vendor that you are following their supported or recommended configurations.
  - **iSCSI:** If you are using iSCSI, each clustered server must have one or more network adapters or host bus adapters that are dedicated to the ISCSI storage. The network you use for iSCSI cannot be used for network communication. In all clustered servers, the network adapters you use to connect to the iSCSI storage target should be identical, and we recommend that you use Gigabit Ethernet or higher.
- **Storage:** You must use shared storage that is certified for Windows Server 2016 or Windows Server 2019.

  For a two-node failover cluster, the storage should contain at least two separate volumes (LUNs) if using a witness disk for quorum. The witness disk is a disk in the cluster storage that is designated to hold a copy of the cluster configuration database. For this two-node cluster example, the quorum configuration will be Node and Disk Majority. Node and Disk Majority means that the nodes and the witness disk each contain copies of the cluster configuration, and the cluster has quorum as long as a majority (two out of

three) of these copies are available. The other volume (LUN) will contain the files that are being shared to users.

Storage requirements include the following:

- To use the native disk support included in failover clustering, use basic disks, not dynamic disks.
- We recommend that you format the partitions with NTFS (for the witness disk, the partition must be NTFS).
- For the partition style of the disk, you can use either master boot record (MBR) or GUID partition table (GPT).
- The storage must respond correctly to specific SCSI commands, the storage must follow the standard called SCSI Primary Commands-3 (SPC-3). In particular, the storage must support Persistent Reservations as specified in the SPC-3 standard.
- The miniport driver used for the storage must work with the Microsoft Storport storage driver.

Deploying storage area networks with failover clusters

When deploying a storage area network (SAN) with a failover cluster, the following guidelines should be observed.

- **Confirm certification of the storage:** Using the Windows Server Catalog site, confirm the vendor's storage, including drivers, firmware and software, is certified for Windows Server 2016 or Windows Server 2019.

- **Isolate storage devices, one cluster per device:** Servers from different clusters must not be able to access the same storage devices. In most cases, a LUN that is used for one set of cluster servers should be isolated from all other servers through LUN masking or zoning.

- **Consider using multipath I/O software:** In a highly available storage fabric, you can deploy failover clusters with multiple host bus adapters by using multipath I/O software. This provides the highest level of redundancy and availability. The multipath solution must be based on Microsoft Multipath I/O (MPIO). The storage hardware vendor may supply an MPIO device-specific module (DSM) for your hardware, although Windows Server 2016 and Windows Server 2019 include one or more DSMs as part of the operating system.

Network infrastructure and domain account requirements

You will need the following network infrastructure for a two-node failover cluster and an administrative account with the following domain permissions:

- **Network settings and IP addresses:** When you use identical network adapters for a network, also use identical communication settings on those adapters (for example, Speed, Duplex Mode, Flow Control, and Media Type). Also, compare the settings between the network adapter and the switch it connects to and make sure that no settings are in conflict.

  If you have private networks that are not routed to the rest of your network infrastructure, ensure that each of these private networks uses a unique subnet. This is necessary even if you give each network adapter a unique IP address. For example, if you have a cluster node in a central office that uses one physical network, and another node in a branch office that uses a separate physical network, do not specify 10.0.0.0/24 for both networks, even if you give each adapter a unique IP address.

  For more information about the network adapters, see Hardware requirements for a two-node failover cluster, earlier in this guide.

- **DNS:** The servers in the cluster must be using Domain Name System (DNS) for name resolution. The DNS dynamic update protocol can be used.

- **Domain role:** All servers in the cluster must be in the same Active Directory domain. As a best practice, all clustered servers should have the same domain role (either member server or domain controller). The recommended role is member server.
- **Domain controller:** We recommend that your clustered servers be member servers. If they are, you need an additional server that acts as the domain controller in the domain that contains your failover cluster.
- **Clients:** As needed for testing, you can connect one or more networked clients to the failover cluster that you create, and observe the effect on a client when you move or fail over the clustered file server from one cluster node to the other.
- **Account for administering the cluster:** When you first create a cluster or add servers to it, you must be logged on to the domain with an account that has administrator rights and permissions on all servers in that cluster. The account does not need to be a Domain Admins account, but can be a Domain Users account that is in the Administrators group on each clustered server. In addition, if the account is not a Domain Admins account, the account (or the group that the account is a member of) must be given the **Create Computer Objects** and **Read All Properties** permissions in the domain organizational unit (OU) that is will reside in.

Steps for installing a two-node file server cluster

You must complete the following steps to install a two-node file server failover cluster.

Step 1: Connect the cluster servers to the networks and storage

Step 2: Install the failover cluster feature

Step 3: Validate the cluster configuration

Step 4: Create the cluster

If you have already installed the cluster nodes and want to configure a file server failover cluster, see Steps for configuring a two-node file server cluster, later in this guide.

Step 1: Connect the cluster servers to the networks and storage

For a failover cluster network, avoid having single points of failure. There are multiple ways of accomplishing this. You can connect your cluster nodes by multiple, distinct networks. Alternatively, you can connect your cluster nodes with one network that is constructed with teamed network adapters, redundant switches, redundant routers, or similar hardware that removes single points of failure (If you use a network for iSCSI, you must create this network in addition to the other networks).

For a two-node file server cluster, when you connect the servers to the cluster storage, you must expose at least two volumes (LUNs). You can expose additional volumes as needed for thorough testing of your configuration. Do not expose the clustered volumes to servers that are not in the cluster.

To connect the cluster servers to the networks and storage

1. Review the details about networks in Hardware requirements for a two-node failover cluster and Network infrastructure and domain account requirements for a two-node failover cluster, earlier in this guide.
2. Connect and configure the networks that the servers in the cluster will use.
3. If your test configuration includes clients or a non-clustered domain controller, make sure that these computers can connect to the clustered servers through at least one network.
4. Follow the manufacturer's instructions for physically connecting the servers to the storage.
5. Ensure that the disks (LUNs) that you want to use in the cluster are exposed to the servers that you will

cluster (and only those servers). You can use any of the following interfaces to expose disks or LUNs:

- The interface provided by the manufacturer of the storage.
- If you are using iSCSI, an appropriate iSCSI interface.

6. If you have purchased software that controls the format or function of the disk, follow instructions from the vendor about how to use that software with Windows Server.
7. On one of the servers that you want to cluster, click Start, click Administrative Tools, click Computer Management, and then click Disk Management. (If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.) In Disk Management, confirm that the cluster disks are visible.
8. If you want to have a storage volume larger than 2 terabytes, and you are using the Windows interface to control the format of the disk, convert that disk to the partition style called GUID partition table (GPT). To do this, back up any data on the disk, delete all volumes on the disk and then, in Disk Management, right-click the disk (not a partition) and click Convert to GPT Disk. For volumes smaller than 2 terabytes, instead of using GPT, you can use the partition style called master boot record (MBR).
9. Check the format of any exposed volume or LUN. We recommend NTFS for the format (for the witness disk, you must use NTFS).

Step 2: Install the file server role and failover cluster feature

In this step, the file server role and failover cluster feature will be installed. Both servers must be running either Windows Server 2016 or Windows Server 2019.

Using Server Manager

1. Open **Server Manager** and under the **Manage** drop down, select **Add Roles and Features**.

2. If the **Before you begin** window opens, choose **Next**.
3. For the **Installation Type**, select **Role-based or feature-based installation** and **Next**.
4. Ensure **Select a server from the server pool** is selected, the name of the machine is highlighted, and **Next**.
5. For the Server Role, from the list of roles, open **File Services**, select **File Server**, and **Next**.

6. For the Features, from the list of features, select **Failover Clustering**. A popup dialog will show that lists the administration tools also being installed. Keep all the selected, choose **Add Features** and **Next**.

7. On the Confirmation page, select Install.

8. Once the installation completes, restart the computer.

9. Repeat the steps on the second machine.

Using PowerShell

1. Open an administrative PowerShell session by right-clicking the Start button and then selecting **Windows PowerShell (Admin)**.

2. To install the File Server Role, run the command:

```
Install-WindowsFeature -Name FS-FileServer
```

3. To install the Failover Clustering feature and its management tools, run the command:

```
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

4. Once they have completed, you can verify they are installed with the commands:

```
Get-WindowsFeature -Name FS-FileServer
Get-WindowsFeature -Name Failover-Clustering
```

5. Once verified they are installed, restart the machine with the command:

```
Restart-Computer
```

6. Repeat the steps on the second server.

Step 3: Validate the cluster configuration

Before creating a cluster, we strongly recommend that you validate your configuration. Validation helps you confirm that the configuration of your servers, network, and storage meets a set of specific requirements for failover clusters.

Using Failover Cluster Manager

1. From **Server Manager**, choose the **Tools** drop down and select **Failover Cluster Manager**.
2. In **Failover Cluster Manager**, go to the middle column under **Management** and choose **Validate Configuration**.
3. If the **Before you begin** window opens, choose **Next**.
4. In the **Select Servers or a Cluster** window, add in the names of the two machines that will be the nodes of the cluster. For example, if the names are NODE1 and NODE2, enter the name and select **Add**. You can also choose the **Browse** button to search Active Directory for the names. Once both are listed under **Selected Servers**, choose **Next**.
5. In the **Testing Options** window, select **Run all tests (recommended)**, and **Next**.
6. On the **Confirmation** page, it will give you the listing of all the tests it will check. Choose **Next** and the tests will begin.
7. Once completed, the **Summary** page appears after the tests run. To view Help topics that will help you interpret the results, click **More about cluster validation tests**.
8. While still on the Summary page, click View Report and read the test results. Make any necessary changes in the configuration and rerun the tests.
   To view the results of the tests after you close the wizard, see *SystemRoot\Cluster\Reports\Validation Report date and time.html*.
9. To view Help topics about cluster validation after you close the wizard, in Failover Cluster Management, click Help, click Help Topics, click the Contents tab, expand the contents for the failover cluster Help, and click Validating a Failover Cluster Configuration.

Using PowerShell

1. Open an administrative PowerShell session by right-clicking the Start button and then selecting **Windows PowerShell (Admin)**.
2. To validate the machines (for example, the machine names being NODE1 and NODE2) for Failover Clustering, run the command:

```
Test-Cluster -Node "NODE1","NODE2"
```

3. To view the results of the tests after you close the wizard, see the file specified (in

SystemRoot\Cluster\Reports), then make any necessary changes in the configuration and rerun the tests.

For more info, see Validating a Failover Cluster Configuration.

Step 4: Create the Cluster

The following will create a cluster out of the machines and configuration you have.

Using Failover Cluster Manager

1. From **Server Manager**, choose the **Tools** drop down and select **Failover Cluster Manager**.
2. In **Failover Cluster Manager**, go to the middle column under **Management** and choose **Create Cluster**.
3. If the **Before you begin** window opens, choose **Next**.
4. In the **Select Servers** window, add in the names of the two machines that will be the nodes of the cluster. For example, if the names are NODE1 and NODE2, enter the name and select **Add**. You can also choose the **Browse** button to search Active Directory for the names. Once both are listed under **Selected Servers**, choose **Next**.
5. In the **Access Point for Administering the Cluster** window, input the name of the cluster you will be using. Please note that this is not the name you will be using to connect to your file shares with. This is for simply administrating the cluster.

   > **NOTE**
   > If you are using static IP Addresses, you will need to select the network to use and input the IP Address it will use for the cluster name. If you are using DHCP for your IP Addresses, the IP Address will be configured automatically for you.

6. Choose **Next**.
7. On the **Confirmation** page, verify what you have configured and select **Next** to create the Cluster.
8. On the **Summary** page, it will give you the configuration it has created. You can select View Report to see the report of the creation.

Using PowerShell

1. Open an administrative PowerShell session by right-clicking the Start button and then selecting **Windows PowerShell (Admin)**.
2. Run the following command to create the cluster if you are using static IP Addresses. For example, the machine names are NODE1 and NODE2, the name of the cluster will be CLUSTER, and the IP Address will be 1.1.1.1.

   ```
   New-Cluster -Name CLUSTER -Node "NODE1","NODE2" -StaticAddress 1.1.1.1
   ```

3. Run the following command to create the cluster if you are using DHCP for IP Addresses. For example, the machine names are NODE1 and NODE2, and the name of the cluster will be CLUSTER.

   ```
   New-Cluster -Name CLUSTER -Node "NODE1","NODE2"
   ```

Steps for configuring a file server failover cluster

To configure a file server failover cluster, follow the below steps.

1. From **Server Manager**, choose the **Tools** drop down and select **Failover Cluster Manager**.

2. When Failover Cluster Manager opens, it should automatically bring in the name of the cluster you created. If it does not, go to the middle column under **Management** and choose **Connect to Cluster**. Input the name of the cluster you created and **OK**.

3. In the console tree, click the ">" sign next to the cluster that you created to expand the items underneath it.

4. Right mouse click on **Roles** and select **Configure Role**.

5. If the **Before you begin** window opens, choose **Next**.

6. In the list of roles, choose **File Server** and **Next**.

7. For the File Server Type, select **File Server for general use** and **Next**.
   For info about Scale-Out File Server, see Scale-Out File Server overview.

8. In the **Client Access Point** window, input the name of the file server you will be using. Please note that this is not the name of the cluster. This is for the file share connectivity. For example, if I want to connect to \SERVER, the name inputted would be SERVER.

   > **NOTE**
   >
   > If you are using static IP Addresses, you will need to select the network to use and input the IP Address it will use for the cluster name. If you are using DHCP for your IP Addresses, the IP Address will be configured automatically for you.

9. Choose **Next**.

10. In the **Select Storage** window, select the additional drive (not the witness) that will hold your shares, and click **Next**.

11. On the **Confirmation** page, verify your configuration and select **Next**.

12. On the **Summary** page, it will give you the configuration it has created. You can select View Report to see the report of the file server role creation.

> **NOTE**
> If the role does not add or start correctly, the CNO (Cluster Name Object) may not have permission to create objects in Active Directory. The File Server role requires a Computer object of the same name as the "Client Access Point" provided in Step 8.

13. Under **Roles** in the console tree, you will see the new role you created listed as the name you created. With it highlighted, under the **Actions** pane on the right, choose **Add a share**.
14. Run through the share wizard inputting the following:
    - Type of share it will be
    - Location/path the folder shared will be
    - The name of the share users will connect to
    - Additional settings such as Access-based enumeration, caching, encryption, etc.
    - File level permissions if they will be other than the defaults
15. On the **Confirmation** page, verify what you have configured, and select **Create** to create the file server share.
16. On the **Results** page, select Close if it created the share. If it could not create the share, it will give you the errors incurred.
17. Choose **Close**.
18. Repeat this process for any additional shares.

Deploy a cluster set

12/9/2022 • 13 minutes to read • Edit Online

Applies to: Windows Server 2019

This article provides information on how to deploy a cluster set for Windows Server Failover Clusters using PowerShell. A cluster set is a group of multiple failover clusters that are clustered together. By using a cluster set, you can increase the number of server nodes in a single Software Defined Data Center (SDDC) cloud by orders of magnitude.

Cluster sets have been tested and supported up to 64 total cluster nodes. However, cluster sets can scale to much larger limits and aren't hardcoded for a limit.

Benefits

Cluster sets offer the following benefits:

- Significantly increases the supported SDDC cloud scale for running highly available virtual machines (VMs) by combining multiple smaller clusters into a single large fabric, while keeping the software fault boundary to a single cluster. You can easily migrate VMs across the cluster set.
- Increased resiliency. Having four 4-node clusters in a cluster set gives you better resiliency than a single 16-node cluster in that multiple compute nodes can go down and production remains intact.
- Management of failover cluster lifecycle, including onboarding and retiring clusters, without impacting tenant VM availability.
- VM flexibility across individual clusters and a present a unified storage namespace.
- Easily change the compute-to-storage workload ratio in your hyper-converged environment.
- Benefit from Azure-like Fault Domains and Availability sets across individual clusters in initial VM placement and subsequent migration.
- Can use even if compute and storage hardware between cluster nodes isn't identical.
- Live migration of VMs between clusters.
- Azure-like availability sets and fault domains across multiple clusters.
- Moving of SQL Server VMs between clusters.

Requirements and limitations

There are a few requirements and limitations for using cluster sets:

- All member clusters in a cluster set must be in the same Active Directory (AD) forest.
- Member servers in the set must run the same operating system version. Virtual machines can't be live migrated between different operating systems. You can have a cluster set that consists of any one, but not multiples, of the following options:
  - Windows Server 2019 Failover Cluster and Windows Server 2019 Failover Cluster
  - Windows Server 2019 Failover Cluster and Windows Server 2019 Storage Spaces Direct

- Windows Server 2019 Storage Spaces Direct and Windows Server 2019 Storage Spaces Direct

- Identical processor hardware is needed for all member servers for live migration between member clusters to occur; otherwise, you must select **CPU Processor Compatibility** in virtual machines settings.
- Cluster set VMs must be manually live-migrated across clusters - they can't automatically fail over.
- Storage Replica must be used between member clusters to realize storage resiliency to cluster failures. When using Storage Replica, bear in mind that namespace storage UNC paths will not change automatically on Storage Replica failover to the replica target cluster.
- Storage Spaces Direct doesn't function across member clusters in a cluster set. Rather, Storage Spaces Direct applies to a single cluster, with each cluster having its own storage pool.

Architecture

The following diagram illustrates a cluster set at a high level:

The following provides a summary of each of the elements shown:

Management cluster

The management cluster hosts the highly-available management plane and the namespace referral scale-out file server (SOFS) for the cluster set. A management cluster is logically decoupled from individual member clusters that run VM workloads. This makes the cluster set management plane resilient to any localized cluster-wide failures, such as loss of power of a member cluster.

Cluster set namespace referral SOFS

A namespace for the cluster set is provided with an SOFS server role running on the management cluster. This is similar to a Distributed File System Namespace (DFSN). Unlike DFSN however, cluster set namespace referral metadata is auto-populated on all cluster nodes without any intervention, so there's almost no performance overhead in the storage access path. This lightweight referral mechanism doesn't participate in the I/O path.

Each Server Message Block (SMB) referral share on the cluster set namespace referral SOFS is of type `SimpleReferral`. This referral allows SMB clients access to the target SMB share hosted on the member cluster SOFS. Referrals are cached perpetually on each of the client nodes and the cluster set namespace dynamically updates the referrals as needed automatically. Referral information is persistently cached in each cluster set node, even during reboots.

Cluster set master

Communication between member clusters is loosely coupled and coordinated by the cluster set master (CS-Master) resource. Like other cluster set resources, CS-Master is highly available and resilient to individual member cluster failures or management cluster node failures. Through a cluster set WMI provider, CS-Master provides the management endpoint for all cluster set management actions.

Member cluster

A member cluster runs VM and Storage Spaces Direct workloads. Multiple member clusters participate in a cluster set deployment, forming the larger SDDC cloud fabric. Member clusters differ from the management cluster in two key aspects: member clusters participate in fault domain and availability set constructs, and member clusters are sized to host VM and Storage Spaces Direct workloads. VMs that move across member clusters aren't hosted on the management cluster for this reason.

Cluster set worker

The CS-Master interacts with a cluster resource on member clusters called the cluster set worker (CS-Worker). CS-Worker responds to requests by the CS-Master, including VM placement and resource inventorying. There's one CS-Worker instance per member cluster.

Fault domain

A fault domain is a group of hardware and software that could fail together. While you could designate one or more clusters together as a fault domain, each node could participate in a fault domain in an availability set. Fault domain boundaries are based on data center topology, networking architecture, and other considerations.

Availability set

An availability set is used to configure the desired redundancy of clustered workloads across fault domains by grouping and deploying workloads. For a two-tier application, you should configure at least two VMs in an availability set for each tier, which ensures that when a fault domain in an availability set goes down, your application will have at least one VM in each tier hosted on a different fault domain.

Create a cluster set

Use PowerShell within the following example workflow to create a cluster set using two clusters. The name of the cluster set here is `CSMASTER`.

CLUSTER NAME	INFRASTRUCTURE SOFS NAME
SET-CLUSTER	SOFS-CLUSTERSET
CLUSTER1	SOFS-CLUSTER1
CLUSTER2	SOFS-CLUSTER2

1. Use a management client computer running Windows Server 2022 or Windows Server 2019.
2. Install Failover Cluster tools on the management cluster server.
3. Create two cluster members and with at least two Cluster Shared Volumes (CSVs) in each cluster.
4. Create a management cluster (physical or guest) that straddles the member clusters. This ensures that the cluster set management plane continues to be available despite possible member cluster failures.
5. To create the cluster set:

```
New-ClusterSet -Name CSMASTER -NamespaceRoot SOFS-CLUSTERSET -CimSession SET-CLUSTER
```

> **NOTE**
> If you are using a static IP address, you must include *-StaticAddress x.x.x.x* on the **New-ClusterSet** command.

6. To add cluster members to the cluster set:

```
Add-ClusterSetMember -ClusterName CLUSTER1 -CimSession CSMASTER -InfraSOFSName SOFS-CLUSTER1
Add-ClusterSetMember -ClusterName CLUSTER2 -CimSession CSMASTER -InfraSOFSName SOFS-CLUSTER2
```

7. To enumerate all member clusters in the cluster set:

```
Get-ClusterSetMember -CimSession CSMASTER
```

8. To enumerate all the member clusters in the cluster set including the management cluster nodes:

```
Get-ClusterSet -CimSession CSMASTER | Get-Cluster | Get-ClusterNode
```

9. To list all server nodes from all member clusters:

```
Get-ClusterSetNode -CimSession CSMASTER
```

10. To list all resource groups across the cluster set:

```
Get-ClusterSet -CimSession CSMASTER | Get-Cluster | Get-ClusterGroup
```

11. To verify the cluster set contains one SMB share (`ScopeName` being the Infrastructure File Server name) on the infrastructure SOFS for each cluster member CSV volume:

```
Get-SmbShare -CimSession CSMASTER
```

12. Review the cluster set debug log files for the cluster set, the management cluster, and each cluster member:

```
Get-ClusterSetLog -ClusterSetCimSession CSMASTER -IncludeClusterLog -IncludeManagementClusterLog -
DestinationFolderPath <path>
```

13. Configure Kerberos with constrained delegation between all cluster set members.

14. Configure the cross-cluster VM live migration authentication type to Kerberos on each node in the cluster set:

```
foreach($h in $hosts){ Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos -ComputerName
$h }
```

15. Add the management cluster to the local administrators group on each cluster member server node in the cluster set:

```
foreach($h in $hosts){ Invoke-Command -ComputerName $h -ScriptBlock {Net localgroup administrators
/add <management_cluster_name>$} }
```

Create cluster set VMs

After creating the cluster set, the next step is to create VMs. You should perform the following checks beforehand:

- Check available memory on each cluster server node
- Check available disk space on each cluster server node
- Check any specific VM storage requirements in terms of speed and performance

The `Get-ClusterSetOptimalNodeForVM` command identifies the optimal cluster and node in the cluster set and then deploys the VM on it. In the following example, a new VM is created with:

- 4 GB available
- One virtual processor
- 10% minimum CPU available

```
# Identify the optimal node to create a new virtual machine
$memoryinMB=4096
$vpcount = 1
$targetnode = Get-ClusterSetOptimalNodeForVM -CimSession CSMASTER -VMMemory $memoryinMB -VMVirtualCoreCount
$vpcount -VMCpuReservation 10
$secure_string_pwd = convertto-securestring "<password>" -asplaintext -force
$cred = new-object -typename System.Management.Automation.PSCredential ("
<domain\account>",$secure_string_pwd)

# Deploy the virtual machine on the optimal node
Invoke-Command -ComputerName $targetnode.name -scriptblock { param([String]$storagepath); New-VM CSVM1 -
MemoryStartupBytes 3072MB -path $storagepath -NewVHDPath CSVM.vhdx -NewVHDSizeBytes 4194304 } -ArgumentList
@("\\SOFS-CLUSTER1\VOLUME1") -Credential $cred | Out-Null

Start-VM CSVM1 -ComputerName $targetnode.name | Out-Null
Get-VM CSVM1 -ComputerName $targetnode.name | fl State, ComputerName
```

When complete, you are shown which cluster node the VM was deployed on. For the above example, it would show as:

```
State         : Running
ComputerName  : 1-S2D2
```

If there's not enough memory, CPU capacity, or disk space available to add the VM, you'll receive the following error:

```
Get-ClusterSetOptimalNodeForVM : A cluster node isn't available for this operation.
```

Once the VM is created, it is displayed in Hyper-V manager on the specific node specified. To add it as a cluster set VM and add it to the cluster, use this command:

```
Register-ClusterSetVM -CimSession CSMASTER -MemberName $targetnode.Member -VMName CSVM1
```

When complete, the output is:

```
Id  VMName  State  MemberName  PSComputerName
--  ------  -----  ----------  --------------
 1  CSVM1     On   CLUSTER1    CSMASTER
```

If you've created a cluster using existing VMs, the VMs need to be registered with the cluster set. To register all VMs at once, use:

```
Get-ClusterSetMember -Name CLUSTER3 -CimSession CSMASTER | Register-ClusterSetVM -RegisterAll -CimSession
CSMASTER
```

Next, add the VM path to the cluster set namespace.

As an example, suppose an existing cluster is added to the cluster set with pre-configured VMs that reside on the local Cluster Shared Volume (CSV). The path for the VHDX would be something similar to `C:\ClusterStorage\Volume1\MYVM\Virtual Hard Disks\MYVM.vhdx1`.

A storage migration is needed, as CSV paths are by design local to a single member cluster and are therefore not accessible to the VM once they are live migrated across member clusters.

In this example, CLUSTER3 is added to the cluster set using `Add-ClusterSetMember` with the scale-out file server SOFS-CLUSTER3. To move the VM configuration and storage, the command is:

```
Move-VMStorage -DestinationStoragePath \\SOFS-CLUSTER3\Volume1 -Name MyVM
```

Once complete, you may receive a warning:

```
WARNING: There were issues updating the virtual machine configuration that may prevent the virtual machine
from running. For more information view the report file below.
WARNING: Report file location: C:\Windows\Cluster\Reports\Update-ClusterVirtualMachineConfiguration '' on
date at time.htm.
```

This warning may be ignored as there were no physical changes in the virtual machine role storage configuration. The actual physical location doesn't change; only the configuration paths do.

For more information on `Move-VMStorage`, see Move-VMStorage.

Live migrating a VM within a cluster set involves the following:

```
Set-VMHost -UseAnyNetworkForMigration $true
```

Then, to move a cluster set VM from CLUSTER1 to NODE2-CL3 on CLUSTER3 for example, the command would be:

```
Move-ClusterSetVM -CimSession CSMASTER -VMName CSVM1 -Node NODE2-CL3
```

This command doesn't move the VM storage or configuration files and isn't necessary as the path to the VM remains as \\SOFS-CLUSTER1\VOLUME1. Once a VM has been registered with the infrastructure file server share path, the drives and VM don't require being on the same node as the VM.

Create the infrastructure scale-out file server

There's one Infrastructure SOFS cluster role on a cluster. The Infrastructure SOFS role is created by specifying the `-Infrastructure` switch parameter to the `Add-ClusterScaleOutFileServerRole` cmdlet. For example:

```
Add-ClusterScaleoutFileServerRole -Name "my_infra_sofs_name" -Infrastructure
```

Each CSV volume created automatically triggers the creation of an SMB share with an auto-generated name based on the CSV volume name. You can't directly create or modify SMB shares under an SOFS role, other than by using CSV volume create and modify operations.

In hyperconverged configurations, an Infrastructure SOFS allows an SMB client (Hyper-V host) to communicate with continuous availability (CA) to the Infrastructure SOFS SMB server. This hyper-converged SMB loopback CA is achieved by VMs accessing their virtual disk (VHDX) files where the owning VM identity is forwarded between the client and server. This identity forwarding allows the use of ACLs for VHDx files just as in standard hyperconverged cluster configurations as before.

Once a cluster set is created, the cluster set namespace relies on an Infrastructure SOFS on each of the member clusters, and additionally an Infrastructure SOFS in the management cluster.

At the time a member cluster is added to a cluster set, you can specify the name of an Infrastructure SOFS on that cluster if one already exists. If the Infrastructure SOFS doesn't exist, a new Infrastructure SOFS role on the new member cluster is created. If an Infrastructure SOFS role already exists on the member cluster, the Add operation implicitly renames it to the specified name as needed. Any existing SMB servers, or non-infrastructure SOFS roles on the member clusters, aren't used by the cluster set.

When the cluster set is created, you have the option to use an existing AD computer object as the namespace root on the management cluster. Cluster set creation creates the Infrastructure SOFS cluster role on the management cluster or renames the existing Infrastructure SOFS role. The Infrastructure SOFS on the management cluster is used as the cluster set namespace referral SOFS.

Create fault domains and availability sets

Azure-like fault domains and availability sets can be configured in a cluster set. This is beneficial for initial VM placements and migrations between clusters.

The example below has four clusters in a cluster set. Within the set, one fault domain is created with two of the clusters and a second fault domain is created with the other two clusters. These two fault domains comprise the availability set.

In the example below, CLUSTER1 and CLUSTER2 are in the fault domain **FD1** and CLUSTER3 and CLUSTER4 are in the fault domain **FD2**. The availability set is **CSMASTER-AS**.

To create the fault domains, the commands are:

```
New-ClusterSetFaultDomain -Name FD1 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER1,CLUSTER2 -
Description "First fault domain"

New-ClusterSetFaultDomain -Name FD2 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER3,CLUSTER4 -
Description "Second fault domain"
```

To ensure they've been created successfully, `Get-ClusterSetFaultDomain` can be run with its output shown for FD1:

```
PS C:\> Get-ClusterSetFaultDomain -CimSession CSMASTER -FdName FD1 | fl *

PSShowComputerName    : True
FaultDomainType       : Logical
ClusterName           : {CLUSTER1, CLUSTER2}
Description           : First fault domain
FDName                : FD1
Id                    : 1
PSComputerName        : CSMASTER
```

Now that the fault domains have been created, the availability set is created:

```
New-ClusterSetAvailabilitySet -Name CSMASTER-AS -FdType Logical -CimSession CSMASTER -ParticipantName
FD1,FD2
```

To validate it has been created, use:

```
Get-ClusterSetAvailabilitySet -AvailabilitySetName CSMASTER-AS -CimSession CSMASTER
```

When creating new VMs, use the `-AvailabilitySet` parameter to determine the optimal node for placement. Here's an example:

```
# Identify the optimal node to create a new VM
$memoryinMB=4096
$vpcount = 1
$av = Get-ClusterSetAvailabilitySet -Name CSMASTER-AS -CimSession CSMASTER
$targetnode = Get-ClusterSetOptimalNodeForVM -CimSession CSMASTER -VMMemory $memoryinMB -VMVirtualCoreCount
$vpcount -VMCpuReservation 10 -AvailabilitySet $av
$secure_string_pwd = convertto-securestring "<password>" -asplaintext -force
$cred = new-object -typename System.Management.Automation.PSCredential ("
<domain\account>",$secure_string_pwd)
```

Remove a cluster from a set

There are times when a cluster needs to be removed from a cluster set. As a best practice, all cluster set VMs should be moved out of the cluster beforehand. This can be done using the `Move-ClusterSetVM` and `Move-VMStorage` commands.

If the VMs aren't moved out of the cluster first, all remaining cluster set VMs hosted on the cluster being removed will become highly available VMs bound to that cluster, assuming they have access to their storage. Cluster sets also automatically update their inventory by no longer tracking the health of a removed cluster and the VMs running on it, and by removing the namespace and all references to shares hosted on the removed cluster.

For example, the command to remove the CLUSTER1 cluster from a cluster set is:

```
Remove-ClusterSetMember -ClusterName CLUSTER1 -CimSession CSMASTER
```

System state backup

System state backup will back up the cluster state and metadata. Using Windows Server Backup, you can restore just a node's cluster database if needed or do an authoritative restore to roll back the entire cluster database across all nodes. For cluster sets, we recommend doing an authoritative restore first for the member clusters and then for the management cluster. For more information on system state backup, see Back up system state

and bare metal.

Next steps

- Learn more about Storage Replica.

Prestage cluster computer objects in Active Directory Domain Services

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This topic shows how to prestage cluster computer objects in Active Directory Domain Services (AD DS). You can use this procedure to enable a user or group to create a failover cluster when they do not have permissions to create computer objects in AD DS.

When you create a failover cluster by using the Create Cluster Wizard or by using Windows PowerShell, you must specify a name for the cluster. If you have sufficient permissions when you create the cluster, the cluster creation process automatically creates a computer object in AD DS that matches the cluster name. This object is called the *cluster name object* or CNO. Through the CNO, virtual computer objects (VCOs) are automatically created when you configure clustered roles that use client access points. For example, if you create a highly available file server with a client access point that is named *FileServer1*, the CNO will create a corresponding VCO in AD DS.

> **NOTE**
>
> There is the option to create an Active Directory-detached cluster, where no CNO or VCOs are created in AD DS. This is targeted for specific types of cluster deployments. For more information, see Deploy an Active Directory-Detached Cluster.

To create the CNO automatically, the user who creates the failover cluster must have the **Create Computer objects** permission to the organizational unit (OU) or the container where the servers that will form the cluster reside. To enable a user or group to create a cluster without having this permission, a user with appropriate permissions in AD DS (typically a domain administrator) can prestage the CNO in AD DS. This also provides the domain administrator more control over the naming convention that is used for the cluster, and control over which OU the cluster objects are created in.

Step 1: Prestage the CNO in AD DS

Before you begin, make sure that you know the following:

- The name that you want to assign the cluster
- The name of the user account or group to which you want to grant rights to create the cluster

As a best practice, we recommend that you create an OU for the cluster objects. If an OU already exists that you want to use, membership in the **Account Operators** group is the minimum required to complete this step. If you need to create an OU for the cluster objects, membership in the **Domain Admins** group, or equivalent, is the minimum required to complete this step.

> **NOTE**
>
> If you create the CNO in the default Computers container instead of an OU, you do not have to complete Step 3 of this topic. In this scenario, a cluster administrator can create up to 10 VCOs without any additional configuration.

Prestage the CNO in AD DS

1. On a computer that has the AD DS Tools installed from the Remote Server Administration Tools, or on a domain controller, open **Active Directory Users and Computers**. To do this on a server, start Server Manager, and then on the **Tools** menu, select **Active Directory Users and Computers**.

2. To create an OU for the cluster computer objects, right-click the domain name or an existing OU, point to **New**, and then select **Organizational Unit**. In the **Name** box, enter the name of the OU, and then select **OK**.

3. In the console tree, right-click the OU where you want to create the CNO, point to **New**, and then select **Computer**.

4. In the **Computer name** box, enter the name that will be used for the failover cluster, and then select **OK**.

> **NOTE**
>
> This is the cluster name that the user who creates the cluster will specify on the **Access Point for Administering the Cluster** page in the Create Cluster wizard or as the value of the *–Name* parameter for the **New-Cluster** Windows PowerShell cmdlet.

5. As a best practice, right-click the computer account that you just created, select **Properties**, and then select the **Object** tab. On the **Object** tab, select the **Protect object from accidental deletion** check box, and then select **OK**.

6. Right-click the computer account that you just created, and then select **Disable Account**. Select **Yes** to confirm, and then select **OK**.

> **NOTE**
>
> You must disable the account so that during cluster creation, the cluster creation process can confirm that the account is not currently in use by an existing computer or cluster in the domain.

Figure 1. Disabled CNO in the example Clusters OU

Step 2: Grant the user permissions to create the cluster

You must configure permissions so that the user account that will be used to create the failover cluster has Full Control permissions to the CNO.

Membership in the **Account Operators** group is the minimum required to complete this step.

Here's how to grant the user permissions to create the cluster:

1. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.
2. Locate and then right-click the CNO, and then select **Properties**.
3. On the **Security** tab, select **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, specify the user account or group that you want to grant permissions to, and then select **OK**.
5. Select the user account or group that you just added, and then next to **Full control**, select the **Allow** check box.

Figure 2. Granting Full Control to the user or group that will create the cluster

6. Select **OK**.

After you complete this step, the user who you granted permissions to can create the failover cluster. However, if the CNO is located in an OU, the user cannot create clustered roles that require a client access point until you complete Step 3.

> **NOTE**
> If the CNO is in the default Computers container, a cluster administrator can create up to 10 VCOs without any additional configuration. To add more than 10 VCOs, you must explicitly grant the **Create Computer objects** permission to the CNO for the Computers container.

Step 3: Grant the CNO permissions to the OU or prestage VCOs for clustered roles

When you create a clustered role with a client access point, the cluster creates a VCO in the same OU as the CNO. For this to occur automatically, the CNO must have permissions to create computer objects in the OU.

If you prestaged the CNO in AD DS, you can do either of the following to create VCOs:

- Option 1: Grant the CNO permissions to the OU. If you use this option, the cluster can automatically create VCOs in AD DS. Therefore, an administrator for the failover cluster can create clustered roles without having to request that you prestage VCOs in AD DS.

> **NOTE**
> Membership in the **Domain Admins** group, or equivalent, is the minimum required to complete the steps for this option.

- Option 2: Prestage a VCO for a clustered role. Use this option if it is necessary to prestage accounts for clustered roles because of requirements in your organization. For example, you may want to control the naming convention, or control which clustered roles are created.

> **NOTE**
> Membership in the **Account Operators** group is the minimum required to complete the steps for this option.

Grant the CNO permissions to the OU

1. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.
2. Right-click the OU where you created the CNO in Step 1: Prestage the CNO in AD DS, and then select **Properties**.
3. On the **Security** tab, select **Advanced**.
4. In the **Advanced Security Settings** dialog box, select **Add**.
5. Next to **Principal**, select **Select a principal**.
6. In the **Select User, Computer, Service Account, or Groups** dialog box, select **Object Types**, select the **Computers** check box, and then select **OK**.
7. Under **Enter the object names to select**, enter the name of the CNO, select **Check Names**, and then select **OK**. In response to the warning message that says that you are about to add a disabled object, select **OK**.
8. In the **Permission Entry** dialog box, make sure that the **Type** list is set to **Allow**, and the **Applies to** list is set to **This object and all descendant objects**.
9. Under **Permissions**, select the **Create Computer objects** check box.

Figure 3. Granting the Create Computer objects permission to the CNO

10. Select **OK** until you return to the Active Directory Users and Computers snap-in.

An administrator on the failover cluster can now create clustered roles with client access points, and bring the resources online.

Prestage a VCO for a clustered role

1. Before you begin, make sure that you know the name of the cluster and the name that the clustered role will have.
2. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.
3. In Active Directory Users and Computers, right-click the OU where the CNO for the cluster resides, point to **New**, and then select **Computer**.
4. In the **Computer name** box, enter the name that you will use for the clustered role, and then select **OK**.
5. As a best practice, right-click the computer account that you just created, select **Properties**, and then select the **Object** tab. On the **Object** tab, select the **Protect object from accidental deletion** check box, and then select **OK**.
6. Right-click the computer account that you just created, and then select **Properties**.
7. On the **Security** tab, select **Add**.
8. In the **Select User, Computer, Service Account, or Groups** dialog box, select **Object Types**, select the **Computers** check box, and then select **OK**.
9. Under **Enter the object names to select**, enter the name of the CNO, select **Check Names**, and then select **OK**. If you receive a warning message that says that you are about to add a disabled object, select **OK**.
10. Make sure that the CNO is selected, and then next to **Full control**, select the **Allow** check box.
11. Select **OK**.

An administrator on the failover cluster can now create the clustered role with a client access point that matches the prestaged VCO name, and bring the resource online.

More information

- Failover Clustering
- Configuring cluster accounts in Active Directory

Configuring cluster accounts in Active Directory

12/9/2022 • 21 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Azure Stack HCI, versions 21H2 and 20H2

In Windows Server, when you create a failover cluster and configure clustered services or applications, the failover cluster wizards create the necessary Active Directory computer accounts (also called computer objects) and give them specific permissions. The wizards create a computer account for the cluster itself (this account is also called the cluster name object or CNO) and a computer account for most types of clustered services and applications, the exception being a Hyper-V virtual machine. The permissions for these accounts are set automatically by the failover cluster wizards. If the permissions are changed, they will need to be changed back to match cluster requirements. This guide describes these Active Directory accounts and permissions, provides background about why they are important, and describes steps for configuring and managing the accounts.

Overview of Active Directory accounts needed by a failover cluster

This section describes the Active Directory computer accounts (also called Active Directory computer objects) that are important for a failover cluster. These accounts are as follows:

- **The user account used to create the cluster.** This is the user account used to start the Create Cluster wizard. The account is important because it provides the basis from which a computer account is created for the cluster itself.

- **The cluster name account.** (the computer account of the cluster itself, also called the cluster name object or CNO). This account is created automatically by the Create Cluster wizard and has the same name as the cluster. The cluster name account is very important, because through this account, other accounts are automatically created as you configure new services and applications on the cluster. If the cluster name account is deleted or permissions are taken away from it, other accounts cannot be created as required by the cluster, until the cluster name account is restored or the correct permissions are reinstated.

  For example, if you create a cluster called Cluster1 and then try to configure a clustered print server called PrintServer1 on your cluster, the Cluster1 account in Active Directory will need to retain the correct permissions so that it can be used to create a computer account called PrintServer1.

  The cluster name account is created in the default container for computer accounts in Active Directory. By default this is the "Computers" container, but the domain administrator can choose to redirect it to another container or organizational unit (OU).

- **The computer account (computer object) of a clustered service or application.** These accounts are created automatically by the High Availability wizard as part of the process of creating most types of clustered services or application, the exception being a Hyper-V virtual machine. The cluster name account is granted the necessary permissions to control these accounts.

  For example, if you have a cluster called Cluster1 and then you create a clustered file server called FileServer1, the High Availability wizard creates an Active Directory computer account called FileServer1. The High Availability wizard also gives the Cluster1 account the necessary permissions to control the FileServer1 account.

The following table describes the permissions required for these accounts.

ACCOUNT	DETAILS ABOUT PERMISSIONS
Account used to create the cluster	Requires administrative permissions on the servers that will become cluster nodes. Also requires **Create Computer objects** and **Read All Properties** permissions in the container that is used for computer accounts in the domain.
Cluster name account (computer account of the cluster itself)	When the Create Cluster wizard is run, it creates the cluster name account in the default container that is used for computer accounts in the domain. By default, the cluster name account (like other computer accounts) can create up to ten computer accounts in the domain. If you create the cluster name account (cluster name object) before creating the cluster—that is, prestage the account—you must give it the **Create Computer objects** and **Read All Properties** permissions in the container that is used for computer accounts in the domain. You must also disable the account, and give **Full Control** of it to the account that will be used by the administrator who installs the cluster. For more information, see Steps for prestaging the cluster name account, later in this guide.
Computer account of a clustered service or application	When the High Availability wizard is run (to create a new clustered service or application), in most cases a computer account for the clustered service or application is created in Active Directory. The cluster name account is granted the necessary permissions to control this account. The exception is a clustered Hyper-V virtual machine: no computer account is created for this. If you prestage the computer account for a clustered service or application, you must configure it with the necessary permissions. For more information, see Steps for prestaging an account for a clustered service or application, later in this guide.

NOTE

In earlier versions of Windows Server, there was an account for the Cluster service. Since Windows Server 2008, however, the Cluster service automatically runs in a special context that provides the specific permissions and privileges necessary for the service (similar to the local system context, but with reduced privileges). Other accounts are needed, however, as described in this guide.

How accounts are created through wizards in failover clustering

The following diagram illustrates the use and creation of computer accounts (Active Directory objects) that are described in the previous subsection. These accounts come into play when an administrator runs the Create Cluster wizard and then runs the High Availability wizard (to configure a clustered service or application).

Note that the above diagram shows a single administrator running both the Create Cluster wizard and the High Availability wizard. However, this could be two different administrators using two different user accounts, if both accounts had sufficient permissions. The permissions are described in more detail in Requirements related to failover clusters, Active Directory domains, and accounts, later in this guide.

How problems can result if accounts needed by the cluster are changed

The following diagram illustrates how problems can result if the cluster name account (one of the accounts required by the cluster) is changed after it is automatically created by the Create Cluster wizard.

If the type of problem shown in the diagram occurs, a certain event (1193, 1194, 1206, or 1207) is logged in Event Viewer. For more information about these events, see https://go.microsoft.com/fwlink/?LinkId=118271.

Note that a similar problem with creating an account for a clustered service or application can occur if the domain-wide quota for creating computer objects (by default, 10) has been reached. If it has, it might be appropriate to consult with the domain administrator about increasing the quota, although this is a domain-wide setting and should be changed only after careful consideration, and only after confirming that the preceding diagram does not describe your situation. For more information, see Steps for troubleshooting problems caused by changes in cluster-related Active Directory accounts, later in this guide.

Requirements related to failover clusters, Active Directory domains, and accounts

As described in the preceding three sections, certain requirements must be met before clustered services and applications can be successfully configured on a failover cluster. The most basic requirements concern the location of cluster nodes (within a single domain) and the level of permissions of the account of the person who installs the cluster. If these requirements are met, the other accounts required by the cluster can be created automatically by the failover cluster wizards. The following list provides details about these basic requirements.

- **Nodes:** All nodes must be in the same Active Directory domain. (The domain cannot be based on Windows NT 4.0, which does not include Active Directory.)
- **Account of the person who installs the cluster:** The person who installs the cluster must use an account with the following characteristics:
  - The account must be a domain account. It does not have to be a domain administrator account. It can be a domain user account if it meets the other requirements in this list.
  - The account must have administrative permissions on the servers that will become cluster nodes. The simplest way to provide this is to create a domain user account, and then add that account to the local Administrators group on each of the servers that will become cluster nodes. For more information, see Steps for configuring the account for the person who installs the cluster, later in this guide.
  - The account (or the group that the account is a member of) must be given the **Create Computer objects** and **Read All Properties** permissions in the container that is used for computer accounts in the domain. For more information, see Steps for configuring the account for the person who installs the cluster, later in this guide.
  - If your organization chooses to prestage the cluster name account (a computer account with the same name as the cluster), the prestaged cluster name account must give "Full Control" permission to the account of the person who installs the cluster. For other important details about how to prestage the cluster name account, see Steps for prestaging the cluster name account, later in this guide.

Planning ahead for password resets and other account maintenance

The administrators of failover clusters might sometimes need to reset the password of the cluster name account. This action requires a specific permission, the **Reset password** permission. Therefore, it is a best practice to edit the permissions of the cluster name account (by using the Active Directory Users and Computers snap-in) to give the administrators of the cluster the **Reset password** permission for the cluster name account. For more information, see Steps for troubleshooting password problems with the cluster name account, later in this guide.

Steps for configuring the account for the person who installs the cluster

The account of the person who installs the cluster is important because it provides the basis from which a computer account is created for the cluster itself.

The minimum group membership required to complete the following procedure depends on whether you are creating the domain account and assigning it the required permissions in the domain, or whether you are only placing the account (created by someone else) into the local **Administrators** group on the servers that will be nodes in the failover cluster. If the former, membership in **Account Operators** or equivalent, is the minimum required to complete this procedure. If the latter, membership in the local **Administrators** group on the servers that will be nodes in the failover cluster, or equivalent, is all that is required. Review details about using the appropriate accounts and group memberships at https://go.microsoft.com/fwlink/?LinkId=83477.

To configure the account for the person who installs the cluster

1. Create or obtain a domain account for the person who installs the cluster. This account can be a domain user account or an **Account Operators** account. If you use a standard user account, you'll have to give it

some extra permissions later in this procedure.

2. If the account that was created or obtained in step 1 isn't automatically included in the local **Administrators** group on computers in the domain, add the account to the local **Administrators** group on the servers that will be nodes in the failover cluster:

   a. Click **Start**, click **Administrative Tools**, and then click **Server Manager**.

   b. In the console tree, expand **Configuration**, expand **Local Users and Groups**, and then expand **Groups**.

   c. In the center pane, right-click **Administrators**, click **Add to Group**, and then click **Add**.

   d. Under **Enter the object names to select**, type the name of the user account that was created or obtained in step 1. If prompted, enter an account name and password with sufficient permissions for this action. Then click **OK**.

   e. Repeat these steps on each server that will be a node in the failover cluster.

   > **IMPORTANT**
   >
   > These steps must be repeated on all servers that will be nodes in the cluster.

3. If the account that was created or obtained in step 1 is a domain administrator account, skip the rest of this procedure. Otherwise, give the account the **Create Computer objects** and **Read All Properties** permissions in the container that is used for computer accounts in the domain:

   a. On a domain controller, click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.

   b. On the **View** menu, make sure that **Advanced Features** is selected.

      When **Advanced Features** is selected, you can see the **Security** tab in the properties of accounts (objects) in **Active Directory Users and Computers**.

   c. Right-click the default **Computers** container or the default container in which computer accounts are created in your domain, and then click **Properties**. **Computers** is located in **Active Directory Users and Computers/***domain-node***/Computers**.

   d. On the **Security** tab, click **Advanced**.

   e. Click **Add**, type the name of the account that was created or obtained in step 1, and then click **OK**.

   f. In the **Permission Entry for** *container* dialog box, locate the **Create Computer objects** and **Read All Properties** permissions, and make sure that the **Allow** check box is selected for each one.

Steps for prestaging the cluster name account

It is usually simpler if you do not prestage the cluster name account, but instead allow the account to be created and configured automatically when you run the Create Cluster wizard. However, if it is necessary to prestage the cluster name account because of requirements in your organization, use the following procedure.

Membership in the **Domain Admins** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at https://go.microsoft.com/fwlink/?LinkId=83477. Note that you can use the same account for this procedure as you will use when creating the cluster.

To prestage a cluster name account

1. Make sure that you know the name that the cluster will have, and the name of the user account that will be used by the person who creates the cluster. (Note that you can use that account to perform this procedure.)

2. On a domain controller, click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.

3. In the console tree, right-click **Computers** or the default container in which computer accounts are created in your domain. **Computers** is located in **Active Directory Users and Computers/** *domain-node*/**Computers**.

4. Click **New** and then click **Computer**.

5. Type the name that will be used for the failover cluster, in other words, the cluster name that will be specified in the Create Cluster wizard, and then click **OK**.

6. Right-click the account that you just created, and then click **Disable Account**. If prompted to confirm your choice, click **Yes**.

   The account must be disabled so that when the **Create Cluster** wizard is run, it can confirm that the account it will use for the cluster is not currently in use by an existing computer or cluster in the domain.

7. On the **View** menu, make sure that **Advanced Features** is selected.

When **Advanced Features** is selected, you can see the **Security** tab in the properties of accounts (objects) in **Active Directory Users and Computers**.

8. Right-click the folder that you right-clicked in step 3, and then click **Properties**.

9. On the **Security** tab, click **Advanced**.

10. Click **Add**, click **Object Types** and make sure that **Computers** is selected, and then click **OK**. Then, under **Enter the object name to select**, type the name of the computer account you just created, and then click **OK**. If a message appears, saying that you are about to add a disabled object, click **OK**.

11. In the **Permission Entry** dialog box, locate the **Create Computer objects** and **Read All Properties** permissions, and make sure that the **Allow** check box is selected for each one.

12. Click **OK** until you have returned to the **Active Directory Users and Computers** snap-in.

13. If you are using the same account to perform this procedure as will be used to create the cluster, skip the remaining steps. Otherwise, you must configure permissions so that the user account that will be used to create the cluster has full control of the computer account you just created:

    a. On the **View** menu, make sure that **Advanced Features** is selected.

    b. Right-click the computer account you just created, and then click **Properties**.

    c. On the **Security** tab, click **Add**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.

    d. Use the **Select Users, Computers, or Groups** dialog box to specify the user account that will be used when creating the cluster. Then click **OK**.

    e. Make sure that the user account that you just added is selected, and then, next to **Full Control**, select the **Allow** check box.

Steps for prestaging an account for a clustered service or application

It is usually simpler if you do not prestage the computer account for a clustered service or application, but instead allow the account to be created and configured automatically when you run the High Availability wizard. However, if it is necessary to prestage accounts because of requirements in your organization, use the following procedure.

Membership in the **Account Operators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at https://go.microsoft.com/fwlink/?LinkId=83477.

To prestage an account for a clustered service or application

1. Make sure that you know the name of the cluster and the name that the clustered service or application will have.

2. On a domain controller, click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.

3. In the console tree, right-click **Computers** or the default container in which computer accounts are created in your domain. **Computers** is located in **Active Directory Users and Computers/** *domain-node*/**Computers**.

4. Click **New** and then click **Computer**.

5. Type the name that you will use for the clustered service or application, and then click **OK**.

6. On the **View** menu, make sure that **Advanced Features** is selected.

   When **Advanced Features** is selected, you can see the **Security** tab in the properties of accounts (objects) in **Active Directory Users and Computers**.

7. Right-click the computer account you just created, and then click **Properties**.

8. On the **Security** tab, click **Add**.

9. Click **Object Types** and make sure that **Computers** is selected, and then click **OK**. Then, under **Enter the object name to select**, type the cluster name account, and then click **OK**. If a message appears, saying that you are about to add a disabled object, click **OK**.

10. Make sure that the cluster name account is selected, and then, next to **Full Control**, select the **Allow** check box.

Steps for troubleshooting problems related to accounts used by the cluster

As described earlier in this guide, when you create a failover cluster and configure clustered services or applications, the failover cluster wizards create the necessary Active Directory accounts and give them the correct permissions. If a needed account is deleted, or necessary permissions are changed, problems can result. The following subsections provide steps for troubleshooting these issues.

- Steps for troubleshooting password problems with the cluster name account
- Steps for troubleshooting problems caused by changes in cluster-related Active Directory accounts

Steps for troubleshooting password problems with the cluster name account

Use this procedure if there is an event message about computer objects or about the cluster identity that includes the following text. Note that this text will be within the event message, not at the beginning of the event message:

```
Logon failure: unknown user name or bad password.
```

Event messages that fit the previous description indicate that the password for the cluster name account and the corresponding password stored by the clustering software no longer match.

For information about ensuring that cluster administrators have the correct permissions to perform the following procedure as needed, see Planning ahead for password resets and other account maintenance, earlier in this guide.

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this

procedure. In addition, your account must be given **Reset password** permission for the cluster name account (unless your account is a **Domain Admins** account or is the Creator Owner of the cluster name account). The account that was used by the person who installed the cluster can be used for this procedure. Review details about using the appropriate accounts and group memberships at https://go.microsoft.com/fwlink/?LinkId=83477.

To troubleshoot password problems with the cluster name account

1. To open the failover cluster snap-in, click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**. (If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.)
2. In the Failover Cluster Management snap-in, if the cluster you want to configure is not displayed, in the console tree, right-click **Failover Cluster Management**, click **Manage a Cluster**, and select or specify the cluster you want.
3. In the center pane, expand **Cluster Core Resources**.
4. Under **Cluster Name**, right-click the **Name** item, point to **More Actions**, and then click **Repair Active Directory Object**.

Steps for troubleshooting problems caused by changes in cluster-related Active Directory accounts

If the cluster name account is deleted or if permissions are taken away from it, problems will occur when you try to configure a new clustered service or application. To troubleshoot a problem where this might be the cause, use the Active Directory Users and Computers snap-in to view or change the cluster name account and other related accounts. For information about the events that are logged when this type of problem occurs (event 1193, 1194, 1206, or 1207), see https://go.microsoft.com/fwlink/?LinkId=118271.

Membership in the **Domain Admins** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at https://go.microsoft.com/fwlink/?LinkId=83477.

To troubleshoot problems caused by changes in cluster-related Active Directory accounts

1. On a domain controller, click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
2. Expand the default **Computers** container or the folder in which the cluster name account (the computer account for the cluster) is located. **Computers** is located in **Active Directory Users and Computers/** *domain-node*/**Computers**.
3. Examine the icon for the cluster name account. It must not have a downward-pointing arrow on it, that is, the account must not be disabled. If it appears to be disabled, right-click it and look for the command **Enable Account**. If you see the command, click it.
4. On the **View** menu, make sure that **Advanced Features** is selected.

   When **Advanced Features** is selected, you can see the **Security** tab in the properties of accounts (objects) in **Active Directory Users and Computers**.
5. Right-click the default **Computers** container or the folder in which the cluster name account is located.
6. Click **Properties**.
7. On the **Security** tab, click **Advanced**.
8. In the list of accounts with permissions, click the cluster name account, and then click **Edit**.

> **NOTE**
>
> If the cluster name account is not listed, click **Add** and add it to the list.

9. For the cluster name account (also known as the cluster name object or CNO), ensure that **Allow** is selected for the **Create Computer objects** and **Read All Properties** permissions.

10. Click **OK** until you have returned to the **Active Directory Users and Computers** snap-in.

11. Review domain policies (consulting with a domain administrator if applicable) related to the creation of computer accounts (objects). Ensure that the cluster name account can create a computer account each time you configure a clustered service or application. For example, if your domain administrator has configured settings that cause all new computer accounts to be created in a specialized container rather than the default **Computers** container, make sure that these settings allow the cluster name account to create new computer accounts in that container also.

12. Expand the default **Computers** container or the container in which the computer account for one of the clustered services or applications is located.

13. Right-click the computer account for one of the clustered services or applications, and then click **Properties**.

14. On the **Security** tab, confirm that the cluster name account is listed among the accounts that have permissions, and select it. Confirm that the cluster name account has **Full Control** permission (the **Allow** check box is selected). If it does not, add the cluster name account to the list and give it **Full Control** permission.

15. Repeat steps 13-14 for each clustered service and application configured in the cluster.

16. Check that the domain-wide quota for creating computer objects (by default, 10) has not been reached (consulting with a domain administrator if applicable). If the previous items in this procedure have all been reviewed and corrected, and if the quota has been reached, consider increasing the quota. To change the quota:

17. Open a command prompt as an administrator and run **ADSIEdit.msc**.

18. Right-click **ADSI Edit**, click **Connect to**, and then click **OK**. The **Default naming context** is added to the console tree.

19. Double-click **Default naming context**, right-click the domain object underneath it, and then click **Properties**.

20. Scroll to **ms-DS-MachineAccountQuota**, select it, click **Edit**, change the value, and then click **OK**.

Configure and manage quorum

12/9/2022 • 21 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This article provides background and steps to configure and manage the quorum in a failover cluster.

For information about cluster and storage pool quorums in Storage Spaces Direct on Azure Stack HCI and Windows Server clusters, see Understanding cluster and pool quorum.

Understanding quorum

The quorum for a cluster is determined by the number of voting elements that must be part of active cluster membership for that cluster to start properly or continue running. For a more detailed explanation, see the understanding cluster and pool quorum doc.

Quorum configuration options

The quorum model in Windows Server is flexible. If you need to modify the quorum configuration for your cluster, you can use the Configure Cluster Quorum Wizard or the FailoverClusters Windows PowerShell cmdlets. For steps and considerations to configure the quorum, see Configure the cluster quorum later in this topic.

The following table lists the three quorum configuration options that are available in the Configure Cluster Quorum Wizard.

OPTION	DESCRIPTION
Use typical settings	The cluster automatically assigns a vote to each node and dynamically manages the node votes. If it is suitable for your cluster, and there is cluster shared storage available, the cluster selects a disk witness. This option is recommended in most cases, because the cluster software automatically chooses a quorum and witness configuration that provides the highest availability for your cluster.
Add or change the quorum witness	You can add, change, or remove a witness resource. You can configure a file share or disk witness. The cluster automatically assigns a vote to each node and dynamically manages the node votes.
Advanced quorum configuration and witness selection	You should select this option only when you have application-specific or site-specific requirements for configuring the quorum. You can modify the quorum witness, add or remove node votes, and choose whether the cluster dynamically manages node votes. By default, votes are assigned to all nodes, and the node votes are dynamically managed.

Depending on the quorum configuration option that you choose and your specific settings, the cluster will be configured in one of the following quorum modes:

MODE	DESCRIPTION
Node majority (no witness)	Only nodes have votes. No quorum witness is configured. The cluster quorum is the majority of voting nodes in the active cluster membership.
Node majority with witness (disk or file share)	Nodes have votes. In addition, a quorum witness has a vote. The cluster quorum is the majority of voting nodes in the active cluster membership plus a witness vote. A quorum witness can be a designated disk witness or a designated file share witness.
No majority (disk witness only)	No nodes have votes. Only a disk witness has a vote. The cluster quorum is determined by the state of the disk witness. Generally, this mode is not recommended, and it should not be selected because it creates a single point of failure for the cluster.

The following subsections will give you more information about advanced quorum configuration settings.

Witness configuration

As a general rule when you configure a quorum, the voting elements in the cluster should be an odd number. Therefore, if the cluster contains an even number of voting nodes, you should configure a disk witness or a file share witness. The cluster will be able to sustain one additional node down. In addition, adding a witness vote enables the cluster to continue running if half the cluster nodes simultaneously go down or are disconnected.

A disk witness is usually recommended if all nodes can see the disk. A file share witness is recommended when you need to consider multisite disaster recovery with replicated storage. Configuring a disk witness with replicated storage is possible only if the storage vendor supports read-write access from all sites to the replicated storage. ***A Disk Witness isn't supported with Storage Spaces Direct***.

The following table provides additional information and considerations about the quorum witness types.

WITNESS TYPE	DESCRIPTION	REQUIREMENTS AND RECOMMENDATIONS
Disk witness	• Dedicated LUN that stores a copy of the cluster database • Most useful for clusters with shared (not replicated) storage	• Size of LUN must be at least 512 MB • Must be dedicated to cluster use and not assigned to a clustered role • Must be included in clustered storage and pass storage validation tests • Cannot be a disk that is a Cluster Shared Volume (CSV) • Basic disk with a single volume • Does not need to have a drive letter • Can be formatted with NTFS or ReFS • Can be optionally configured with hardware RAID for fault tolerance • Should be excluded from backups and antivirus scanning • A Disk witness isn't supported with Storage Spaces Direct

WITNESS TYPE	DESCRIPTION	REQUIREMENTS AND RECOMMENDATIONS
File share witness	• SMB file share that is configured on a file server running Windows Server • Does not store a copy of the cluster database • Maintains cluster information only in a witness.log file • Most useful for multisite clusters with replicated storage	• Must have a minimum of 5 MB of free space • Must be dedicated to the single cluster and not used to store user or application data • Must have write permissions enabled for the computer object for the cluster name The following are additional considerations for a file server that hosts the file share witness: • A single file server can be configured with file share witnesses for multiple clusters. • The file server must be on a site that is separate from the cluster workload. This allows equal opportunity for any cluster site to survive if site-to-site network communication is lost. If the file server is on the same site, that site becomes the primary site, and it is the only site that can reach the file share. • The file server can run on a virtual machine if the virtual machine is not hosted on the same cluster that uses the file share witness. • For high availability, the file server can be configured on a separate failover cluster.
Cloud witness	• A witness file stored in Azure Blob Storage • Does not store a copy of the cluster database • Recommended when all servers in the cluster have a reliable Internet connection.	See Deploy a cloud witness.

NOTE

If you configure a file share witness or a cloud witness then shutdown all nodes for a maintenance or some reason, you have to make sure that start your cluster service from a last-man standing node since the latest cluster database is not stored into those witnesses. See this also.

Node vote assignment

As an advanced quorum configuration option, you can choose to assign or remove quorum votes on a per-node basis. By default, all nodes are assigned votes. Regardless of vote assignment, all nodes continue to function in the cluster, receive cluster database updates, and can host applications.

You might want to remove votes from nodes in certain disaster recovery configurations. For example, in a multisite cluster, you could remove votes from the nodes in a backup site so that those nodes do not affect quorum calculations. This configuration is recommended only for manual failover across sites. For more information, see Quorum considerations for disaster recovery configurations later in this topic.

The configured vote of a node can be verified by looking up the **NodeWeight** common property of the cluster node by using the Get-ClusterNode Windows PowerShell cmdlet. A value of 0 indicates that the node does not have a quorum vote configured. A value of 1 indicates that the quorum vote of the node is assigned, and it is managed by the cluster. For more information about management of node votes, see Dynamic quorum management later in this topic.

The vote assignment for all cluster nodes can be verified by using the **Validate Cluster Quorum** validation test.

Additional considerations for node vote assignment

- Node vote assignment is not recommended to enforce an odd number of voting nodes. Instead, you should configure a disk witness or file share witness. For more information, see Witness configuration later in this topic.
- If dynamic quorum management is enabled, only the nodes that are configured to have node votes assigned can have their votes assigned or removed dynamically. For more information, see Dynamic quorum management later in this topic.

Dynamic quorum management

In Windows Server 2012, as an advanced quorum configuration option, you can choose to enable dynamic quorum management by cluster. For more details on how dynamic quorum works, see this explanation.

With dynamic quorum management, it is also possible for a cluster to run on the last surviving cluster node. By dynamically adjusting the quorum majority requirement, the cluster can sustain sequential node shutdowns to a single node.

The cluster-assigned dynamic vote of a node can be verified with the **DynamicWeight** common property of the cluster node by using the Get-ClusterNode Windows PowerShell cmdlet. A value of 0 indicates that the node does not have a quorum vote. A value of 1 indicates that the node has a quorum vote.

The vote assignment for all cluster nodes can be verified by using the **Validate Cluster Quorum** validation test.

Additional considerations for dynamic quorum management

- Dynamic quorum management does not allow the cluster to sustain a simultaneous failure of a majority of voting members. To continue running, the cluster must always have a quorum majority at the time of a node shutdown or failure.
- If you have explicitly removed the vote of a node, the cluster cannot dynamically add or remove that vote.
- When Storage Spaces Direct is enabled, the cluster can only support two node failures. This is explained more in the pool quorum section

General recommendations for quorum configuration

The cluster software automatically configures the quorum for a new cluster, based on the number of nodes configured and the availability of shared storage. This is usually the most appropriate quorum configuration for that cluster. However, it is a good idea to review the quorum configuration after the cluster is created, before placing the cluster into production. To view the detailed cluster quorum configuration, you can use the Validate a Configuration Wizard, or the Test-Cluster Windows PowerShell cmdlet, to run the **Validate Quorum Configuration** test. In Failover Cluster Manager, the basic quorum configuration is displayed in the summary information for the selected cluster, or you can review the information about quorum resources that returns

when you run the Get-ClusterQuorum Windows PowerShell cmdlet.

At any time, you can run the **Validate Quorum Configuration** test to validate that the quorum configuration is optimal for your cluster. The test output indicates if a change to the quorum configuration is recommended and the settings that are optimal. If a change is recommended, you can use the Configure Cluster Quorum Wizard to apply the recommended settings.

After the cluster is in production, do not change the quorum configuration unless you have determined that the change is appropriate for your cluster. You might want to consider changing the quorum configuration in the following situations:

- Adding or evicting nodes
- Adding or removing storage
- A long-term node or witness failure
- Recovering a cluster in a multisite disaster recovery scenario

For more information about validating a failover cluster, see Validate Hardware for a Failover Cluster.

Configure the cluster quorum

You can configure the cluster quorum settings by using Failover Cluster Manager or the FailoverClusters Windows PowerShell cmdlets.

> **IMPORTANT**
>
> It is usually best to use the quorum configuration that is recommended by the Configure Cluster Quorum Wizard. We recommend customizing the quorum configuration only if you have determined that the change is appropriate for your cluster. For more information, see General recommendations for quorum configuration in this topic.

Configure the cluster quorum settings

Membership in the local **Administrators** group on each clustered server, or equivalent, is the minimum permissions required to complete this procedure. Also, the account you use must be a domain user account.

> **NOTE**
>
> You can change the cluster quorum configuration without stopping the cluster or taking cluster resources offline.

Change the quorum configuration in a failover cluster by using Failover Cluster Manager

1. In Failover Cluster Manager, select or specify the cluster that you want to change.
2. With the cluster selected, under **Actions**, select **More Actions**, and then select **Configure Cluster Quorum Settings**. The Configure Cluster Quorum Wizard appears. Select **Next**.
3. On the **Select Quorum Configuration Option** page, select one of the three configuration options and complete the steps for that option. Before you configure the quorum settings, you can review your choices. For more information about the options, see Understanding quorum, earlier in this topic.
   - To allow the cluster to automatically reset the quorum settings that are optimal for your current cluster configuration, select **Use default quorum configuration** and then complete the wizard.
   - To add or change the quorum witness, select **Select the quorum witness**, and then complete the following steps. For information and considerations about configuring a quorum witness, see Witness configuration earlier in this topic.
     a. On the **Select Quorum Witness** page, select an option to configure a disk witness or a file

share witness. The wizard indicates the witness selection options that are recommended for your cluster.

> **NOTE**
> You can also select **Do not configure a quorum witness** and then complete the wizard. If you have an even number of voting nodes in your cluster, this may not be a recommended configuration.

b. If you select the option to configure a disk witness, on the **Configure Storage Witness** page, select the storage volume that you want to assign as the disk witness, and then complete the wizard.

c. If you select the option to configure a file share witness, on the **Configure File Share Witness** page, type or browse to a file share that will be used as the witness resource, and then complete the wizard.

d. If you select the option to configure a cloud witness, on the **Configure Cloud Witness** page, enter your Azure storage account name, Azure storage account key and the Azure service endpoint, and then complete the wizard.

> **NOTE**
> This option is available in Windows Server 2016 and above.

- To configure quorum management settings and to add or change the quorum witness, select **Advanced quorum configuration**, and then complete the following steps. For information and considerations about the advanced quorum configuration settings, see Node vote assignment and Dynamic quorum management earlier in this topic.

a. On the **Select Voting Configuration** page, select an option to assign votes to nodes. By default, all nodes are assigned a vote. However, for certain scenarios, you can assign votes only to a subset of the nodes.

> **NOTE**
> You can also select **No Nodes**. This is generally not recommended, because it does not allow nodes to participate in quorum voting, and it requires configuring a disk witness. This disk witness becomes the single point of failure for the cluster.

b. On the **Configure Quorum Management** page, you can enable or disable the **Allow cluster to dynamically manage the assignment of node votes** option. Selecting this option generally increases the availability of the cluster. By default the option is enabled, and it is strongly recommended to not disable this option. This option allows the cluster to continue running in failure scenarios that are not possible when this option is disabled.

> **NOTE**
> This option is not present in Windows Server 2016 and above.

c. On the **Select Quorum Witness** page, select an option to configure a disk witness, file share witness or a cloud witness. The wizard indicates the witness selection options that are recommended for your cluster.

> **NOTE**
> You can also select **Do not configure a quorum witness**, and then complete the wizard. If you have an even number of voting nodes in your cluster, this may not be a recommended configuration.

d. If you select the option to configure a disk witness, on the **Configure Storage Witness** page, select the storage volume that you want to assign as the disk witness, and then complete the wizard.

e. If you select the option to configure a file share witness, on the **Configure File Share Witness** page, type or browse to a file share that will be used as the witness resource, and then complete the wizard.

f. If you select the option to configure a cloud witness, on the **Configure Cloud Witness** page, enter your Azure storage account name, Azure storage account key and the Azure service endpoint, and then complete the wizard.

> **NOTE**
> This option is available in Windows Server 2016 and above.

4. Select **Next**. Confirm your selections on the confirmation page that appears, and then select **Next**.

After the wizard runs and the **Summary** page appears, if you want to view a report of the tasks that the wizard performed, select **View Report**. The most recent report will remain in the *systemroot***Cluster\Reports** folder with the name **QuorumConfiguration.mht**.

> **NOTE**
> After you configure the cluster quorum, we recommend that you run the **Validate Quorum Configuration** test to verify the updated quorum settings.

Windows PowerShell equivalent commands

The following examples show how to use the Set-ClusterQuorum cmdlet and other Windows PowerShell cmdlets to configure the cluster quorum.

The following example changes the quorum configuration on cluster *CONTOSO-FC1* to a simple node majority configuration with no quorum witness.

```
Set-ClusterQuorum –Cluster CONTOSO-FC1 -NodeMajority
```

The following example changes the quorum configuration on the local cluster to a node majority with witness configuration. The disk resource named *Cluster Disk 2* is configured as a disk witness.

```
Set-ClusterQuorum -NodeAndDiskMajority "Cluster Disk 2"
```

The following example changes the quorum configuration on the local cluster to a node majority with witness configuration. The file share resource named *\\CONTOSO-FS\fsw* is configured as a file share witness.

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\fileserver\fsw"
```

The following example removes the quorum vote from node *ContosoFCNode1* on the local cluster.

```
(Get-ClusterNode ContosoFCNode1).NodeWeight=0
```

The following example adds the quorum vote to node *ContosoFCNode1* on the local cluster.

```
(Get-ClusterNode ContosoFCNode1).NodeWeight=1
```

The following example enables the **DynamicQuorum** property of the cluster *CONTOSO-FC1* (if it was previously disabled):

```
(Get-Cluster CONTOSO-FC1).DynamicQuorum=1
```

Recover a cluster by starting without quorum

A cluster that does not have enough quorum votes will not start. As a first step, you should always confirm the cluster quorum configuration and investigate why the cluster no longer has quorum. This might happen if you have nodes that stopped responding, or if the primary site is not reachable in a multisite cluster. After you identify the root cause for the cluster failure, you can use the recovery steps described in this section.

> **NOTE**
> - If the Cluster service stops because quorum is lost, Event ID 1177 appears in the system log.
> - It is always necessary to investigate why the cluster quorum was lost.
> - It is always preferable to bring a node or quorum witness to a healthy state (join the cluster) rather than starting the cluster without quorum.

Force start cluster nodes

After you determine that you cannot recover your cluster by bringing the nodes or quorum witness to a healthy state, forcing your cluster to start becomes necessary. Forcing the cluster to start overrides your cluster quorum configuration settings and starts the cluster in **ForceQuorum** mode.

Forcing a cluster to start when it does not have quorum may be especially useful in a multisite cluster. Consider a disaster recovery scenario with a cluster that contains separately located primary and backup sites, *SiteA* and *SiteB*. If there is a genuine disaster at *SiteA*, it could take a significant amount of time for the site to come back online. You would likely want to force *SiteB* to come online, even though it does not have quorum.

When a cluster is started in **ForceQuorum** mode, and after it regains sufficient quorum votes, the cluster automatically leaves the forced state, and it behaves normally. Hence, it is not necessary to start the cluster again normally. If the cluster loses a node and it loses quorum, it goes offline again because it is no longer in the forced state. To bring it back online when it does not have quorum requires forcing the cluster to start without quorum.

> **IMPORTANT**
> - After a cluster is force started, the administrator is in full control of the cluster.
> - The cluster uses the cluster configuration on the node where the cluster is force started, and replicates it to all other nodes that are available.
> - If you force the cluster to start without quorum, all quorum configuration settings are ignored while the cluster remains in **ForceQuorum** mode. This includes specific node vote assignments and dynamic quorum management settings.

Prevent quorum on remaining cluster nodes

After you have force started the cluster on a node, it is necessary to start any remaining nodes in your cluster with a setting to prevent quorum. A node started with a setting that prevents quorum indicates to the Cluster service to join an existing running cluster instead of forming a new cluster instance. This prevents the remaining nodes from forming a split cluster that contains two competing instances.

This becomes necessary when you need to recover your cluster in some multisite disaster recovery scenarios after you have force started the cluster on your backup site, *SiteB*. To join the force started cluster in *SiteB*, the nodes in your primary site, *SiteA*, need to be started with the quorum prevented.

> **IMPORTANT**
> After a cluster is force started on a node, we recommend that you always start the remaining nodes with the quorum prevented.

Here's how to recover the cluster with Failover Cluster Manager:

1. In Failover Cluster Manager, select or specify the cluster you want to recover.
2. With the cluster selected, under **Actions**, select **Force Cluster Start**.

   Failover Cluster Manager force starts the cluster on all nodes that are reachable. The cluster uses the current cluster configuration when starting.

> **NOTE**
> - To force the cluster to start on a specific node that contains a cluster configuration that you want to use, you must use the Windows PowerShell cmdlets or equivalent command-line tools as presented after this procedure.
> - If you use Failover Cluster Manager to connect to a cluster that is force started, and you use the **Start Cluster Service** action to start a node, the node is automatically started with the setting that prevents quorum.

Windows PowerShell equivalent commands (Start-Clusternode)

The following example shows how to use the **Start-ClusterNode** cmdlet to force start the cluster on node *ContosoFCNode1*.

```
Start-ClusterNode -Node ContosoFCNode1 -FQ
```

Alternatively, you can type the following command locally on the node:

```
Net Start ClusSvc /FQ
```

The following example shows how to use the **Start-ClusterNode** cmdlet to start the Cluster service with the quorum prevented on node *ContosoFCNode1*.

```
Start-ClusterNode -Node ContosoFCNode1 -PQ
```

Alternatively, you can type the following command locally on the node:

```
Net Start ClusSvc /PQ
```

Quorum considerations for disaster recovery configurations

This section summarizes characteristics and quorum configurations for two multisite cluster configurations in disaster recovery deployments. The quorum configuration guidelines differ depending on if you need automatic failover or manual failover for workloads between the sites. Your configuration usually depends on the service level agreements (SLAs) that are in place in your organization to provide and support clustered workloads in the event of a failure or disaster at a site.

Automatic failover

In this configuration, the cluster consists of two or more sites that can host clustered roles. If a failure occurs at any site, the clustered roles are expected to automatically fail over to the remaining sites. Therefore, the cluster quorum must be configured so that any site can sustain a complete site failure.

The following table summarizes considerations and recommendations for this configuration.

ITEM	DESCRIPTION
Number of node votes per site	Should be equal
Node vote assignment	Node votes should not be removed because all nodes are equally important
Dynamic quorum management	Should be enabled
Witness configuration	File share witness is recommended, configured in a site that is separate from the cluster sites
Workloads	Workloads can be configured on any of the sites

Additional considerations for automatic failover

- Configuring the file share witness in a separate site is necessary to give each site an equal opportunity to survive. For more information, see Witness configuration earlier in this topic.

Manual failover

In this configuration, the cluster consists of a primary site, *SiteA*, and a backup (recovery) site, *SiteB*. Clustered roles are hosted on *SiteA*. Because of the cluster quorum configuration, if a failure occurs at all nodes in *SiteA*, the cluster stops functioning. In this scenario the administrator must manually fail over the cluster services to *SiteB* and perform additional steps to recover the cluster.

The following table summarizes considerations and recommendations for this configuration.

ITEM	DESCRIPTION
Number of node votes per site	• Node votes should not be removed from nodes at the primary site, **SiteA** • Node votes should be removed from nodes at the backup site, **SiteB** • If a long-term outage occurs at **SiteA**, votes must be assigned to nodes at **SiteB** to enable a quorum majority at that site as part of recovery
Dynamic quorum management	Should be enabled

ITEM	DESCRIPTION
Witness configuration	• Configure a witness if there is an even number of nodes at **SiteA** • If a witness is needed, configure either a file share witness or a disk witness that is accessible only to nodes in **SiteA** (sometimes called an asymmetric disk witness)
Workloads	Use preferred owners to keep workloads running on nodes at **SiteA**

Additional considerations for manual failover

- Only the nodes at *SiteA* are initially configured with quorum votes. This is necessary to ensure that the state of nodes at *SiteB* does not affect the cluster quorum.
- Recovery steps can vary depending on if *SiteA* sustains a temporary failure or a long-term failure.

More information

- Failover Clustering
- Failover Clusters Windows PowerShell cmdlets

Deploy a Cloud Witness for a Failover Cluster

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Cloud Witness is a type of Failover Cluster quorum witness that uses Microsoft Azure to provide a vote on cluster quorum. This topic provides an overview of the Cloud Witness feature, the scenarios that it supports, and instructions about how to configure a cloud witness for a Failover Cluster. For more information, see Set up a cluster witness.

Cloud Witness overview

The following figure illustrates a multi-site stretched Failover Cluster quorum configuration with Windows Server 2016. In this example configuration (figure 1), there are 2 nodes in 2 datacenters (referred to as Sites). Note, it is possible for a cluster to span more than 2 datacenters. Also, each datacenter can have more than 2 nodes. A typical cluster quorum configuration in this setup (automatic failover SLA) gives each node a vote. One extra vote is given to the quorum witness to allow cluster to keep running even if either one of the datacenter experiences a power outage. The math is simple - there are 5 total votes and you need 3 votes for the cluster to keep it running.

Using a File Share Witness as a quorum witness

If there is a power outage in one datacenter, to give equal opportunity for the cluster in other datacenter to keep it running, it is recommended to host the quorum witness in a location other than the two datacenters. This typically means requiring a third separate datacenter (site) to host a File Server that is backing the File Share, which is used as the quorum witness (File Share Witness).

Most organizations do not have a third separate datacenter that will host File Server backing the File Share Witness. This means organizations primarily host the File Server in one of the two datacenters, which by extension, makes that datacenter the primary datacenter. In a scenario where there is power outage in the primary datacenter, the cluster would go down as the other datacenter would only have 2 votes which is below the quorum majority of 3 votes needed. For the customers that have third separate datacenter to host the File Server, it is an overhead to maintain the highly available File Server backing the File Share Witness. Hosting virtual machines in the public cloud that have the File Server for File Share Witness running in Guest OS is a significant overhead in terms of both setup and maintenance.

Cloud Witness is a new type of Failover Cluster quorum witness that uses Microsoft Azure as the arbitration point (see the following figure). It uses Azure Blob Storage to read/write a blob file which is then used as an arbitration point in case of split-brain resolution.

There are significant benefits which this approach:

- Uses Microsoft Azure (no need for third separate datacenter).
- Uses standard available Azure Blob Storage (no extra maintenance overhead of virtual machines hosted in public cloud).
- Same Azure Storage Account can be used for multiple clusters (one blob file per cluster; cluster unique ID used as blob file name).
- Low on-going $cost to the Storage Account (small data written per blob file, blob file updated only once when cluster nodes' state changes).
- Built-in Cloud Witness resource type.

Multi-site stretched clusters with Cloud Witness as a quorum witness

As shown in the preceding figure, there is no third separate site that is required. Cloud Witness, like any other quorum witness, gets a vote and can participate in quorum calculations.

Cloud Witness: Supported scenarios for single witness type

If you have a Failover Cluster deployment, where all nodes can reach the internet (by extension of Azure), it is recommended that you configure a Cloud Witness as your quorum witness resource.

Some of the scenarios that are supported use of Cloud Witness as a quorum witness are as follows:

- Disaster recovery stretched multi-site clusters (see preceding figure).
- Failover Clusters without shared storage (SQL Always On etc.).
- Failover Clusters running inside Guest OS hosted in Microsoft Azure Virtual Machine Role (or any other public cloud).
- Failover Clusters running inside Guest OS of Virtual Machines hosted in private clouds.
- Storage clusters with or without shared storage, such as Scale-out File Server clusters.
- Small branch-office clusters (even 2-node clusters)

Starting with Windows Server 2012 R2, it is recommended to always configure a witness as the cluster automatically manages the witness vote and the nodes vote with Dynamic Quorum.

Set up a Cloud Witness for a cluster

To set up a Cloud Witness as a quorum witness for your cluster, complete the following steps:

1. Create an Azure Storage Account to use as a Cloud Witness
2. Configure the Cloud Witness as a quorum witness for your cluster.

Create an Azure Storage Account to use as a Cloud Witness

This section describes how to create a storage account and view and copy endpoint URLs and access keys for that account.

To configure Cloud Witness, you must have a valid Azure general purpose Storage Account which can be used to store the blob file (used for arbitration). Cloud Witness creates a well-known Container **msft-cloud-witness** under the Microsoft Storage Account. Cloud Witness writes a single blob file with corresponding cluster's unique ID used as the file name of the blob file under this **msft-cloud-witness** container. This means that you can use the same Microsoft Azure Storage Account to configure a Cloud Witness for multiple different clusters.

When you use the same Azure Storage Account for configuring Cloud Witness for multiple different clusters, a single **msft-cloud-witness** container gets created automatically. This container will contain one-blob file per cluster.

To create an Azure storage account

1. Sign in to the Azure portal.
2. On the Hub menu, select New -> Data + Storage -> Storage account.
3. In the Create a storage account page, do the following:
   a. Enter a name for your storage account.
      Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only. The storage account name must also be unique within Azure.

   b. For **Account kind**, select **General purpose**.
      You can't use a Blob storage account for a Cloud Witness.

   c. For **Performance**, select **Standard**.
      You can't use Azure Premium Storage for a Cloud Witness.

   d. For **Replication**, select **Locally-redundant storage (LRS)** or **Zone-redundant storage (ZRS)** as applicable.
      Failover Clustering uses the blob file as the arbitration point, which requires some consistency guarantees when reading the data. Therefore, you must select **Locally-redundant storage** for **Replication** type when the Cloud Witness is for a cluster that resides on premises, or it's a cluster in Azure which isn't deployed across different availability zones in the same region. When the cluster nodes are in the same region but different availability zone, use **Zone-redundant storage** as **Replication** type.

View and copy storage access keys for your Azure Storage Account

When you create a Microsoft Azure Storage Account, it is associated with two Access Keys that are automatically generated - Primary Access key and Secondary Access key. For a first-time creation of Cloud Witness, use the **Primary Access Key**. There is no restriction regarding which key to use for Cloud Witness.

To view and copy storage access keys

In the Azure portal, navigate to your storage account, click **All settings** and then click **Access Keys** to view, copy, and regenerate your account access keys. The Access Keys blade also includes pre-configured connection strings using your primary and secondary keys that you can copy to use in your applications (see figure 4).

Figure 4: Storage Access Keys

View and copy endpoint URL Links

When you create a Storage Account, the following URLs are generated using the format:

```
https://<Storage Account Name>.<Storage Type>.<Endpoint>
```

Cloud Witness always uses **Blob** as the file storage type in a general purpose storage account. Azure uses **.core.windows.net** as the Endpoint. When configuring Cloud Witness, it is possible that you configure it with a different endpoint as per your scenario (for example the Microsoft Azure datacenter in China has a different endpoint).

> **NOTE**
>
> The endpoint URL is generated automatically by the Cloud Witness resource. Make sure that port 443 is open in your firewalls and that `*.core.windows.net` is included in any firewall allow lists you're using between the cluster and Azure Storage.

To view and copy endpoint URL links

In the Azure portal, navigate to your storage account, click **All settings** and then click **Properties** to view and copy your endpoint URLs (see figure 5).

Figure 5: Cloud Witness endpoint URL links

For more information about creating and managing Azure Storage Accounts, see About Azure Storage Accounts

Configure Cloud Witness as a quorum witness for your cluster

Cloud Witness configuration is well integrated within the existing Quorum Configuration Wizard built into the Failover Cluster Manager.

To configure Cloud Witness as a Quorum Witness

1. Launch Failover Cluster Manager.
2. Right-click the cluster -> **More Actions** -> **Configure Cluster Quorum Settings** (see figure 6). This launches the Configure Cluster Quorum wizard.

Figure 6. Cluster Quorum Settings

3. On the **Select Quorum Configurations** page, select **Select the quorum witness** (see figure 7).

Figure 7. Select the Quorum Configuration

4. On the **Select Quorum Witness** page, select **Configure a cloud witness** (see figure 8).

Figure 8. Select the Quorum Witness

5. On the **Configure Cloud Witness** page, enter the following information:

   a. (Required parameter) Azure Storage Account Name.

   b. (Required parameter) Access Key corresponding to the Storage Account.

      a. When creating for the first time, use Primary Access Key.
      b. When rotating the Primary Access Key, use Secondary Access Key.

   c. (Optional parameter) If you intend to use a different Azure service endpoint (for example the Microsoft Azure service in China), then update the endpoint server name.

Figure 9: Configure your Cloud Witness

6. Upon successful configuration of Cloud Witness, you can view the newly created witness resource in the

Failover Cluster Manager snap-in (see figure 10).

Figure 10: Successful configuration of Cloud Witness

Configuring Cloud Witness using PowerShell

The existing Set-ClusterQuorum PowerShell command has new additional parameters corresponding to Cloud Witness.

You can configure Cloud Witness with the cmdlet `Set-ClusterQuorum` using the following PowerShell command:

```
Set-ClusterQuorum -CloudWitness -AccountName <StorageAccountName> -AccessKey <StorageAccountAccessKey>
```

In case you need to use a different endpoint (rare):

```
Set-ClusterQuorum -CloudWitness -AccountName <StorageAccountName> -AccessKey <StorageAccountAccessKey> -
Endpoint <servername>
```

Azure Storage Account considerations with Cloud Witness

When configuring a Cloud Witness as a quorum witness for your Failover Cluster, consider the following:

- Instead of storing the Access Key, your Failover Cluster will generate and securely store a Shared Access Security (SAS) token.
- The generated SAS token is valid as long as the Access Key remains valid. When rotating the Primary Access Key, it is important to first update the Cloud Witness (on all your clusters that are using that Storage Account) with the Secondary Access Key before regenerating the Primary Access Key.
- Cloud Witness uses HTTPS REST interface of the Azure Storage Account service. This means it requires the HTTPS port to be open on all cluster nodes.

Proxy considerations with Cloud Witness

Cloud Witness uses HTTPS (default port 443) to establish outbound communication with the Azure blob service. Ensure that the HTTPS outbound port is accessible via network Proxy. Azure uses **.core.windows.net** as the Endpoint. You need to ensure that it is included in any firewall allow lists you're using between the cluster and Azure Storage.

See Also

- What's New in Failover Clustering in Windows Server

Deploy a file share witness

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

A file share witness is an SMB share that Failover Cluster uses as a vote in the cluster quorum. This topic provides an overview of the technology and the new functionality in Windows Server 2019, including using a USB drive connected to a router as a file share witness.

File share witnesses are handy in the following circumstances:

- A cloud witness can't be used because not all servers in the cluster have a reliable Internet connection
- A disk witness can't be used because there aren't any shared drives to use for a disk witness. This could be a Storage Spaces Direct cluster, SQL Server Always On Availability Groups (AG), Exchange Database Availability Group (DAG), etc. None of these types of clusters use shared disks.

File share witness requirements

You can host a file share witness on a domain-joined Windows server, or if your cluster is running Windows Server 2019, any device that can host an SMB 2 or later file share.

FILE SERVER TYPE	SUPPORTED CLUSTERS
Any device w/an SMB 2 file share	Windows Server 2019
Domain-joined Windows Server	Windows Server 2008 and later

If the cluster is running Windows Server 2019, here are the requirements:

- An SMB file share *on any device that uses the SMB 2 or later protocol*, including:
  - Network-attached storage (NAS) devices
  - Windows computers joined to a workgroup
  - Routers with locally-connected USB storage
- A local account on the device for authenticating the cluster
- If you're instead using Active Directory for authenticating the cluster with the file share, the Cluster Name Object (CNO) must have write permissions on the share, and the server must be in the same Active Directory forest as the cluster
- The file share has a minimum of 5 MB of free space

If the cluster is running Windows Server 2016 or earlier, here are the requirements:

- SMB file share *on a Windows server joined to the same Active Directory forest as the cluster*
- The Cluster Name Object (CNO) must have write permissions on the share
- The file share has a minimum of 5 MB of free space

Other notes:

- To use a file share witness hosted by devices other than a domain-joined Windows server, you currently must use the **Set-ClusterQuorum -Credential** PowerShell cmdlet to set the witness, as described later in this

topic.

- For high availability, you can use a file share witness on a separate Failover Cluster
- The file share can be used by multiple clusters
- The use of a Distributed File System (DFS) share or replicated storage is not supported with any version of failover clustering. These can cause a split brain situation where clustered servers are running independently of each other and could cause data loss.

Creating a file share witness on a router with a USB device

At Microsoft Ignite 2018, DataOn Storage had a Storage Spaces Direct Cluster in their kiosk area. This cluster was connected to a NetGear Nighthawk X4S WiFi Router using the USB port as a file share witness similar to this.

The steps for creating a file share witness using a USB device on this particular router are listed below. Note that steps on other routers and NAS appliances will vary and should be accomplished using the vendor supplied directions.

1. Log into the router with the USB device plugged in.

2. From the list of options, select ReadySHARE which is where shares can be created.

3. For a file share witness, a basic share is all that is needed. Selecting the Edit button will pop up a dialog where the share can be created on the USB device.

4. Once selecting the Apply button, the share is created and can be seen in the list.

5. Once the share has been created, creating the file share witness for Cluster is done with PowerShell.

```
Set-ClusterQuorum -FileShareWitness \\readyshare\Witness -Credential (Get-Credential)
```

This displays a dialog box to enter the local account on the device.

These same similar steps can be done on other routers with USB capabilities, NAS devices, or other Windows devices.

Cluster operating system rolling upgrade

12/9/2022 • 15 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Cluster OS Rolling Upgrade enables an administrator to upgrade the operating system of cluster nodes Hyper-V or Scale-Out File Server workloads without stopping them. Using this feature, the downtime penalties against Service Level Agreements (SLA) can be avoided.

Cluster OS Rolling Upgrade provides the following benefits:

- Failover clusters running Hyper-V virtual machine and Scale-out File Server (SOFS) workloads can be upgraded from a version of Windows Server, starting with Windows Server 2012 R2, to a newer version of Windows Server. For example you can upgrade Windows Server 2016 (running on all cluster nodes of the cluster) to Windows Server 2019 (running on all nodes in the cluster) without downtime.
- It doesn't require any additional hardware. In small clusters, you can add additional cluster nodes temporarily to improve availability of the cluster during the Cluster OS Rolling Upgrade process.
- The cluster doesn't need to be stopped or restarted.
- A new cluster is not required. The existing cluster is upgraded. In addition, existing cluster objects stored in Active Directory are used.
- The upgrade process is reversible until the final step, when all cluster nodes are running the newer version of Windows Server and the `Update-ClusterFunctionalLevel` PowerShell cmdlet is run.
- The cluster can support patching and maintenance operations while running in the mixed-OS mode.
- It supports automation via PowerShell and WMI.
- The cluster public property *ClusterFunctionalLevel* property indicates the state of the cluster on Windows Server 2016 and later cluster nodes. This property can be queried using the PowerShell cmdlet from a cluster node that belongs to a failover cluster:

  ```
  Get-Cluster | Select ClusterFunctionalLevel
  ```

  The table below shows the values and each corresponding functional level:

VALUE	FUNCTIONAL LEVEL
8	Windows Server 2012 R2
9	Windows Server 2016
10	Windows Server 2019

This guide describes the various stages of the Cluster OS Rolling Upgrade process, installation steps, feature limitations, and frequently asked questions (FAQs), and is applicable to the following Cluster OS Rolling Upgrade scenarios in Windows Server:

- Hyper-V clusters

- Scale-Out File Server clusters

The following scenario is not supported:

- Cluster OS Rolling Upgrade of guest clusters using virtual hard disk (.vhdx file) as shared storage.

Cluster OS Rolling Upgrade is fully supported by System Center Virtual Machine Manager (SCVMM). If you are using SCVMM, see Perform a rolling upgrade of a Hyper-V host cluster to Windows Server 2016 in VMM for guidance on upgrading the clusters and automating the steps that are described in this document.

Requirements

Complete the following requirements before you begin the Cluster OS Rolling Upgrade process:

- Start with a Failover Cluster running Windows Server 2012 R2 or newer. You can upgrade to the next version, for example from Windows Server 2016 to Windows Server 2019.
- Verify that the Hyper-V nodes have CPUs that support Second-Level Addressing Table (SLAT) using one of the following methods; - Review the Are you SLAT Compatible? WP8 SDK Tip 01 article that describes two methods to check if a CPU supports SLATs - Download the Coreinfo v3.31 tool to determine if a CPU supports SLAT.

Cluster transition states during Cluster OS Rolling Upgrade

This section describes the various transition states of the Windows Server cluster that is being upgraded to the next version of Windows Server using Cluster OS Rolling Upgrade.

In order to keep the cluster workloads running during the Cluster OS Rolling Upgrade process, moving a cluster workload from a node running an older version of Windows Server to a node running a newer version of Windows Server works by using a compatibility mode. This compatibility mode makes the nodes running the newer version of Windows Server appear as if they are running the the same older version of Windows Server. For example, when upgrading a Windows Server 2016 cluster to Windows Server 2019, Windows Server 2019 nodes operate in a Windows Server 2016 compatibility mode as a temporary measure. A new conceptual cluster mode, called *mixed-OS mode*, allows nodes of different versions to exist in the same cluster (see Figure 1).

Figure 1: Cluster operating system state transitions

A Windows Server cluster enters mixed-OS mode when a node running a newer version of Windows Server is added to the cluster. The process is fully reversible at this point - newer Windows Server nodes can be removed from the cluster and nodes running the existing version of Windows Server can be added to the cluster in this mode. The process is not reversible once the `Update-ClusterFunctionalLevel` PowerShell cmdlet is run on the cluster. In order for this cmdlet to succeed, all nodes must be running the newer version of Windows Server, and

all nodes must be online.

Transition states of a four-node cluster while performing Rolling OS Upgrade

This section illustrates and describes the four different stages of a cluster with shared storage whose nodes are upgraded from Windows Server 2012 R2 to Windows Server 2016. The process is the same for later versions of Window Server.

"Stage 1" is the initial state - we start with a Windows Server 2012 R2 cluster.

Figure 2: Initial State: Windows Server 2012 R2 Failover Cluster (Stage 1)

In "Stage 2", two nodes have been paused, drained, evicted, reformatted, and installed with Windows Server 2016.

Figure 3: Intermediate State: Mixed-OS mode: Windows Server 2012 R2 and Windows Server 2016 Failover cluster (Stage 2)

At "Stage 3", all of the nodes in the cluster have been upgraded to Windows Server 2016, and the cluster is ready to be upgraded with `Update-ClusterFunctionalLevel` PowerShell cmdlet.

> **NOTE**
>
> At this stage, the process can be fully reversed, and Windows Server 2012 R2 nodes can be added to this cluster.

Figure 4: Intermediate State: All nodes upgraded to Windows Server 2016, ready for Update-ClusterFunctionalLevel (Stage 3)

After the `Update-ClusterFunctionalLevel` cmdlet is run, the cluster enters "Stage 4", where new Windows Server 2016 cluster features can be used.

Figure 5: Final State: Windows Server 2016 Failover Cluster (Stage 4)

Cluster OS Rolling Upgrade Process

This section describes the workflow for performing Cluster OS Rolling Upgrade.

Figure 6: Cluster OS Rolling Upgrade Process Workflow

Cluster OS Rolling upgrade includes the steps below for upgrading from Windows Server 2012 R2 to Windows Server 2016, however the process is the same for later versions of Window Server.

1. Prepare the cluster for the operating system upgrade as follows:

    a. Cluster OS Rolling Upgrade requires removing one node at a time from the cluster. Check if you have sufficient capacity on the cluster to maintain HA SLAs when one of the cluster nodes is removed from the cluster for an operating system upgrade. In other words, do you require the capability to failover workloads to another node when one node is removed from the cluster during the process of Cluster OS Rolling Upgrade? Does the cluster have the capacity to run the required workloads when one node is removed from the cluster for Cluster OS Rolling Upgrade?

    b. For Hyper-V workloads, check that all Windows Server Hyper-V hosts have CPU support for Second-Level Address Table (SLAT). Only SLAT-capable machines can use the Hyper-V role in Windows Server 2016 and newer.

c. Check that any workload backups have completed, and consider backing-up the cluster. Stop backup operations while adding nodes to the cluster.

d. Check that all cluster nodes are online /running/up using the `Get-ClusterNode` cmdlet (see Figure 7).

Figure 7: Determining node status using Get-ClusterNode cmdlet

e. If you are running Cluster Aware Updates (CAU), verify if CAU is currently running by using the **Cluster-Aware Updating** UI, or the `Get-CauRun` cmdlet (see Figure 8). Stop CAU using the `Disable-CauClusterRole` cmdlet (see Figure 9) to prevent any nodes from being paused and drained by CAU during the Cluster OS Rolling Upgrade process.

Figure 8: Using the `Get-CauRun` cmdlet to determine if Cluster Aware Updates is running on the cluster

Figure 9: Disabling the Cluster Aware Updates role using the `Disable-CauClusterRole` cmdlet

2. For each node in the cluster, complete the following:

a. Using Cluster Manager UI, select a node and use the **Pause | Drain** menu option to drain the node (see Figure 10) or use the `Suspend-ClusterNode` cmdlet (see Figure 11).

Figure 10: Draining roles from a node using Failover Cluster Manager

Figure 11: Draining roles from a node using the `Suspend-ClusterNode` cmdlet

b. Using Cluster Manager UI, **Evict** the paused node from cluster, or use the `Remove-ClusterNode` cmdlet.

Figure 12: Remove a node from the cluster using `Remove-ClusterNode` cmdlet

c. Reformat the system drive and perform a "clean operating system install" of Windows Server 2016 on the node using the **Custom: Install Windows only (advanced)** installation (See Figure 13) option in setup.exe. Avoid selecting the **Upgrade: Install Windows and keep files, settings, and applications** option since Cluster OS Rolling Upgrade doesn't encourage in-place upgrade.

Figure 13: Available installation options for Windows Server 2016

d. Add the node to the appropriate Active Directory domain.

e. Add the appropriate users to the Administrators group.

f. Using the Server Manager UI or Install-WindowsFeature PowerShell cmdlet, install any server roles that you need, such as Hyper-V.

```
Install-WindowsFeature -Name Hyper-V
```

g. Using the Server Manager UI or Install-WindowsFeature PowerShell cmdlet, install the Failover

Clustering feature.

```
Install-WindowsFeature -Name Failover-Clustering
```

h. Install any additional features needed by your cluster workloads.

i. Check network and storage connectivity settings using the Failover Cluster Manager UI.

j. If Windows Firewall is used, check that the Firewall settings are correct for the cluster. For example, Cluster Aware Updating (CAU) enabled clusters may require Firewall configuration.

k. For Hyper-V workloads, use the Hyper-V Manger UI to launch the Virtual Switch Manager dialog (see Figure 14).

   Check that the name of the Virtual Switch(s) used are identical for all Hyper-V host nodes in the cluster.

Figure 14: Virtual Switch Manager

l. On a Windows Server 2016 node (do not use a Windows Server 2012 R2 node), use the Failover Cluster Manager (see Figure 15) to connect to the cluster.

Figure 15: Adding a node to the cluster using Failover Cluster Manager

m. Use either the Failover Cluster Manager UI or the `Add-ClusterNode` cmdlet (see Figure 16) to add the node to the cluster.

Figure 16: Adding a node to the cluster using `Add-ClusterNode` cmdlet

> **NOTE**
>
> When the first Windows Server 2016 node joins the cluster, the cluster enters "Mixed-OS" mode, and the cluster core resources are moved to the Windows Server 2016 node. A "Mixed-OS" mode cluster is a fully functional cluster where the new nodes run in a compatibility mode with the old nodes. "Mixed-OS" mode is a transitory mode for the cluster. It is not intended to be permanent and customers are expected to update all nodes of their cluster within four weeks.

n. After the Windows Server 2016 node is successfully added to the cluster, you can (optionally) move some of the cluster workload to the newly added node in order to rebalance the workload across the cluster as follows:

Figure 17: Moving a cluster workload (cluster VM role) using `Move-ClusterVirtualMachineRole` cmdlet

a. Use **Live Migration** from the Failover Cluster Manager for virtual machines or the `Move-ClusterVirtualMachineRole` cmdlet (see Figure 17) to perform a live migration of the virtual machines.

```
Move-ClusterVirtualMachineRole -Name VM1 -Node robhind-host3
```

b. Use **Move** from the Failover Cluster Manager or the `Move-ClusterGroup` cmdlet for other cluster workloads.

3. When every node has been upgraded to Windows Server 2016 and added back to the cluster, or when any remaining Windows Server 2012 R2 nodes have been evicted, do the following:

> **IMPORTANT**
>
> - After you update the cluster functional level, you cannot go back to Windows Server 2012 R2 functional level and Windows Server 2012 R2 nodes cannot be added to the cluster.
> - Until the `Update-ClusterFunctionalLevel` cmdlet is run, the process is fully reversible and Windows Server 2012 R2 nodes can be added to this cluster and Windows Server 2016 nodes can be removed.
> - After the `Update-ClusterFunctionalLevel` cmdlet is run, new features will be available.

a. Using the Failover Cluster Manager UI or the `Get-ClusterGroup` cmdlet, check that all cluster roles are running on the cluster as expected. In the following example, Available Storage is not being used, instead CSV is used, hence, Available Storage displays an **Offline** status (see Figure 18).

Figure 18: Verifying that all cluster groups (cluster roles) are running using the `Get-ClusterGroup` cmdlet

b. Check that all cluster nodes are online and running using the `Get-ClusterNode` cmdlet.

c. Run the `Update-ClusterFunctionalLevel` cmdlet - no errors should be returned (see Figure 19).

Figure 19: Updating the functional level of a cluster using PowerShell

d. After the `Update-ClusterFunctionalLevel` cmdlet is run, new features are available.

4. Resume normal cluster updates and backups:

   a. If you were previously running CAU, restart it using the CAU UI or use the `Enable-CauClusterRole` cmdlet (see Figure 20).

Figure 20: Enable Cluster Aware Updates role using the `Enable-CauClusterRole` cmdlet

   b. Resume backup operations.

5. Enable and use the Windows Server 2016 features on Hyper-V Virtual Machines.

   a. After the cluster has been upgraded to Windows Server 2016 functional level, many workloads like Hyper-V VMs will have new capabilities. For a list of new Hyper-V capabilities. see Migrate and upgrade virtual machines

   b. On each Hyper-V host node in the cluster, use the `Get-VMHostSupportedVersion` cmdlet to view the Hyper-V VM configuration versions that are supported by the host.

Figure 21: Viewing the Hyper-V VM configuration versions supported by the host

   c. On each Hyper-V host node in the cluster, Hyper-V VM configuration versions can be upgraded by scheduling a brief maintenance window with users, backing up, turning off virtual machines, and running the `Update-VMVersion` cmdlet (see Figure 22). This will update the virtual machine version, and enable new Hyper-V features, eliminating the need for future Hyper-V Integration Component (IC) updates. This cmdlet can be run from the Hyper-V node that is hosting the VM, or the `-ComputerName` parameter can be used to update the VM Version remotely. In this example, here we upgrade the configuration version of VM1 from 5.0 to 7.0 to take advantage of many new Hyper-V features associated with this VM configuration version such as Production Checkpoints (Application Consistent backups), and binary VM configuration file.

```
Administrator: Windows PowerShell
PS C:\> Stop-VM -Save -Name Blue-VM1
PS C:\> Stop-VM -TurnOff -Name Blue-VM1
PS C:\> Get-VM

Name     State CPUUsage(%) MemoryAssigned(M) Uptime   Status             Version
----     ----- ----------- ----------------- ------   ------             -------
Blue-VM1 Off   0           0                 00:00:00 Operating normally 5.0


PS C:\> Update-VMVersion -Name Blue-VM1

Confirm
Are you sure you want to perform this action?
Performing a configuration version update of "Blue-VM1" will prevent it from being migrated to or imported on previous
versions of Windows. This operation is not reversible.

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\> Get-VM

Name     State CPUUsage(%) MemoryAssigned(M) Uptime   Status             Version
----     ----- ----------- ----------------- ------   ------             -------
Blue-VM1 Off   0           0                 00:00:00 Operating normally 7.0


PS C:\> Start-VM -Name Blue-VM1
PS C:\> _
```

Figure 22: Upgrading a VM version using the Update-VMVersion PowerShell cmdlet

6. Storage pools can be upgraded using the Update-StoragePool PowerShell cmdlet - this is an online operation.

Although we are targeting Private Cloud scenarios, specifically Hyper-V and Scale-out File Server clusters, which can be upgraded without downtime, the Cluster OS Rolling Upgrade process can be used for any cluster role.

Restrictions / Limitations

- This feature works only for versions of Windows Server starting with Windows Server 2012 R2. This feature cannot upgrade earlier versions of Windows Server such as Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012.
- Each Windows Server 2016 node should be reformatted/new installation only. *In-place* or *upgrade* installation types are discouraged.
- A node running the newer version of Windows Server must be used to add the new nodes to the cluster.
- When managing a mixed-OS mode cluster, always perform the management tasks from an up-level node that is running Windows Server 2016. Downlevel Windows Server nodes cannot use UI or management tools against newer versions of Windows Server.
- We encourage customers to move through the cluster upgrade process quickly because some cluster features are not optimized for mixed-OS mode.
- Avoid creating or resizing storage on newer Windows Server nodes while the cluster is running in mixed-OS mode because of possible incompatibilities on failover from a newer Windows Server node to down-level Windows Server nodes.

Frequently asked questions

How long can the failover cluster run in mixed-OS mode? We encourage customers to complete the upgrade within four weeks. We have successfully upgraded Hyper-V and Scale-out File Server clusters with zero downtime in less than four hours total.

Will you port this feature back to Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008? We do not have any plans to port this feature back to previous versions. Cluster OS Rolling Upgrade is our vision for upgrading Windows Server clusters.

Do the nodes running the older Windows Server version need to have all the software updates installed before starting the Cluster OS Rolling Upgrade process? Yes, before starting the Cluster OS Rolling Upgrade process, verify that all cluster nodes are updated with the latest software updates.

Can I run the `Update-ClusterFunctionalLevel` cmdlet while nodes are Off or Paused? No. All cluster nodes

must be on and in active membership for the `Update-ClusterFunctionalLevel` cmdlet to work.

Does Cluster OS Rolling Upgrade work for any cluster workload? Does it work for SQL Server? Yes, Cluster OS Rolling Upgrade works for any cluster workload. However, it is only zero-downtime for Hyper-V and Scale-out File Server clusters. Most other workloads incur some downtime (typically a couple of minutes) when they failover, and failover is required at least once during the Cluster OS Rolling Upgrade process.

Can I automate this process using PowerShell? Yes, we have designed Cluster OS Rolling Upgrade to be automated using PowerShell.

For a large cluster that has extra failover capacity, can I upgrade multiple nodes simultaneously? Yes. When one node is removed from the cluster to upgrade the OS, the cluster will have one less node for failover, hence will have a reduced failover capacity. For large clusters with enough workload and failover capacity, multiple nodes can be upgraded simultaneously. You can temporarily add cluster nodes to the cluster to provide improved workload and failover capacity during the Cluster OS Rolling Upgrade process.

What if I discover an issue in my cluster after `Update-ClusterFunctionalLevel` has been run successfully? If you have backed-up the cluster database with a System State backup before running `Update-ClusterFunctionalLevel`, you should be able to perform an Authoritative restore on a node running the previous version of Windows Server and restore the original cluster database and configuration.

Can I use in-place upgrade for each node instead of using clean-OS install by reformatting the system drive? We do not encourage the use of in-place upgrade of Windows Server, but we are aware that it works in some cases where default drivers are used. Please carefully read all warning messages displayed during in-place upgrade of a cluster node.

If I am using Hyper-V replication for a Hyper-V VM on my Hyper-V cluster, will replication remain intact during and after the Cluster OS Rolling Upgrade process? Yes, Hyper-V replica remains intact during and after the Cluster OS Rolling Upgrade process.

Can I use System Center Virtual Machine Manager (SCVMM) to automate the Cluster OS Rolling Upgrade process? Yes, you can automate the Cluster OS Rolling Upgrade process using VMM in System Center.

Upgrading Failover Clusters on the same hardware

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service.

This guide describes the steps for upgrading the cluster nodes to Windows Server 2019 or Windows Server 2016 from an earlier version using the same hardware.

Overview

Upgrading the operating system on an existing failover cluster is only supported when going from Windows Server 2016 to Windows 2019. If the failover cluster is running an earlier version, such as Windows Server 2012 R2 and earlier, upgrading while the cluster services are running will not allow joining nodes together. If using the same hardware, steps can be taken to get it to the newer version.

Before any upgrade of your failover cluster, please consult the Windows Server upgrade content. When you upgrade a Windows Server in-place, you move from an existing operating system release to a more recent release while staying on the same hardware. Windows Server can be upgraded in-place at least one, and sometimes two versions forward. For example, Windows Server 2012 R2 and Windows Server 2016 can be upgraded in-place to Windows Server 2019. Also keep in mind that the Cluster Migration Wizard can be used but is only supported up to two versions back. The following graphic shows the upgrade paths for Windows Server. Downward pointing arrows represent the supported upgrade path moving from earlier versions up to Windows Server 2019.

The following steps are an example of going from a Windows Server 2012 failover cluster server to Windows Server 2019 using the same hardware.

Before starting any upgrade, please ensure a current backup, including system state, has been done. Also ensure all drivers and firmware have been updated to the certified levels for the operating system you will be using. These two notes will not be covered here.

In the example below, the name of the failover cluster is CLUSTER and the node names are NODE1 and NODE2.

Step 1: Evict first node and upgrade to Windows Server 2016

1. In Failover Cluster Manager, drain all resources from NODE1 to NODE2 by right mouse clicking on the node and selecting **Pause** and **Drain Roles**. Alternatively, you can use the PowerShell command SUSPEND-CLUSTERNODE.

2. Evict NODE1 from the Cluster by right mouse clicking the node and selecting **More Actions** and **Evict**. Alternatively, you can use the PowerShell command REMOVE-CLUSTERNODE.

3. As a precaution, detach NODE1 from the storage you are using. In some cases, disconnecting the storage cables from the machine will suffice. Check with your storage vendor for proper detachment steps if needed. Depending on your storage, this may not be necessary.

4. Rebuild NODE1 with Windows Server 2016. Ensure you have added all the necessary roles, features, drivers and security updates.

5. Create a new cluster called CLUSTER1 with NODE1. Open Failover Cluster Manager and in the **Management** pane, choose **Create Cluster** and follow the instructions in the wizard.

6. Once the Cluster is created, the roles will need to be migrated from the original cluster to this new cluster. On the new cluster, right mouse click on the cluster name (CLUSTER1) and selecting **More Actions** and **Copy Cluster Roles**. Follow along in the wizard to migrate the roles.

7. Once all the resources have been migrated, power down NODE2 (original cluster) and disconnect the storage so as to not cause any interference. Connect the storage to NODE1. Once all is connected, bring all the resources online and ensure they are functioning as should.

Step 2: Rebuild second node to Windows Server 2019

Once you have verified everything is working as it should, NODE2 can be rebuilt to Windows Server 2019 and joined to the Cluster.

1. Perform a clean installation of Windows Server 2019 on NODE2. Ensure you have added all the necessary roles, features, drivers and security updates.

2. Now that the original cluster (CLUSTER) is gone, you can leave the new cluster name as CLUSTER1 or go back to the original name. If you wish to go back to the original name, follow these steps:

   a. On NODE1, in Failover Cluster Manager right mouse click the name of the cluster (CLUSTER1) and choose **Properties**.

   b. On the **General** tab, rename the cluster to CLUSTER.

   c. When choosing OK or APPLY, you will see the below dialog popup.

   d. The Cluster Service will be stopped and needed to be started again for the rename to complete.

3. On NODE1, open Failover Cluster Manager. Right mouse click on **Nodes** and select **Add Node**. Go through the wizard adding NODE2 to the Cluster.

4. Attach the storage to NODE2. This could include reconnecting the storage cables.

5. Drain all resources from NODE1 to NODE2 by right mouse clicking on the node and selecting **Pause** and **Drain Roles**. Alternatively, you can use the PowerShell command SUSPEND-CLUSTERNODE. Ensure all resources are online and they are functioning as should.

Step 3: Rebuild first node to Windows Server 2019

1. Evict NODE1 from the cluster and disconnect the storage from the node in the manner from which you previously .
2. Rebuild or upgrade NODE1 to Windows Server 2019. Ensure you have added all the necessary roles, features, drivers and security updates.
3. Re-attach the storage and add NODE1 back to the cluster.
4. Move all the resources to NODE1 and ensure they come online and function as necessary.
5. The current cluster functional level remains at Windows 2016. Update the functional level to Windows 2019 with the PowerShell command UPDATE-CLUSTERFUNCTIONALLEVEL.

You are now running with a fully functional Windows Server 2019 Failover Cluster.

Additional notes

- As explained previously, disconnecting the storage may or may not be necessary. In our documentation, we want to err on the side of caution. Please consult with your storage vendor.
- If your starting point is Windows Server 2008 or 2008 R2 clusters, an additional run through of steps may be needed.
- If the cluster is running virtual machines, ensure you upgrade the virtual machine level once the cluster functional level has been done with the PowerShell command UPDATE-VMVERSION.
- Please note that if you are running an application such as SQL Server, Exchange Server, etc, the application will not be migrated with the Copy Cluster Roles wizard. You should consult your application vendor for proper migration steps of the application.

Cluster-Aware Updating overview

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This topic provides an overview of Cluster-Aware Updating (CAU), a feature that automates the software updating process on clustered servers while maintaining availability.

> **NOTE**
> When updating Storage Spaces Direct clusters, we recommend using Cluster-Aware Updating.

Feature description

Cluster-Aware Updating is an automated feature that enables you to update servers in a failover cluster with little or no loss in availability during the update process. During an Updating Run, Cluster-Aware Updating transparently performs the following tasks:

1. Puts each node of the cluster into node maintenance mode.
2. Moves the clustered roles off the node.
3. Installs the updates and any dependent updates.
4. Performs a restart if necessary.
5. Brings the node out of maintenance mode.
6. Restores the clustered roles on the node.
7. Moves to update the next node.

For many clustered roles in the cluster, the automatic update process triggers a planned failover. This can cause a transient service interruption for connected clients. However, in the case of continuously available workloads, such as Hyper-V with live migration or file server with SMB Transparent Failover, Cluster-Aware Updating can coordinate cluster updates with no impact to the service availability.

Practical applications

- CAU reduces service outages in clustered services, reduces the need for manual updating workarounds, and makes the end-to-end cluster updating process more reliable for the administrator. When the CAU feature is used in conjunction with continuously available cluster workloads, such as continuously available file servers (file server workload with SMB Transparent Failover) or Hyper-V, the cluster updates can be performed with zero impact to service availability for clients.
- CAU facilitates the adoption of consistent IT processes across the enterprise. Updating Run Profiles can be created for different classes of failover clusters and then managed centrally on a file share to ensure that CAU deployments throughout the IT organization apply updates consistently, even if the clusters are managed by different lines-of-business or administrators.
- CAU can schedule Updating Runs on regular daily, weekly, or monthly intervals to help coordinate cluster updates with other IT management processes.
- CAU provides an extensible architecture to update the cluster software inventory in a cluster-aware

fashion. This can be used by publishers to coordinate the installation of software updates that are not published to Windows Update or Microsoft Update or that are not available from Microsoft, for example, updates for non-Microsoft device drivers.

- CAU self-updating mode enables a "cluster in a box" appliance (a set of clustered physical machines, typically packaged in one chassis) to update itself. Typically, such appliances are deployed in branch offices with minimal local IT support to manage the clusters. Self-updating mode offers great value in these deployment scenarios.

Important functionality

The following is a description of important Cluster-Aware Updating functionality:

- A user interface (UI) - the Cluster Aware Updating window - and a set of cmdlets that you can use to preview, apply, monitor, and report on the updates
- An end-to-end automation of the cluster-updating operation (an Updating Run), orchestrated by one or more Update Coordinator computers
- A default plug-in that integrates with the existing Windows Update Agent (WUA) and Windows Server Update Services (WSUS) infrastructure in Windows Server to apply important Microsoft updates
- A second plug-in that can be used to apply Microsoft hotfixes, and that can be customized to apply non-Microsoft updates
- Updating Run Profiles that you configure with settings for Updating Run options, such as the maximum number of times that the update will be retried per node. Updating Run Profiles enable you to rapidly reuse the same settings across Updating Runs and easily share the update settings with other failover clusters.
- An extensible architecture that supports new plug-in development to coordinate other node-updating tools across the cluster, such as custom software installers, BIOS updating tools, and network adapter or host bus adapter (HBA) updating tools.

Cluster-Aware Updating can coordinate the complete cluster updating operation in two modes:

- **Self-updating mode** For this mode, the CAU clustered role is configured as a workload on the failover cluster that is to be updated, and an associated update schedule is defined. The cluster updates itself at scheduled times by using a default or custom Updating Run profile. During the Updating Run, the CAU Update Coordinator process starts on the node that currently owns the CAU clustered role, and the process sequentially performs updates on each cluster node. To update the current cluster node, the CAU clustered role fails over to another cluster node, and a new Update Coordinator process on that node assumes control of the Updating Run. In self-updating mode, CAU can update the failover cluster by using a fully automated, end-to-end updating process. An administrator can also trigger updates on-demand in this mode, or simply use the remote-updating approach if desired. In self-updating mode, an administrator can get summary information about an Updating Run in progress by connecting to the cluster and running the **Get-CauRun** Windows PowerShell cmdlet.
- **Remote-updating mode** For this mode, a remote computer, which is called an Update Coordinator, is configured with the CAU tools. The Update Coordinator is not a member of the cluster that is updated during the Updating Run. From the remote computer, the administrator triggers an on-demand Updating Run by using a default or custom Updating Run profile. Remote-updating mode is useful for monitoring real-time progress during the Updating Run, and for clusters that are running on Server Core installations.

Hardware and software requirements

CAU can be used on all editions of Windows Server, including Server Core installations. For detailed requirements information, see Cluster-Aware Updating requirements and best practices.

Installing Cluster-Aware Updating

To use CAU, install the Failover Clustering feature in Windows Server and create a failover cluster. The components that support CAU functionality are automatically installed on each cluster node.

To install the Failover Clustering feature, you can use the following tools:

- Add Roles and Features Wizard in Server Manager
- Install-WindowsFeature Windows PowerShell cmdlet
- Deployment Image Servicing and Management (DISM) command-line tool

For more information, see Install the Failover Clustering feature.

You must also install the Failover Clustering Tools, which are part of the Remote Server Administration Tools and are installed by default when you install the Failover Clustering feature in Server Manager. The Failover Clustering tools include the Cluster-Aware Updating user interface and PowerShell cmdlets.

You must install the Failover Clustering Tools as follows to support the different CAU updating modes:

- To use CAU in self-updating mode, install the Failover Clustering Tools on each cluster node.
- To enable remote-updating mode, install the Failover Clustering Tools on a computer that has network connectivity to the failover cluster.

> **NOTE**
>
> - You can't use the Failover Clustering Tools on Windows Server 2012 to manage Cluster-Aware Updating on a newer version of Windows Server.
> - To use CAU only in remote-updating mode, installation of the Failover Clustering Tools on the cluster nodes is not required. However, certain CAU features will not be available. For more information, see Requirements and Best Practices for Cluster-Aware Updating.
> - Unless you are using CAU only in self-updating mode, the computer on which the CAU tools are installed and that coordinates the updates cannot be a member of the failover cluster.

Enabling self-updating mode

To enable the self-updating mode, you must add the Cluster-Aware Updating clustered role to the failover cluster. To do so, use one of the following methods:

- In Server Manager, select **Tools** > **Cluster-Aware Updating**, then in the Cluster-Aware Updating window, select **Configure cluster self-updating options**.
- In a PowerShell session, run the Add-CauClusterRole cmdlet.

To uninstall CAU, uninstall the Failover Clustering feature or Failover Clustering Tools by using Server Manager, the Uninstall-WindowsFeature cmdlet, or the DISM command-line tools.

Additional requirements and best practices

To ensure that CAU can update the cluster nodes successfully, and for additional guidance for configuring your failover cluster environment to use CAU, you can run the CAU Best Practices Analyzer.

For detailed requirements and best practices for using CAU, and information about running the CAU Best Practices Analyzer, see Requirements and Best Practices for Cluster-Aware Updating.

Starting Cluster-Aware Updating

To start Cluster-Aware Updating from Server Manager

1. Start Server Manager.

2. Do one of the following:
   - On the **Tools** menu, click **Cluster-Aware Updating**.
   - If one or more cluster nodes, or the cluster, is added to Server Manager, on the **All Servers** page, right-click the name of a node (or the name of the cluster), and then click **Update Cluster**.

Additional References

The following links provide more information about using Cluster-Aware Updating.

- Requirements and Best Practices for Cluster-Aware Updating
- Cluster-Aware Updating: Frequently Asked Questions
- Advanced Options and Updating Run Profiles for CAU
- How CAU Plug-ins Work
- Cluster-Aware Updating Cmdlets in Windows PowerShell
- Cluster-Aware Updating Plug-in Reference

Cluster-Aware Updating requirements and best practices

12/9/2022 • 20 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This section describes the requirements and dependencies that are needed to use Cluster-Aware Updating (CAU) to apply updates to a failover cluster running Windows Server.

> **NOTE**
> You may need to independently validate that your cluster environment is ready to apply updates if you use a plug-in other than **Microsoft.WindowsUpdatePlugin**. If you are using a non-Microsoft plug-in, contact the publisher for more information. For more information about plug-ins, see How Plug-ins Work.

Install the Failover Clustering feature and the Failover Clustering Tools

CAU requires an installation of the Failover Clustering feature and the Failover Clustering Tools. The Failover Clustering Tools include the CAU tools (clusterawareupdating.dll), the Failover Clustering cmdlets, and other components needed for CAU operations. For steps to install the Failover Clustering feature, see Installing the Failover Clustering Feature and Tools.

The exact installation requirements for the Failover Clustering Tools depend on whether CAU coordinates updates as a clustered role on the failover cluster (by using self-updating mode) or from a remote computer. The self-updating mode of CAU additionally requires the installation of the CAU clustered role on the failover cluster by using the CAU tools.

The following table summarizes the CAU feature installation requirements for the two CAU updating modes.

INSTALLED COMPONENT	SELF-UPDATING MODE	REMOTE-UPDATING MODE
Failover Clustering feature	Required on all cluster nodes	Required on all cluster nodes
Failover Clustering Tools	Required on all cluster nodes	- Required on remote-updating computer - Required on all cluster nodes to run the Save-CauDebugTrace cmdlet
CAU clustered role	Required	Not required

Obtain an administrator account

The following administrator requirements are necessary to use CAU features.

- To preview or apply update actions by using the CAU user interface (UI) or the Cluster-Aware Updating cmdlets, you must use a domain account that has local administrator rights and permissions on all the cluster nodes. If the account doesn't have sufficient privileges on every node, you are prompted in the Cluster-Aware Updating window to supply the necessary credentials when you perform these actions. To

use the Cluster-Aware Updating cmdlets, you can supply the necessary credentials as a cmdlet parameter.

- If you use CAU in remote-updating mode when you are signed in with an account that doesn't have local administrator rights and permissions on the cluster nodes, you must run the CAU tools as an administrator by using a local administrator account on the Update Coordinator computer, or by using an account that has the **Impersonate a client after authentication** user right.
- To run the CAU Best Practices Analyzer, you must use an account that has administrative privileges on the cluster nodes and local administrative privileges on the computer that is used to run the Test-CauSetup cmdlet or to analyze cluster updating readiness using the Cluster-Aware Updating window. For more information, see Test cluster updating readiness.

Verify the cluster configuration

The following are general requirements for a failover cluster to support updates by using CAU. Additional configuration requirements for remote management on the nodes are listed in Configure the nodes for remote management later in this topic.

- Sufficient cluster nodes must be online so that the cluster has quorum.
- All cluster nodes must be in the same Active Directory domain.
- The cluster name must be resolved on the network using DNS.
- If CAU is used in remote-updating mode, the Update Coordinator computer must have network connectivity to the failover cluster nodes, and it must be in the same Active Directory domain as the failover cluster.
- The Cluster service should be running on all cluster nodes. By default this service is installed on all cluster nodes and is configured to start automatically.
- To use PowerShell pre-update or post-update scripts during a CAU Updating Run, ensure that the scripts are installed on all cluster nodes or that they are accessible to all nodes, for example, on a highly available network file share. If scripts are saved to a network file share, configure the folder for Read permission for the Everyone group.

Configure the nodes for remote management

To use Cluster-Aware Updating, all nodes of the cluster must be configured for remote management. By default, the only task you must perform to configure the nodes for remote management is to Enable a firewall rule to allow automatic restarts.

The following table lists the complete remote management requirements, in case your environment diverges from the defaults.

These requirements are in addition to the installation requirements for the Install the Failover Clustering feature and the Failover Clustering Tools and the general clustering requirements that are described in previous sections in this topic.

REQUIREMENT	DEFAULT STATE	SELF-UPDATING MODE	REMOTE-UPDATING MODE
Enable a firewall rule to allow automatic restarts	Disabled	Required on all cluster nodes if a firewall is in use	Required on all cluster nodes if a firewall is in use
Enable Windows Management Instrumentation	Enabled	Required on all cluster nodes	Required on all cluster nodes

REQUIREMENT	DEFAULT STATE	SELF-UPDATING MODE	REMOTE-UPDATING MODE
Enable Windows PowerShell 3.0 or 4.0 and Windows PowerShell remoting	Enabled	Required on all cluster nodes	Required on all cluster nodes to run the following: - The Save-CauDebugTrace cmdlet - PowerShell pre-update and post-update scripts during an Updating Run - Tests of cluster updating readiness using the Cluster-Aware Updating window or the Test-CauSetup Windows PowerShell cmdlet
Install .NET Framework 4.6 or 4.5	Enabled	Required on all cluster nodes	Required on all cluster nodes to run the following: - The Save-CauDebugTrace cmdlet - PowerShell pre-update and post-update scripts during an Updating Run - Tests of cluster updating readiness using the Cluster-Aware Updating window or the Test-CauSetup Windows PowerShell cmdlet

Enable a firewall rule to allow automatic restarts

To allow automatic restarts after updates are applied (if the installation of an update requires a restart), if Windows Firewall or a non-Microsoft firewall is in use on the cluster nodes, a firewall rule must be enabled on each node that allows the following traffic:

- Protocol: TCP
- Direction: inbound
- Program: wininit.exe
- Ports: RPC Dynamic Ports
- Profile: Domain

If Windows Firewall is used on the cluster nodes, you can do this by enabling the **Remote Shutdown** Windows Firewall rule group on each cluster node. When you use the Cluster-Aware Updating window to apply updates and to configure self-updating options, the **Remote Shutdown** Windows Firewall rule group is automatically enabled on each cluster node.

> **NOTE**
>
> The **Remote Shutdown** Windows Firewall rule group cannot be enabled when it will conflict with Group Policy settings that are configured for Windows Firewall.

The **Remote Shutdown** firewall rule group is also enabled by specifying the **–EnableFirewallRules** parameter when running the following CAU cmdlets: Add-CauClusterRole, Invoke-CauRun, and SetCauClusterRole.

The following PowerShell example shows an additional method to enable automatic restarts on a cluster node.

```
Set-NetFirewallRule -Group "@firewallapi.dll,-36751" -Profile Domain -Enabled true
```

Enable Windows Management Instrumentation (WMI)

All cluster nodes must be configured for remote management using Windows Management Instrumentation (WMI). This is enabled by default.

To manually enable remote management, do the following:

1. In the Services console, start the **Windows Remote Management** service and set the startup type to **Automatic**.
2. Run the Set-WSManQuickConfig cmdlet, or run the following command from an elevated command prompt:

   ```
   winrm quickconfig -q
   ```

To support WMI remoting, if Windows Firewall is in use on the cluster nodes, the inbound firewall rule for **Windows Remote Management (HTTP-In)** must be enabled on each node. By default, this rule is enabled.

Enable Windows PowerShell and Windows PowerShell remoting

To enable self-updating mode and certain CAU features in remote-updating mode, PowerShell must be installed and enabled to run remote commands on all cluster nodes. By default, PowerShell is installed and enabled for remoting.

To enable PowerShell remoting, use one of the following methods:

- Run the Enable-PSRemoting cmdlet.
- Configure a domain-level Group Policy setting for Windows Remote Management (WinRM).

For more information about enabling PowerShell remoting, see About Remote Requirements.

Install .NET Framework 4.6 or 4.5

To enable self-updating mode and certain CAU features in remote-updating mode,.NET Framework 4.6, or .NET Framework 4.5 (on Windows Server 2012 R2) must be installed on all cluster nodes. By default, NET Framework is installed.

To install .NET Framework 4.6 (or 4.5) using PowerShell if it's not already installed, use the following command:

```
Install-WindowsFeature -Name NET-Framework-45-Core
```

Best practices recommendations for using Cluster-Aware Updating

Recommendations for applying Microsoft updates

We recommend that when you begin to use CAU to apply updates with the default **Microsoft.WindowsUpdatePlugin** plug-in on a cluster, you stop using other methods to install software updates from Microsoft on the cluster nodes.

Caution

Combining CAU with methods that update individual nodes automatically (on a fixed time schedule) can cause unpredictable results, including interruptions in service and unplanned downtime.

We recommend that you follow these guidelines:

- For optimal results, we recommend that you disable settings on the cluster nodes for automatic updating, for example, through the Automatic Updates settings in Control Panel, or in settings that are configured using Group Policy.

  Caution

  Automatic installation of updates on the cluster nodes can interfere with installation of updates by CAU and can cause CAU failures.

  If they are needed, the following Automatic Updates settings are compatible with CAU, because the administrator can control the timing of update installation:

  - Settings to notify before downloading updates and to notify before installation
  - Settings to automatically download updates and to notify before installation

  However, if Automatic Updates is downloading updates at the same time as a CAU Updating Run, the Updating Run might take longer to complete.

- Do not configure an update system such as Windows Server Update Services (WSUS) to apply updates automatically (on a fixed time schedule) to cluster nodes.
- All cluster nodes should be uniformly configured to use the same update source, for example, a WSUS server, Windows Update, or Microsoft Update.
- If you use a configuration management system to apply software updates to computers on the network, exclude cluster nodes from all required or automatic updates. Examples of configuration management systems include Microsoft Endpoint Configuration Manager and Microsoft System Center Virtual Machine Manager 2008.
- If internal software distribution servers (for example, WSUS servers) are used to contain and deploy the updates, ensure that those servers correctly identify the approved updates for the cluster nodes.

Apply Microsoft updates in branch office scenarios

To download Microsoft updates from Microsoft Update or Windows Update to cluster nodes in certain branch office scenarios, you may need to configure proxy settings for the Local System account on each node. For example, you might need to do this if your branch office clusters access Microsoft Update or Windows Update to download updates by using a local proxy server.

If necessary, configure WinHTTP proxy settings on each node to specify a local proxy server and configure local address exceptions (that is, a bypass list for local addresses). To do this, you can run the following command on each cluster node from an elevated command prompt:

```
netsh winhttp set proxy <ProxyServerFQDN >:<port> "<local>"
```

where <*ProxyServerFQDN*> is the fully qualified domain name for the proxy server and <*port*> is the port over which to communicate (usually port 443).

For example, to configure WinHTTP proxy settings for the Local System account specifying the proxy server *MyProxy.CONTOSO.com*, with port 443 and local address exceptions, type the following command:

```
netsh winhttp set proxy MyProxy.CONTOSO.com:443 "<local>"
```

Recommendations for using the Microsoft.HotfixPlugin

- We recommend that you configure permissions in the hotfix root folder and hotfix configuration file to restrict Write access to only local administrators on the computers that are used to store these files. This helps prevent tampering with these files by unauthorized users that could compromise the functionality of the failover cluster when hotfixes are applied.
- To help ensure data integrity for the server message block (SMB) connections that are used to access the hotfix root folder, you should configure SMB Encryption in the SMB shared folder, if it is possible to configure it. The **Microsoft.HotfixPlugin** requires that SMB signing or SMB Encryption is configured to help ensure data integrity for the SMB connections.

  For more information, see Restrict access to the hotfix root folder and hotfix configuration file.

Additional recommendations

- To avoid interfering with a CAU Updating Run that may be scheduled at the same time, do not schedule password changes for cluster name objects and virtual computer objects during scheduled maintenance windows.
- You should set appropriate permissions on pre-update and post-update scripts that are saved on network shared folders to prevent potential tampering with these files by unauthorized users.
- To configure CAU in self-updating mode, a virtual computer object (VCO) for the CAU clustered role must be created in Active Directory. CAU can create this object automatically at the time that the CAU clustered role is added, if the failover cluster has sufficient permissions. However, because of the security policies in certain organizations, it may be necessary to prestage the object in Active Directory. For a procedure to do this, see Steps for prestaging an account for a clustered role.
- To save and reuse Updating Run settings across failover clusters with similar updating needs in the IT organization, you can create Updating Run Profiles. Additionally, depending on the updating mode, you can save and manage the Updating Run Profiles on a file share that is accessible to all remote Update Coordinator computers or failover clusters. For more information, see Advanced Options and Updating Run Profiles for CAU.

Test cluster updating readiness

You can run the CAU Best Practices Analyzer (BPA) model to test whether a failover cluster and the network environment meet many of the requirements to have software updates applied by CAU. Many of the tests check the environment for readiness to apply Microsoft updates by using the default plug-in, **Microsoft.WindowsUpdatePlugin**.

> **NOTE**
>
> You might need to independently validate that your cluster environment is ready to apply software updates by using a plug-in other than **Microsoft.WindowsUpdatePlugin**. If you are using a non-Microsoft plug-in, such as one provided by your hardware manufacturer, contact the publisher for more information.

You can run the BPA in the following two ways:

1. Select **Analyze cluster updating readiness** in the CAU console. After the BPA completes the readiness tests, a test report appears. If issues are detected on cluster nodes, the specific issues and the nodes where the issues appear are identified so that you can take corrective action. The tests can take several minutes to complete.
2. Run the Test-CauSetup cmdlet. You can run the cmdlet on a local or remote computer on which the Failover Clustering Module for Windows PowerShell (part of the Failover Clustering Tools) is installed. You can also run the cmdlet on a node of the failover cluster.

NOTE

- You must use an account that has administrative privileges on the cluster nodes and local administrative privileges on the computer that is used to run the **Test-CauSetup** cmdlet or to analyze cluster updating readiness using the Cluster-Aware Updating window. To run the tests using the Cluster-Aware Updating window, you must be logged on to the computer with the necessary credentials.
- The tests assume that the CAU tools that are used to preview and apply software updates run from the same computer and with the same user credentials as are used to test cluster updating readiness.

IMPORTANT

We highly recommend that you test the cluster for updating readiness in the following situations:

- Before you use CAU for the first time to apply software updates.
- After you add a node to the cluster or perform other hardware changes in the cluster that require running the Validate a Cluster Wizard.
- After you change an update source, or change update settings or configurations (other than CAU) that can affect the application of updates on the nodes.

Tests for cluster updating readiness

The following table lists the cluster updating readiness tests, some common issues, and resolution steps.

TEST	POSSIBLE ISSUES AND IMPACTS	RESOLUTION STEPS
The failover cluster must be available	Cannot resolve the failover cluster name, or one or more cluster nodes cannot be accessed. The BPA cannot run the cluster readiness tests.	- Check the spelling of the name of the cluster specified during the BPA run. - Ensure that all nodes of the cluster are online and running. - Check that the Validate a Configuration Wizard can successfully run on the failover cluster.
The failover cluster nodes must be enabled for remote management via WMI	One or more failover cluster nodes are not enabled for remote management by using Windows Management Instrumentation (WMI). CAU cannot update the cluster nodes if the nodes are not configured for remote management.	Ensure that all failover cluster nodes are enabled for remote management through WMI. For more information, see Configure the nodes for remote management in this topic.
PowerShell remoting should be enabled on each failover cluster node	PowerShell isn't installed or isn't enabled for remoting on one or more failover cluster nodes. CAU cannot be configured for self-updating mode or use certain features in remote-updating mode.	Ensure that PowerShell is installed on all cluster nodes and is enabled for remoting. For more information, see Configure the nodes for remote management in this topic.
Failover cluster version	One or more nodes in the failover cluster don't run Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012. CAU cannot update the failover cluster.	Verify that the failover cluster that is specified during the BPA run is running Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012. For more information, see Verify the cluster configuration in this topic.

TEST	POSSIBLE ISSUES AND IMPACTS	RESOLUTION STEPS
The required versions of .NET Framework and Windows PowerShell must be installed on all failover cluster nodes	.NET Framework 4.6, 4.5 or Windows PowerShell isn't installed on one or more cluster nodes. Some CAU features might not work.	Ensure that .NET Framework 4.6 or 4.5 and Windows PowerShell are installed on all cluster nodes, if they are required. For more information, see Configure the nodes for remote management in this topic.
The Cluster service should be running on all cluster nodes	The Cluster service is not running on one or more nodes. CAU cannot update the failover cluster.	- Ensure that the Cluster service (clussvc) is started on all nodes in the cluster, and it is configured to start automatically. - Check that the Validate a Configuration Wizard can successfully run on the failover cluster. For more information, see Verify the cluster configuration in this topic.
Automatic Updates must not be configured to automatically install updates on any failover cluster node	On at least one failover cluster node, Automatic Updates is configured to automatically install Microsoft updates on that node. Combining CAU with other update methods can result in unplanned downtime or unpredictable results.	If Windows Update functionality is configured for Automatic Updates on one or more cluster nodes, ensure that Automatic Updates is not configured to automatically install updates. For more information, see Recommendations for applying Microsoft updates.
The failover cluster nodes should use the same update source	One or more failover cluster nodes are configured to use an update source for Microsoft updates that is different from the rest of the nodes. Updates might not be applied uniformly on the cluster nodes by CAU.	Ensure that every cluster node is configured to use the same update source, for example, a WSUS server, Windows Update, or Microsoft Update. For more information, see Recommendations for applying Microsoft updates.
A firewall rule that allows remote shutdown should be enabled on each node in the failover cluster	One or more failover cluster nodes do not have a firewall rule enabled that allows remote shutdown, or a Group Policy setting prevents this rule from being enabled. An Updating Run that applies updates that require restarting the nodes automatically might not complete properly.	If Windows Firewall or a non-Microsoft firewall is in use on the cluster nodes, configure a firewall rule that allows remote shutdown. For more information, see Enable a firewall rule to allow automatic restarts in this topic.
The proxy server setting on each failover cluster node should be set to a local proxy server	One or more failover cluster nodes have an incorrect proxy server configuration. If a local proxy server is in use, the proxy server setting on each node must be configured properly for the cluster to access Microsoft Update or Windows Update.	Ensure that the WinHTTP proxy settings on each cluster node are set to a local proxy server if it is needed. If a proxy server is not in use in your environment, this warning can be ignored. For more information, see Apply updates in branch office scenarios in this topic.

TEST	POSSIBLE ISSUES AND IMPACTS	RESOLUTION STEPS
The CAU clustered role should be installed on the failover cluster to enable self-updating mode	The CAU clustered role is not installed on this failover cluster. This role is required for cluster self-updating.	To use CAU in self-updating mode, add the CAU clustered role on the failover cluster in one of the following ways: - Run the Add-CauClusterRole PowerShell cmdlet. - Select the **Configure cluster self-updating options** action in the Cluster-Aware Updating window.
The CAU clustered role should be enabled on the failover cluster to enable self-updating mode	The CAU clustered role is disabled. For example, the CAU clustered role is not installed, or it has been disabled by using the Disable-CauClusterRole PowerShell cmdlet. This role is required for cluster self-updating.	To use CAU in self-updating mode, enable the CAU clustered role on this failover cluster in one of the following ways: - Run the Enable-CauClusterRole PowerShell cmdlet. - Select the **Configure cluster self-updating options** action in the Cluster-Aware Updating window.
The configured CAU plug-in for self-updating mode must be registered on all failover cluster nodes	The CAU clustered role on one or more nodes of this failover cluster cannot access the CAU plug-in module that is configured in the self-updating options. A self-updating run might fail.	- Ensure that the configured CAU plug-in is installed on all cluster nodes by following the installation procedure for the product that supplies the CAU plug-in. - Run the Register-CauPlugin PowerShell cmdlet to register the plug-in on the required cluster nodes.
All failover cluster nodes should have the same set of registered CAU plug-ins	A self-updating run might fail if the plug-in that is configured to be used in an Updating Run is changed to one that is not available on all cluster nodes.	- Ensure that the configured CAU plug-in is installed on all cluster nodes by following the installation procedure for the product that supplies the CAU plug-in. - Run the Register-CauPlugin PowerShell cmdlet to register the plug-in on the required cluster nodes.
The configured Updating Run options must be valid	The self-updating schedule and Updating Run options that are configured for this failover cluster are incomplete or are not valid. A self-updating run might fail.	Configure a valid self-updating schedule and set of Updating Run options. For example, you can use the Set-CauClusterRole PowerShell cmdlet to configure the CAU clustered role.
At least two failover cluster nodes must be owners of the CAU clustered role	An Updating Run launched in self-updating mode will fail because the CAU clustered role does not have a possible owner node to move to.	Use the Failover Clustering Tools to ensure that all cluster nodes are configured as possible owners of the CAU clustered role. This is the default configuration.
All failover cluster nodes must be able to access Windows PowerShell scripts	Not all possible owner nodes of the CAU clustered role can access the configured Windows PowerShell pre-update and post-update scripts. A self-updating run will fail.	Ensure that all possible owner nodes of the CAU clustered role have permissions to access the configured PowerShell pre-update and post-update scripts.

TEST	POSSIBLE ISSUES AND IMPACTS	RESOLUTION STEPS
All failover cluster nodes should use identical Windows PowerShell scripts	Not all possible owner nodes of the CAU clustered role use the same copy of the specified Windows PowerShell pre-update and post-update scripts. A self-updating run might fail or show unexpected behavior.	Ensure that all possible owner nodes of the CAU clustered role use the same PowerShell pre-update and post-update scripts.
The WarnAfter setting specified for the Updating Run should be less than the StopAfter setting	The specified CAU Updating Run timeout values make the warning timeout ineffective. An Updating Run might be canceled before a warning event log can be generated.	In the Updating Run options, configure a **WarnAfter** option value that is less than the **StopAfter** option value.

Additional References

- Cluster-Aware Updating overview

Cluster-Aware Updating advanced options and updating run profiles

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

This topic describes Updating Run options that can be configured for a Cluster-Aware Updating (CAU) Updating Run. These advanced options can be configured when you use either the CAU UI or the CAU Windows PowerShell cmdlets to apply updates or to configure self-updating options.

Most configuration settings can be saved as an XML file called an Updating Run Profile and reused for later Updating Runs. The default values for the Updating Run options that are provided by CAU can also be used in many cluster environments.

For information about additional options that you can specify for each Updating Run and about Updating Run Profiles, see the following sections later in this topic:

Options that you specify when you request an Updating Run Use Updating Run Profiles Options that can be set in an Updating Run Profile

The following table lists options that you can set in a CAU Updating Run Profile.

> **NOTE**
>
> To set the PreUpdateScript or PostUpdateScript option, ensure that Windows PowerShell and .NET Framework 4.6 or 4.5 are installed and that PowerShell remoting is enabled on each node in the cluster. For more information, see Configure the nodes for remote management in Requirements and Best Practices for Cluster-Aware Updating.

OPTION	DEFAULT VALUE	DETAILS
StopAfter	Unlimited time	Time in minutes after which the Updating Run will be stopped if it has not completed. **Note:** If you specify a pre-update or a post-update PowerShell script, the entire process of running scripts and performing updates must be complete within the **StopAfter** time limit.
WarnAfter	By default, no warning appears	Time in minutes after which a warning will appear if the Updating Run (including a pre-update script and a post-update script, if they are configured) has not completed.
MaxRetriesPerNode	3	Maximum number of times that the update process (including a pre-update script and a post-update script, if they are configured) will be retried per node. The maximum is 64.

OPTION	DEFAULT VALUE	DETAILS
MaxFailedNodes	For most clusters, an integer that is approximately one-third of the number of cluster nodes	Maximum number of nodes on which updating can fail, either because the nodes fail or the Cluster service stops running. If one more node fails, the Updating Run is stopped. The valid range of values is 0 to 1 less than the number of cluster nodes.
RequireAllNodesOnline	None	Specifies that all nodes must be online and reachable before updating begins.
RebootTimeoutMinutes	15	Time in minutes that CAU will allow for restarting a node (if a restart is necessary) and starting all auto-start services. If the restart process doesn't complete within this time, the Updating Run on that node is marked as failed.
PreUpdateScript	None	The path and file name for a PowerShell script to run on each node before updating begins, and before the node is put into maintenance mode. The file name extension must be **.ps1**, and the total length of the path plus file name must not exceed 260 characters. As a best practice, the script should be located on a disk in cluster storage, or at a highly available network file share, to ensure that it is always accessible to all of the cluster nodes. If the script is located on a network file share, ensure that you configure the file share for Read permission for the Everyone group, and restrict write access to prevent tampering with the files by unauthorized users. If you specify a pre-update script, be sure that settings such as the time limits (for example, **StopAfter**) are configured to allow the script to run successfully. These limits span the entire process of running scripts and installing updates, not just the process of installing updates.

OPTION	DEFAULT VALUE	DETAILS
PostUpdateScript	None	The path and file name for a PowerShell script to run after updating completes (after the node leaves maintenance mode). The file name extension must be **.ps1** and the total length of the path plus file name must not exceed 260 characters. As a best practice, the script should be located on a disk in cluster storage, or at a highly available network file share, to ensure that it is always accessible to all of the cluster nodes. If the script is located on a network file share, ensure that you configure the file share for Read permission for the Everyone group, and restrict write access to prevent tampering with the files by unauthorized users. If you specify a post-update script, be sure that settings such as the time limits (for example, **StopAfter**) are configured to allow the script to run successfully. These limits span the entire process of running scripts and installing updates, not just the process of installing updates.
ConfigurationName	This setting only has an effect if you run scripts. If you specify a pre-update script or a post-update script, but you do not specify a **ConfigurationName**, the default session configuration for PowerShell (Microsoft.PowerShell) is used.	Specifies the PowerShell session configuration that defines the session in which scripts (specified by **PreUpdateScript** and **PostUpdateScript**) are run, and can limit the commands that can be run.
CauPluginName	**Microsoft.WindowsUpdatePlugin**	Plug-in that you configure Cluster-Aware Updating to use to preview updates or perform an Updating Run. For more information, see How Cluster-Aware Updating plug-ins work.

OPTION	DEFAULT VALUE	DETAILS
CauPluginArguments	None	A set of *name=value* pairs (arguments) for the updating plug-in to use, for example: **Domain=Domain.local** These *name=value* pairs must be meaningful to the plug-in that you specify in **CauPluginName**. To specify an argument using the CAU UI, type the *name*, press the Tab key, and then type the corresponding *value*. Press the Tab key again to provide the next argument. Each *name* and *value* are automatically separated with an equal (=) sign. Multiple pairs are automatically separated with semicolons. For the default **Microsoft.WindowsUpdatePlugin** plug-in, no arguments are needed. However, you can specify an optional argument, for example to specify a standard Windows Update Agent query string to filter the set of updates that are applied by the plug-in. For a *name*, use **QueryString**, and for a *value*, enclose the full query in quotation marks. For more information, see How Cluster-Aware Updating plug-ins work.

Options that you specify when you request an Updating Run

The following table lists options (other than those in an Updating Run Profile) that you can specify when you request an Updating Run. For information about options that you can set in an Updating Run Profile, see the preceding table.

OPTION	DEFAULT VALUE	DETAILS
ClusterName	None **Note:** This option must be set only when the CAU UI is not run on a failover cluster node, or you want to reference a failover cluster different from where the CAU UI is run.	NetBIOS name of the cluster on which to perform the Updating Run.

OPTION	DEFAULT VALUE	DETAILS
Credential	Current account credentials	Administrative credentials for the target cluster on which the Updating Run will be performed. You may already have the necessary credentials if you start the CAU UI (or open a PowerShell session, if you're using the CAU PowerShell cmdlets) from an account that has administrator rights and permissions on the cluster.
NodeOrder	By default, CAU starts with the node that owns the smallest number of clustered roles, then progresses to the node that has the second smallest number, and so on.	Names of the cluster nodes in the order that they should be updated (if possible).

Use Updating Run Profiles

Each Updating Run can be associated with a specific Updating Run Profile. The default Updating Run Profile is stored in the *%windir%\cluster* folder. If you're using the CAU UI in remote-updating mode, you can specify an Updating Run Profile at the time that you apply updates, or you can use the default Updating Run profile. If you're using CAU in self-updating mode, you can import the settings from a specified Updating Run Profile when you configure the self-updating options. In both cases, you can override the displayed values for the Updating Run options according to your needs. If you want, you can save the Updating Run options as an Updating Run Profile with the same file name or a different file name. The next time that you apply updates or configure self-updating options, CAU automatically selects the Updating Run Profile that was previously selected.

You can modify an existing Updating Run Profile or create a new one by selecting **Create or modify Updating Run Profile** in the CAU UI.

Here are some important notes about using Updating Run Profiles:

- An Updating Run Profile doesn't store cluster-specific information such as administrative credentials. If you're using CAU in self-updating mode, the Updating Run Profile also doesn't store the self-updating schedule information. This makes it possible to share an Updating Run Profile across all failover clusters in a specified class.
- If you configure self-updating options using an Updating Run Profile and later modify the profile with different values for the Updating Run options, the self-updating configuration doesn't change automatically. To apply the new Updating Run settings, you must configure the self-updating options again.
- The Run Profile Editor unfortunately doesn't support file paths that include spaces, such as *C:\Program Files*. As a workaround, store your pre and post update scripts in a path that doesn't include spaces, or use PowerShell exclusively to manage Run Profiles, putting quotes around the path when running **Invoke-CauRun**.

Windows PowerShell equivalent commands

You can import the settings from an Updating Run Profile when you run the **Invoke-CauRun**, **Add-CauClusterRole**, or **Set-CauClusterRole** cmdlet.

The following example performs a scan and a full Updating Run on the cluster named *CONTOSO-FC1*, using the Updating Run options that are specified in *C:\Windows\Cluster\DefaultParameters.xml*. Default values are used for the remaining cmdlet parameters.

```
$MyRunProfile = Import-Clixml C:\Windows\Cluster\DefaultParameters.xml
Invoke-CauRun –ClusterName CONTOSO-FC1 @MyRunProfile
```

By using an Updating Run Profile, you can update a failover cluster in a repeatable fashion with consistent settings for exception management, time bounds, and other operational parameters. Because these settings are typically specific to a class of failover clusters—such as "All Microsoft SQL Server clusters", or "My business-critical clusters"—you might want to name each Updating Run Profile according to the class of Failover Clusters it will be used with. In addition, you might want to manage the Updating Run Profile on a file share that is accessible to all of the failover clusters of a specific class in your IT organization.

Additional References

- Cluster-Aware Updating
- Cluster-Aware Updating Cmdlets in Windows PowerShell

How Cluster-Aware Updating plug-ins work

12/9/2022 • 21 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Azure Stack HCI, versions 21H2 and 20H2

Cluster-Aware Updating (CAU) uses plug-ins to coordinate the installation of updates across nodes in a failover cluster. This topic provides information about using the built-in CAU plug-ins or other plug-ins that you install for CAU.

Install a plug-in

A plug-in other than the default plug-ins that are installed with CAU (**Microsoft.WindowsUpdatePlugin** and **Microsoft.HotfixPlugin**) must be installed separately. If CAU is used in self-updating mode, the plug-in must be installed on all cluster nodes. If CAU is used in remote-updating mode, the plug-in must be installed on the remote Update Coordinator computer. A plug-in that you install may have additional installation requirements on each node.

To install a plug-in, follow the instructions from the plug-in publisher. To manually register a plug-in with CAU, run the Register-CauPlugin cmdlet on each computer where the plug-in is installed.

Specify a plug-in and plug-in arguments

Specify a CAU plug-in

In the CAU UI, you select a plug-in from a drop-down list of available plug-ins when you use CAU to perform the following actions:

- Apply updates to the cluster
- Preview updates for the cluster
- Configure cluster self-updating options

By default, CAU selects the plug-in **Microsoft.WindowsUpdatePlugin**. However, you can specify any plug-in that is installed and registered with CAU.

> **TIP**
> In the CAU UI, you can only specify a single plug-in for CAU to use to preview or to apply updates during an Updating Run. By using the CAU PowerShell cmdlets, you can specify one or more plug-ins. If you need to install multiple types of updates on the cluster, it is usually more efficient to specify multiple plug-ins in one Updating Run, rather than using a separate Updating Run for each plug-in. For example, fewer node restarts will typically occur.

By using the CAU PowerShell cmdlets that are listed in the following table, you can specify one or more plug-ins for an Updating Run or scan by passing the **–CauPluginName** parameter. You can specify multiple plug-in names by separating them with commas. If you specify multiple plug-ins, you can also control how the plug-ins influence each other during an Updating Run by specifying the **-RunPluginsSerially**, **-StopOnPluginFailure**, and **–SeparateReboots** parameters. For more information about using multiple plug-ins, use the links provided to the cmdlet documentation in the following table.

CMDLET	DESCRIPTION
Add-CauClusterRole	Adds the CAU clustered role that provides the self-updating functionality to the specified cluster.
Invoke-CauRun	Performs a scan of cluster nodes for applicable updates and installs those updates through an Updating Run on the specified cluster.
Invoke-CauScan	Performs a scan of cluster nodes for applicable updates and returns a list of the initial set of updates that would be applied to each node in the specified cluster.
Set-CauClusterRole	Sets configuration properties for the CAU clustered role on the specified cluster.

If you do not specify a CAU plug-in parameter by using these cmdlets, the default is the plug-in **Microsoft.WindowsUpdatePlugin**.

Specify CAU plug-in arguments

When you configure the Updating Run options, you can specify one or more *name=value* pairs (arguments) for the selected plug-in to use. For example, in the CAU UI, you can specify multiple arguments as follows:

Name1=Value1;Name2=Value2;Name3=Value3

These *name=value* pairs must be meaningful to the plug-in that you specify. For some plug-ins the arguments are optional.

The syntax of the CAU plug-in arguments follows these general rules:

- Multiple *name=value* pairs are separated by semicolons.
- A value that contains spaces is surrounded by quotation marks, for example: **Name1="Value with Spaces"**.
- The exact syntax of *value* depends on the plug-in.

To specify plug-in arguments by using the CAU PowerShell cmdlets that support the **–CauPluginParameters** parameter, pass a parameter of the form:

-CauPluginArguments @{Name1=Value1;Name2=Value2;Name3=Value3}

You can also use a predefined PowerShell hash table. To specify plug-in arguments for more than one plug-in, pass multiple hash tables of arguments, separated with commas. Pass the plug-in arguments in the plug-in order that is specified in **CauPluginName**.

Specify optional plug-in arguments

The plug-ins that CAU installs (**Microsoft.WindowsUpdatePlugin** and **Microsoft.HotfixPlugin**) provide additional options that you can select. In the CAU UI, these appear on an **Additional Options** page after you configure Updating Run options for the plug-in. If you are using the CAU PowerShell cmdlets, these options are configured as optional plug-in arguments. For more information, see Use the Microsoft.WindowsUpdatePlugin and Use the Microsoft.HotfixPlugin later in this topic.

Manage plug-ins using Windows PowerShell cmdlets

CMDLET	DESCRIPTION
Get-CauPlugin	Retrieves information about one or more software updating plug-ins that are registered on the local computer.
Register-CauPlugin	Registers a CAU software updating plug-in on the local computer.
Unregister-CauPlugin	Removes a software updating plug-in from the list of plug-ins that can be used by CAU. **Note:** The plug-ins that are installed with CAU (**Microsoft.WindowsUpdatePlugin** and the **Microsoft.HotfixPlugin**) cannot be unregistered.

Using the Microsoft.WindowsUpdatePlugin

The default plug-in for CAU, **Microsoft.WindowsUpdatePlugin**, performs the following actions:

- Communicates with the Windows Update Agent on each failover cluster node to apply updates that are needed for the Microsoft products that are running on each node.
- Installs cluster updates directly from Windows Update or Microsoft Update, or from an on-premises Windows Server Update Services (WSUS) server.
- Installs only selected, general distribution release (GDR) updates. By default, the plug-in applies only important software updates. No configuration is required. The default configuration downloads and installs important GDR updates on each node.

> **NOTE**
> To apply updates other than the important software updates that are selected by default (for example, driver updates), you can configure an optional plug-in parameter. For more information, see Configure the Windows Update Agent query string.

Requirements

- The failover cluster and remote Update Coordinator computer (if used) must meet the requirements for CAU and the configuration that is required for remote management listed in Requirements and Best Practices for CAU.
- Review Recommendations for applying Microsoft updates, and then make any necessary changes to your Microsoft Update configuration for the failover cluster nodes.
- For best results, we recommend that you run the CAU Best Practices Analyzer (BPA) to ensure that the cluster and update environment are configured properly to apply updates by using CAU. For more information, see Test CAU updating readiness.

> **NOTE**
> Updates that require the acceptance of Microsoft license terms or require user interaction are excluded, and they must be installed manually.

Additional options

Optionally, you can specify the following plug-in arguments to augment or restrict the set of updates that are applied by the plug-in:

- To configure the plug-in to apply recommended updates in addition to important updates on each node, in the CAU UI, on the **Additional Options** page, select the **Give me recommended updates the same way**

that I receive important updates check box.
Alternatively, configure the **'IncludeRecommendedUpdates'='True'** plug-in argument.

- To configure the plug-in to filter the types of GDR updates that are applied to each cluster node, specify a Windows Update Agent query string using a **QueryString** plug-in argument. For more information, see Configure the Windows Update Agent query string.

Configure the Windows Update Agent query string

You can configure a plug-in argument for the default plug-in, **Microsoft.WindowsUpdatePlugin**, that consists of a Windows Update Agent (WUA) query string. This instruction uses the WUA API to identify one or more groups of Microsoft updates to apply to each node, based on specific selection criteria. You can combine multiple criteria by using a logical AND or a logical OR. The WUA query string is specified in a plug-in argument as follows:

```
QueryString="Criterion1=Value1 and/or Criterion2=Value2 and/or..."
```

For example, **Microsoft.WindowsUpdatePlugin** automatically selects important updates by using a default **QueryString** argument that is constructed using the **IsInstalled**, **Type**, **IsHidden**, and **IsAssigned** criteria:

```
QueryString="IsInstalled=0 and Type='Software' and IsHidden=0 and IsAssigned=1"
```

If you specify a **QueryString** argument, it is used in place of the default **QueryString** that is configured for the plug-in.

Example 1

To configure a **QueryString** argument that installs a specific update as identified by ID *f6ce46c1-971c-43f9-a2aa-783df125f003*:

```
QueryString="UpdateID='f6ce46c1-971c-43f9-a2aa-783df125f003' and IsInstalled=0"
```

> **NOTE**
> The preceding example is valid for applying updates by using the Cluster-Aware Updating Wizard. If you want to install a specific update by configuring self-updating options with the CAU UI or by using the **Add-CauClusterRole** or **Set-CauClusterRole**PowerShell cmdlet, you must format the UpdateID value with two single-quote characters:
>
> ```
> QueryString="UpdateID=''f6ce46c1-971c-43f9-a2aa-783df125f003'' and IsInstalled=0"
> ```

Example 2

To configure a **QueryString** argument that installs only drivers:

```
QueryString="IsInstalled=0 and Type='Driver' and IsHidden=0"
```

For more information about query strings for the default plug-in, **Microsoft.WindowsUpdatePlugin**, the search criteria (such as **IsInstalled**), and the syntax that you can include in the query strings, see the section about search criteria in the Windows Update Agent (WUA) API Reference.

Use the Microsoft.HotfixPlugin

The plug-in **Microsoft.HotfixPlugin** can be used to apply Microsoft limited distribution release (LDR) updates (also called hotfixes, and formerly called QFEs) that you download independently to address specific Microsoft software issues. The plug-in installs updates from a root folder on an SMB file share and can also be customized to apply non-Microsoft driver, firmware, and BIOS updates.

> **NOTE**
> Hotfixes are sometimes available for download from Microsoft in Knowledge Base articles, but they are also provided to customers on an as-needed basis.

Requirements

- The failover cluster and remote Update Coordinator computer (if used) must meet the requirements for CAU and the configuration that is required for remote management listed in Requirements and Best Practices for CAU.
- Review Recommendations for using the Microsoft.HotfixPlugin.
- For best results, we recommend that you run the CAU Best Practices Analyzer (BPA) model to ensure that the cluster and update environment are configured properly to apply updates by using CAU. For more information, see Test CAU updating readiness.
- Obtain the updates from the publisher, and copy them or extract them to a Server Message Block (SMB) file share (hotfix root folder) that supports at least SMB 2.0 and that is accessible by all of the cluster nodes and the remote Update Coordinator computer (if CAU is used in remote-updating mode). For more information, see Configure a hotfix root folder structure later in this topic.

  > **NOTE**
  > By default, this plug-in only installs hotfixes with the following file name extensions: .msu, .msi, and .msp.

- Copy the DefaultHotfixConfig.xml file (which is provided in the **%systemroot%\System32\WindowsPowerShell\v1.0\Modules\ClusterAwareUpdating** folder on a computer where the CAU tools are installed) to the hotfix root folder that you created and under which you extracted the hotfixes. For example, copy the configuration file to *\\MyFileServer\Hotfixes\Root*.

  > **NOTE**
  > To install most hotfixes provided by Microsoft and other updates, the default hotfix configuration file can be used without modification. If your scenario requires it, you can customize the configuration file as an advanced task. The configuration file can include custom rules, for example, to handle hotfix files that have specific extensions, or to define behaviors for specific exit conditions. For more information, see Customize the hotfix configuration file later in this topic.

Configuration

Configure the following settings. For more information, see the links to sections later in this topic.

- The path to the shared hotfix root folder that contains the updates to apply and that contains the hotfix configuration file. You can type this path in the CAU UI or configure the **HotfixRootFolderPath=<Path>** PowerShell plug-in argument.

  > **NOTE**
  > You can specify the hotfix root folder as a local folder path or as a UNC path of the form *\\ServerName\Share\RootFolderName*. A domain-based or standalone DFS Namespace path can be used. However, the plug-in features that check access permissions in the hotfix configuration file are incompatible with a DFS Namespace path, so if you configure one, you must disable the check for access permissions by using the CAU UI or by configuring the **DisableAclChecks='True'** plug-in argument.

- Settings on the server that hosts the hotfix root folder to check for appropriate permissions to access the folder and ensure the integrity of the data accessed from the SMB shared folder (SMB signing or SMB Encryption). For more information, see Restrict access to the hotfix root folder.

Additional options

- Optionally, configure the plug-in so that SMB Encryption is enforced when accessing data from the hotfix file share. In the CAU UI, on the **Additional Options** page, select the **Require SMB Encryption in accessing the hotfix root folder** option, or configure the **RequireSMBEncryption='True'** PowerShell plug-in argument.

> **IMPORTANT**
>
> You must perform additional configuration steps on the SMB server to enable SMB data integrity with SMB signing or SMB Encryption. For more information, see Step 4 in Restrict access to the hotfix root folder. If you select the option to enforce the use of SMB Encryption, and the hotfix root folder is not configured for access by using SMB Encryption, the Updating Run will fail.

- Optionally, disable the default checks for sufficient permissions for the hotfix root folder and the hotfix configuration file. In the CAU UI, select **Disable check for administrator access to the hotfix root folder and configuration file**, or configure the **DisableAclChecks='True'** plug-in argument.
- Optionally, configure the **HotfixInstallerTimeoutMinutes=<Integer>** argument to specify how long the hotfix plug-in waits for the hotfix installer process to return. (The default is 30 minutes.) For example, to specify a timeout period of two hours, set **HotfixInstallerTimeoutMinutes=120**.
- Optionally, configure the **HotfixConfigFileName = <name>** plug-in argument to specify a name for the hotfix configuration file that is located in the hotfix root folder. If not specified, the default name DefaultHotfixConfig.xml is used.

Configure a hotfix root folder structure

For the hotfix plug-in to work, hotfixes must be stored in a well-defined structure in an SMB file share (hotfix root folder), and you must configure the hotfix plug-in with the path to the hotfix root folder by using the CAU UI or the CAU PowerShell cmdlets. This path is passed to the plug-in as the **HotfixRootFolderPath** argument. You can choose one of several structures for the hotfix root folder, according to your updating needs, as shown in the following examples. Files or folders that do not adhere to the structure are ignored.

Example 1 - Folder structure used to apply hotfixes to all cluster nodes

To specify that hotfixes apply to all cluster nodes, copy them to a folder named **CAUHotfix_All** under the hotfix root folder. In this example, the **HotfixRootFolderPath** plug-in argument is set to *\\MyFileServer\Hotfixes\Root*. The **CAUHotfix_All** folder contains three updates with the extensions .msu, .msi, and .msp that will be applied to all cluster nodes. The update file names are only for illustration purposes.

> **NOTE**
>
> In this and the following examples, the hotfix configuration file with its default name DefaultHotfixConfig.xml is shown in its required location in the hotfix root folder.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...
```

Example 2 - Folder structure used to apply certain updates only to a specific node

To specify hotfixes that apply only to a specific node, use a subfolder under the hotfix root folder with the name of the node. Use the NetBIOS name of the cluster node, for example, *ContosoNode1*. Then, move the updates that apply only to this node to this subfolder. In the following example, the **HotfixRootFolderPath** plug-in argument is set to *\\MyFileServer\Hotfixes\Root*. Updates in the **CAUHotfix_All** folder will be applied to all cluster nodes, and *Node1_Specific_Update.msu* will be applied only to *ContosoNode1*.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...
   ContosoNode1\
      Node1_Specific_Update.msu
      ...
```

Example 3 - Folder structure used to apply updates other than .msu, .msi, and .msp files

By default, **Microsoft.HotfixPlugin** only applies updates with the .msu, .msi, or .msp extension. However, certain updates might have different extensions and require different installation commands. For example, you might need to apply a firmware update with the extension .exe to a node in a cluster. You can configure the hotfix root folder with a subfolder that indicates a specific, non-default update type should be installed. You must also configure a corresponding folder installation rule that specifies the installation command in the `<FolderRules>` element in the hotfix configuration XML file.

In the following example, the **HotfixRootFolderPath** plug-in argument is set to *\\MyFileServer\Hotfixes\Root*. Several updates will be applied to all cluster nodes, and a firmware update *SpecialHotfix1.exe* will be applied to *ContosoNode1* by using *FolderRule1*. For information about configuring *FolderRule1* in the hotfix configuration file, see Customize the hotfix configuration file later in this topic.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...

   ContosoNode1\
      FolderRule1\
          SpecialHotfix1.exe
      ...
```

Customize the hotfix configuration file

The hotfix configuration file controls how **Microsoft.HotfixPlugin** installs specific hotfix file types in a failover cluster. The XML schema for the configuration file is defined in HotfixConfigSchema.xsd, which is located in the following folder on a computer where the CAU tools are installed:

%systemroot%\System32\WindowsPowerShell\v1.0\Modules\ClusterAwareUpdating folder

To customize the hotfix configuration file, copy the sample configuration file DefaultHotfixConfig.xml from this location to the hotfix root folder and make appropriate modifications for your scenario.

> **IMPORTANT**
>
> To apply most hotfixes provided by Microsoft and other updates, the default hotfix configuration file can be used without modification. Customization of the hotfix configuration file is a task only in advanced usage scenarios.

By default, the hotfix configuration XML file defines installation rules and exit conditions for the following two categories of hotfixes:

- Hotfix files with extensions that the plug-in can install by default (.msu, .msi, and .msp files).

  These are defined as `<ExtensionRules>` elements in the `<DefaultRules>` element. There is one `<Extension>` element for each of the default supported file types. The general XML structure is as follows:

  ```
  <DefaultRules>
      <ExtensionRules>
        <Extension name="MSI">
          <!-- Template and ExitConditions elements for installation of .msi files follow -->
           ...
        </Extension>
        <Extension name="MSU">
          <!-- Template and ExitConditions elements for installation of .msu files follow -->
           ...
        </Extension>
        <Extension name="MSP">
          <!-- Template and ExitConditions elements for installation of .msp files follow -->
           ...
        </Extension>
           ...
     </ExtensionRules>
  </DefaultRules>
  ```

  If you need to apply certain update types to all cluster nodes in your environment, you can define additional `<Extension>` elements.

- Hotfix or other update files that are not .msi, .msu, or .msp files, for example, non-Microsoft drivers, firmware, and BIOS updates.

  Each non-default file type is configured as a `<Folder>` element in the `<FolderRules>` element. The name attribute of the `<Folder>` element must be identical to the name of a folder in the hotfix root folder that will contain updates of the corresponding type. The folder can be in the **CAUHotfix_All** folder or in a node-specific folder. For example, if *FolderRule1* is configured in the hotfix root folder, configure the following element in the XML file to define an installation template and exit conditions for the updates in that folder:

  ```
  <FolderRules>
        <Folder name="FolderRule1">
          <!-- Template and ExitConditions elements for installation of updates in FolderRule1 follow -
  ->
           ...
        </Folder>
        ...
  </FolderRules>
  ```

The following tables describe the `<Template>` attributes and the possible `<ExitConditions>` subelements.

`<TEMPLATE>` ATTRIBUTE	DESCRIPTION
`path`	The full path to the installation program for the file type that is defined in the `<Extension name>` attribute. To specify the path to an update file in the hotfix root folder structure, use `$update$`.

`<TEMPLATE>` ATTRIBUTE	DESCRIPTION
`parameters`	A string of required and optional parameters for the program that is specified in `path`. To specify a parameter that is the path to an update file in the hotfix root folder structure, use `$update$`.

`<EXITCONDITIONS>` SUBELEMENT	DESCRIPTION
`<Success>`	Defines one or more exit codes that indicate the specified update succeeded. This is a required subelement.
`<Success_RebootRequired>`	Optionally defines one or more exit codes that indicate the specified update succeeded and the node must restart. **Note:** Optionally, the `<Folder>` element can contain the `alwaysReboot` attribute. If this attribute is set, it indicates that if a hotfix installed by this rule returns one of the exit codes that is defined in `<Success>`, it is interpreted as a `<Success_RebootRequired>` exit condition.
`<Fail_RebootRequired>`	Optionally defines one or more exit codes that indicate the specified update failed and the node must restart.
`<AlreadyInstalled>`	Optionally defines one or more exit codes that indicate the specified update was not applied because it is already installed.
`<NotApplicable>`	Optionally defines one or more exit codes that indicate the specified update was not applied because it does not apply to the cluster node.

> **IMPORTANT**
> Any exit code that is not explicitly defined in `<ExitConditions>` is interpreted as the update failed, and the node does not restart.

Restrict access to the hotfix root folder

You must perform several steps to configure the SMB file server and file share to help secure the hotfix root folder files and hotfix configuration file for access only in the context of **Microsoft.HotfixPlugin**. These steps enable several features that help prevent possible tampering with the hotfix files in a way that might compromise the failover cluster.

The general steps are as follows:

1. Identify the user account that is used for Updating Runs by using the plug-in
2. Configure this user account in the necessary groups on an SMB file server
3. Configure permissions to access the hotfix root folder
4. Configure settings for SMB data integrity
5. Enable a Windows Firewall rule on the SMB server

Step 1. Identify the user account that is used for Updating Runs by using the hotfix plug-in

The account that is used in CAU to check security settings while performing an Updating Run using **Microsoft.HotfixPlugin** depends on whether CAU is used in remote-updating mode or self-updating mode, as follows:

- **Remote-updating mode** The account that has administrative privileges on the cluster to preview and apply updates.
- **Self-updating mode** The name of the virtual computer object that is configured in Active Directory for the CAU clustered role. This is either the name of a prestaged virtual computer object in Active Directory for the CAU clustered role or the name that is generated by CAU for the clustered role. To obtain the name if it is generated by CAU, run the **Get-CauClusterRole** CAU PowerShell cmdlet. In the output, **ResourceGroupName** is the name of the generated virtual computer object account.

Step 2. Configure this user account in the necessary groups on an SMB file server

> **IMPORTANT**
> You must add the account that is used for Updating Runs as a local administrator account on the SMB server. If this is not permitted because of the security policies in your organization, configure this account with the necessary permissions on the SMB server by using the following procedure.

To configure a user account on the SMB server

1. Add the account that is used for Updating Runs to the Distributed COM Users group and to one of the following groups: Power User, Server Operation, or Print Operator.
2. To enable the necessary WMI permissions for the account, start the WMI Management Console on the SMB server. Start PowerShell and then type the following command:

   ```
   wmimgmt.msc
   ```

3. In the console tree, right-click **WMI Control (Local)**, and then click **Properties**.
4. Click **Security**, and then expand **Root**.
5. Click **CIMV2**, and then click **Security**.
6. Add the account that is used for Updating Runs to the **Group or user names** list.
7. Grant the **Execute Methods** and **Remote Enable** permissions to the account that is used for Updating Runs.

Step 3. Configure permissions to access the hotfix root folder

By default, when you attempt to apply updates, the hotfix plug-in checks the configuration of the NTFS file system permissions for access to the hotfix root folder. If the folder access permissions are not configured properly, an Updating Run using the hotfix plug-in might fail.

If you use the default configuration of the hotfix plug-in, ensure that the folder access permissions meet the following requirements.

- The Users group has Read permission.
- If the plug-in will apply updates with the .exe extension, the Users group has Execute permission.
- Only certain security principals are permitted (but are not required) to have Write or Modify permission. The allowed principals are the local Administrators group, SYSTEM, CREATOR OWNER, and TrustedInstaller. Other accounts or groups are not permitted to have Write or Modify permission on the hotfix root folder.

Optionally, you can disable the preceding checks that the plug-in performs by default. You can do this in one of

two ways:

- If you are using the CAU PowerShell cmdlets, configure the **DisableAclChecks='True'** argument in the **CauPluginArguments** parameter for the hotfix plug-in.
- If you are using the CAU UI, select the **Disable check for administrator access to the hotfix root folder and configuration file** option on the **Additional Update Options** page of the wizard that is used to configure Updating Run options.

However, as a best practice in many environments, we recommend that you use the default configuration to enforce these checks.

Step 4. Configure settings for SMB data integrity

To check for data integrity in the connections between the cluster nodes and the SMB file share, the hotfix plug-in requires that you enable settings on the SMB file share for SMB signing or SMB Encryption. SMB Encryption, which provides enhanced security and better performance in many environments, is supported starting in Windows Server 2012. You can enable either or both of these settings, as follows:

- To enable SMB signing, see the procedure in the article 887429 in the Microsoft Knowledge Base.
- To enable SMB Encryption for the SMB shared folder, run the following PowerShell cmdlet on the SMB server:

  ```
  Set-SmbShare <ShareName> -EncryptData $true
  ```

  Where <*ShareName*> is the name of the SMB shared folder.

Optionally, to enforce the use of SMB Encryption in the connections to the SMB server, select the **Require SMB Encryption in accessing the hotfix root folder** option in the CAU UI, or configure the **RequireSMBEncryption='True'** plug-in argument by using the CAU PowerShell cmdlets.

> **IMPORTANT**
>
> If you select the option to enforce the use of SMB Encryption, and the hotfix root folder is not configured for connections that use SMB Encryption, the Updating Run will fail.

Step 5. Enable a Windows Firewall rule on the SMB server

You must enable the **File Server Remote Management (SMB-in)** rule in Windows Firewall on the SMB file server. This is enabled by default in Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012.

Additional References

- Cluster-Aware Updating Overview
- Cluster-Aware Updating Windows PowerShell Cmdlets
- Cluster-Aware Updating Plug-in Reference

Health Service reports

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2016

What are reports

The Health Service reduces the work required to get live performance and capacity information from your Storage Spaces Direct cluster. One new cmdlet provides a curated list of essential metrics, which are collected efficiently and aggregated dynamically across nodes, with built-in logic to detect cluster membership. All values are real-time and point-in-time only.

Usage in PowerShell

Use this cmdlet to get metrics for the entire Storage Spaces Direct cluster:

```
Get-StorageSubSystem Cluster* | Get-StorageHealthReport
```

The optional **Count** parameter indicates how many sets of values to return, at one second intervals.

```
Get-StorageSubSystem Cluster* | Get-StorageHealthReport -Count <Count>
```

You can also get metrics for one specific volume or server:

```
Get-Volume -FileSystemLabel <Label> | Get-StorageHealthReport -Count <Count>

Get-StorageNode -Name <Name> | Get-StorageHealthReport -Count <Count>
```

Usage in .NET and C#

Connect

In order to query the Health Service, you will need to establish a **CimSession** with the cluster. To do so, you will need some things that are only available in full .NET, meaning you cannot readily do this directly from a web or mobile app. These code samples will use C#, the most straightforward choice for this data access layer.

```
using System.Security;
using Microsoft.Management.Infrastructure;

public CimSession Connect(string Domain = "...", string Computer = "...", string Username = "...", string
Password = "...")
{
    SecureString PasswordSecureString = new SecureString();
    foreach (char c in Password)
    {
        PasswordSecureString.AppendChar(c);
    }

    CimCredential Credentials = new CimCredential(
        PasswordAuthenticationMechanism.Default, Domain, Username, PasswordSecureString);
    WSManSessionOptions SessionOptions = new WSManSessionOptions();
    SessionOptions.AddDestinationCredentials(Credentials);
    Session = CimSession.Create(Computer, SessionOptions);
    return Session;
}
```

The provided Username should be a local Administrator of the target Computer.

It is recommended that you construct the Password **SecureString** directly from user input in real-time, so their password is never stored in memory in cleartext. This helps mitigate a variety of security concerns. But in practice, constructing it as above is common for prototyping purposes.

Discover objects

With the **CimSession** established, you can query Windows Management Instrumentation (WMI) on the cluster.

Before you can get faults or metrics, you will need to get instances of several relevant objects. First, the **MSFT_StorageSubSystem** which represents Storage Spaces Direct on the cluster. Using that, you can get every **MSFT_StorageNode** in the cluster, and every **MSFT_Volume**, the data volumes. Finally, you will need the **MSFT_StorageHealth**, the Health Service itself, too.

```
CimInstance Cluster;
List<CimInstance> Nodes;
List<CimInstance> Volumes;
CimInstance HealthService;

public void DiscoverObjects(CimSession Session)
{
    // Get MSFT_StorageSubSystem for Storage Spaces Direct
    Cluster = Session.QueryInstances(@"root\microsoft\windows\storage", "WQL", "SELECT * FROM
MSFT_StorageSubSystem")
        .First(Instance =>
(Instance.CimInstanceProperties["FriendlyName"].Value.ToString()).Contains("Cluster"));

    // Get MSFT_StorageNode for each cluster node
    Nodes = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToStorageNode", null, "StorageSubSystem", "StorageNode").ToList();

    // Get MSFT_Volumes for each data volume
    Volumes = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToVolume", null, "StorageSubSystem", "Volume").ToList();

    // Get MSFT_StorageHealth itself
    HealthService = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToStorageHealth", null, "StorageSubSystem", "StorageHealth").First();
}
```

These are the same objects you get in PowerShell using cmdlets like **Get-StorageSubSystem**, **Get-StorageNode**, and **Get-Volume**.

You can access all the same properties, documented at Storage Management API Classes.

```
using System.Diagnostics;

foreach (CimInstance Node in Nodes)
{
    // For illustration, write each node's Name to the console. You could also write State (up/down), or
anything else!
    Debug.WriteLine("Discovered Node " + Node.CimInstanceProperties["Name"].Value.ToString());
}
```

Invoke **GetReport** to begin streaming samples of an expert-curated list of essential metrics, which are collected efficiently and aggregated dynamically across nodes, with built-in logic to detect cluster membership. Samples will arrive every second thereafter. All values are real-time and point-in-time only.

Metrics can be streamed for three scopes: the cluster, any node, or any volume.

The complete list of metrics available at each scope in Windows Server 2016 is documented below.

IObserver.OnNext()

This sample code uses the Observer Design Pattern to implement an Observer whose **OnNext()** method will be invoked when each new sample of metrics arrives. Its **OnCompleted()** method will be called if/when streaming ends. For example, you might use it to reinitiate streaming, so it continues indefinitely.

```
class MetricsObserver<T> : IObserver<T>
{
    public void OnNext(T Result)
    {
        // Cast
        CimMethodStreamedResult StreamedResult = Result as CimMethodStreamedResult;

        if (StreamedResult != null)
        {
            // For illustration, you could store the metrics in this dictionary
            Dictionary<string, string> Metrics = new Dictionary<string, string>();

            // Unpack
            CimInstance Report = (CimInstance)StreamedResult.ItemValue;
            IEnumerable<CimInstance> Records =
(IEnumerable<CimInstance>)Report.CimInstanceProperties["Records"].Value;
            foreach (CimInstance Record in Records)
            {
                /// Each Record has "Name", "Value", and "Units"
                Metrics.Add(
                    Record.CimInstanceProperties["Name"].Value.ToString(),
                    Record.CimInstanceProperties["Value"].Value.ToString()
                    );
            }

            // TODO: Whatever you want!
        }
    }
    public void OnError(Exception e)
    {
        // Handle Exceptions
    }
    public void OnCompleted()
    {
        // Reinvoke BeginStreamingMetrics(), defined in the next section
    }
}
```

Begin streaming

With the Observer defined, you can begin streaming.

Specify the target **CimInstance** to which you want the metrics scoped. It can be the cluster, any node, or any volume.

The count parameter is the number of samples before streaming ends.

```
CimInstance Target = Cluster; // From among the objects discovered in DiscoverObjects()

public void BeginStreamingMetrics(CimSession Session, CimInstance HealthService, CimInstance Target)
{
    // Set Parameters
    CimMethodParametersCollection MetricsParams = new CimMethodParametersCollection();
    MetricsParams.Add(CimMethodParameter.Create("TargetObject", Target, CimType.Instance, CimFlags.In));
    MetricsParams.Add(CimMethodParameter.Create("Count", 999, CimType.UInt32, CimFlags.In));
    // Enable WMI Streaming
    CimOperationOptions Options = new CimOperationOptions();
    Options.EnableMethodResultStreaming = true;
    // Invoke API
    CimAsyncMultipleResults<CimMethodResultBase> InvokeHandler;
    InvokeHandler = Session.InvokeMethodAsync(
        HealthService.CimSystemProperties.Namespace, HealthService, "GetReport", MetricsParams, Options
        );
    // Subscribe the Observer
    MetricsObserver<CimMethodResultBase> Observer = new MetricsObserver<CimMethodResultBase>(this);
    IDisposable Disposeable = InvokeHandler.Subscribe(Observer);
}
```

Needless to say, these metrics can be visualized, stored in a database, or used in whatever way you see fit.

Properties of reports

Every sample of metrics is one "report" which contains many "records" corresponding to individual metrics.

For the full schema, inspect the **MSFT_StorageHealthReport** and **MSFT_HealthRecord** classes in *storagewmi.mof*.

Each metric has just three properties, per this table.

PROPERTY	EXAMPLE
Name	IOLatencyAverage
Value	0.00021
Units	3

Units = { 0, 1, 2, 3, 4 }, where 0 = "Bytes", 1 = "BytesPerSecond", 2 = "CountPerSecond", 3 = "Seconds", or 4 = "Percentage".

Coverage

Below are the metrics available for each scope in Windows Server 2016.

MSFT_StorageSubSystem

NAME	UNITS
CPUUsage	4

NAME	UNITS
CapacityPhysicalPooledAvailable	0
CapacityPhysicalPooledTotal	0
CapacityPhysicalTotal	0
CapacityPhysicalUnpooled	0
CapacityVolumesAvailable	0
CapacityVolumesTotal	0
IOLatencyAverage	3
IOLatencyRead	3
IOLatencyWrite	3
IOPSRead	2
IOPSTotal	2
IOPSWrite	2
IOThroughputRead	1
IOThroughputTotal	1
IOThroughputWrite	1
MemoryAvailable	0
MemoryTotal	0

MSFT_StorageNode

NAME	UNITS
CPUUsage	4
IOLatencyAverage	3
IOLatencyRead	3
IOLatencyWrite	3
IOPSRead	2
IOPSTotal	2

NAME	UNITS
IOPSWrite	2
IOThroughputRead	1
IOThroughputTotal	1
IOThroughputWrite	1
MemoryAvailable	0
MemoryTotal	0

MSFT_Volume

NAME	UNITS
CapacityAvailable	0
CapacityTotal	0
IOLatencyAverage	3
IOLatencyRead	3
IOLatencyWrite	3
IOPSRead	2
IOPSTotal	2
IOPSWrite	2
IOThroughputRead	1
IOThroughputTotal	1
IOThroughputWrite	1

Additional References

- Health Service in Windows Server 2016

Health Service faults

12/9/2022 • 13 minutes to read • Edit Online

Applies to: Windows Server 2016

What are faults

The Health Service constantly monitors your Storage Spaces Direct cluster to detect problems and generate "faults". One new cmdlet displays any current faults, allowing you to easily verify the health of your deployment without looking at every entity or feature in turn. Faults are designed to be precise, easy to understand, and actionable.

Each fault contains five important fields:

- Severity
- Description of the problem
- Recommended next step(s) to address the problem
- Identifying information for the faulting entity
- Its physical location (if applicable)

For example, here is a typical fault:

```
Severity: MINOR
Reason: Connectivity has been lost to the physical disk.
Recommendation: Check that the physical disk is working and properly connected.
Part: Manufacturer Contoso, Model XYZ9000, Serial 123456789
Location: Seattle DC, Rack B07, Node 4, Slot 11
```

> **NOTE**
>
> The physical location is derived from your fault domain configuration. For more information about fault domains, see Fault Domains in Windows Server 2016. If you do not provide this information, the location field will be less helpful - for example, it may only show the slot number.

Root cause analysis

The Health Service can assess the potential causality among faulting entities to identify and combine faults which are consequences of the same underlying problem. By recognizing chains of effect, this makes for less chatty reporting. For example, if a server is down, it is expected than any drives within the server will also be without connectivity. Therefore, only one fault will be raised for the root cause - in this case, the server.

Usage in PowerShell

To see any current faults in PowerShell, run this cmdlet:

```
Get-StorageSubSystem Cluster* | Debug-StorageSubSystem
```

This returns any faults which affect the overall Storage Spaces Direct cluster. Most often, these faults relate to hardware or configuration. If there are no faults, this cmdlet will return nothing.

> **NOTE**
> In a non-production environment, and at your own risk, you can experiment with this feature by triggering faults yourself - for example, by removing one physical disk or shutting down one node. Once the fault has appeared, re-insert the physical disk or restart the node and the fault will disappear again.

You can also view faults that are affecting only specific volumes or file shares with the following cmdlets:

```
Get-Volume -FileSystemLabel <Label> | Debug-Volume

Get-FileShare -Name <Name> | Debug-FileShare
```

This returns any faults that affect only the specific volume or file share. Most often, these faults relate to capacity planning, data resiliency, or features like Storage Quality-of-Service or Storage Replica.

Usage in .NET and C#

Connect

In order to query the Health Service, you will need to establish a **CimSession** with the cluster. To do so, you will need some things that are only available in full .NET, meaning you cannot readily do this directly from a web or mobile app. These code samples will use C#, the most straightforward choice for this data access layer.

```
using System.Security;
using Microsoft.Management.Infrastructure;

public CimSession Connect(string Domain = "...", string Computer = "...", string Username = "...", string
Password = "...")
{
    SecureString PasswordSecureString = new SecureString();
    foreach (char c in Password)
    {
        PasswordSecureString.AppendChar(c);
    }

    CimCredential Credentials = new CimCredential(
        PasswordAuthenticationMechanism.Default, Domain, Username, PasswordSecureString);
    WSManSessionOptions SessionOptions = new WSManSessionOptions();
    SessionOptions.AddDestinationCredentials(Credentials);
    Session = CimSession.Create(Computer, SessionOptions);
    return Session;
}
```

The provided Username should be a local Administrator of the target Computer.

It is recommended that you construct the Password **SecureString** directly from user input in real-time, so their password is never stored in memory in cleartext. This helps mitigate a variety of security concerns. But in practice, constructing it as above is common for prototyping purposes.

Discover objects

With the **CimSession** established, you can query Windows Management Instrumentation (WMI) on the cluster.

Before you can get Faults or Metrics, you will need to get instances of several relevant objects. First, the **MSFT_StorageSubSystem** which represents Storage Spaces Direct on the cluster. Using that, you can get every **MSFT_StorageNode** in the cluster, and every **MSFT_Volume**, the data volumes. Finally, you will need the **MSFT_StorageHealth**, the Health Service itself, too.

```
CimInstance Cluster;
List<CimInstance> Nodes;
List<CimInstance> Volumes;
CimInstance HealthService;

public void DiscoverObjects(CimSession Session)
{
    // Get MSFT_StorageSubSystem for Storage Spaces Direct
    Cluster = Session.QueryInstances(@"root\microsoft\windows\storage", "WQL", "SELECT * FROM
MSFT_StorageSubSystem")
        .First(Instance =>
(Instance.CimInstanceProperties["FriendlyName"].Value.ToString()).Contains("Cluster"));

    // Get MSFT_StorageNode for each cluster node
    Nodes = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToStorageNode", null, "StorageSubSystem", "StorageNode").ToList();

    // Get MSFT_Volumes for each data volume
    Volumes = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToVolume", null, "StorageSubSystem", "Volume").ToList();

    // Get MSFT_StorageHealth itself
    HealthService = Session.EnumerateAssociatedInstances(Cluster.CimSystemProperties.Namespace,
        Cluster, "MSFT_StorageSubSystemToStorageHealth", null, "StorageSubSystem", "StorageHealth").First();
}
```

These are the same objects you get in PowerShell using cmdlets like **Get-StorageSubSystem**, **Get-StorageNode**, and **Get-Volume**.

You can access all the same properties, documented at Storage Management API Classes.

```
using System.Diagnostics;

foreach (CimInstance Node in Nodes)
{
    // For illustration, write each node's Name to the console. You could also write State (up/down), or
anything else!
    Debug.WriteLine("Discovered Node " + Node.CimInstanceProperties["Name"].Value.ToString());
}
```

Query faults

Invoke **Diagnose** to get any current faults scoped to the target **CimInstance**, which be the cluster or any volume.

The complete list of faults available at each scope in Windows Server 2016 is documented below.

```
public void GetFaults(CimSession Session, CimInstance Target)
{
    // Set Parameters (None)
    CimMethodParametersCollection FaultsParams = new CimMethodParametersCollection();
    // Invoke API
    CimMethodResult Result = Session.InvokeMethod(Target, "Diagnose", FaultsParams);
    IEnumerable<CimInstance> DiagnoseResults =
(IEnumerable<CimInstance>)Result.OutParameters["DiagnoseResults"].Value;
    // Unpack
    if (DiagnoseResults != null)
    {
        foreach (CimInstance DiagnoseResult in DiagnoseResults)
        {
            // TODO: Whatever you want!
        }
    }
}
```

Optional: MyFault class

It may make sense for you to construct and persist your own representation of faults. For example, this **MyFault** class stores several key properties of faults, including the **FaultId**, which can be used later to associate update or remove notifications, or to deduplicate in the event that the same fault is detected multiple times, for whatever reason.

```
public class MyFault {
    public String FaultId { get; set; }
    public String Reason { get; set; }
    public String Severity { get; set; }
    public String Description { get; set; }
    public String Location { get; set; }

    // Constructor
    public MyFault(CimInstance DiagnoseResult)
    {
        CimKeyedCollection<CimProperty> Properties = DiagnoseResult.CimInstanceProperties;
        FaultId     = Properties["FaultId"                  ].Value.ToString();
        Reason      = Properties["Reason"                   ].Value.ToString();
        Severity    = Properties["PerceivedSeverity"        ].Value.ToString();
        Description = Properties["FaultingObjectDescription"].Value.ToString();
        Location    = Properties["FaultingObjectLocation"   ].Value.ToString();
    }
}
```

```
List<MyFault> Faults = new List<MyFault>;

foreach (CimInstance DiagnoseResult in DiagnoseResults)
{
    Faults.Add(new Fault(DiagnoseResult));
}
```

The complete list of properties in each fault (**DiagnoseResult**) is documented below.

Fault events

When Faults are created, removed, or updated, the Health Service generates WMI events. These are essential to keeping your application state in sync without frequent polling, and can help with things like determining when to send email alerts, for example. To subscribe to these events, this sample code uses the Observer Design Pattern again.

First, subscribe to **MSFT_StorageFaultEvent** events.

```
public void ListenForFaultEvents()
{
    IObservable<CimSubscriptionResult> Events = Session.SubscribeAsync(
        @"root\microsoft\windows\storage", "WQL", "SELECT * FROM MSFT_StorageFaultEvent");
    // Subscribe the Observer
    FaultsObserver<CimSubscriptionResult> Observer = new FaultsObserver<CimSubscriptionResult>(this);
    IDisposable Disposeable = Events.Subscribe(Observer);
}
```

Next, implement an Observer whose **OnNext()** method will be invoked whenever a new event is generated.

Each event contains **ChangeType** indicating whether a fault is being created, removed, or updated, and the relevant **FaultId**.

In addition, they contain all the properties of the fault itself.

```
class FaultsObserver : IObserver
{
    public void OnNext(T Event)
    {
        // Cast
        CimSubscriptionResult SubscriptionResult = Event as CimSubscriptionResult;

        if (SubscriptionResult != null)
        {
            // Unpack
            CimKeyedCollection<CimProperty> Properties = SubscriptionResult.Instance.CimInstanceProperties;
            String ChangeType = Properties["ChangeType"].Value.ToString();
            String FaultId = Properties["FaultId"].Value.ToString();

            // Create
            if (ChangeType == "0")
            {
                Fault MyNewFault = new MyFault(SubscriptionResult.Instance);
                // TODO: Whatever you want!
            }
            // Remove
            if (ChangeType == "1")
            {
                // TODO: Use FaultId to find and delete whatever representation you have...
            }
            // Update
            if (ChangeType == "2")
            {
                // TODO: Use FaultId to find and modify whatever representation you have...
            }
        }
    }
    public void OnError(Exception e)
    {
        // Handle Exceptions
    }
    public void OnCompleted()
    {
        // Nothing
    }
}
```

Understand fault lifecycle

Faults are not intended to be marked "seen" or resolved by the user. They are created when the Health Service observes a problem, and they are removed automatically and only when the Health Service can no longer observe the problem. In general, this reflects that the problem has been fixed.

However, in some cases, faults may be rediscovered by the Health Service (e.g. after failover, or due to intermittent connectivity, etc.). For this reason, it may makes sense to persist your own representation of faults, so you can easily deduplicate. This is especially important if you send email alerts or equivalent.

Properties of faults

This table presents several key properties of the fault object. For the full schema, inspect the **MSFT_StorageDiagnoseResult** class in *storagewmi.mof*.

PROPERTY	EXAMPLE
FaultId	{12345-12345-12345-12345-12345}
FaultType	Microsoft.Health.FaultType.Volume.Capacity
Reason	"The volume is running out of available space."
PerceivedSeverity	5
FaultingObjectDescription	Contoso XYZ9000 S.N. 123456789
FaultingObjectLocation	Rack A06, RU 25, Slot 11
RecommendedActions	{"Expand the volume.", "Migrate workloads to other volumes."}

FaultId Unique within the scope of one cluster.

PerceivedSeverity PerceivedSeverity = { 4, 5, 6 } = { "Informational", "Warning", and "Error" }, or equivalent colors such as blue, yellow, and red.

FaultingObjectDescription Part information for hardware, typically blank for software objects.

FaultingObjectLocation Location information for hardware, typically blank for software objects.

RecommendedActions List of recommended actions, which are independent and in no particular order. Today, this list is often of length 1.

Properties of fault events

This table presents several key properties of the fault event. For the full schema, inspect the **MSFT_StorageFaultEvent** class in *storagewmi.mof*.

Note the **ChangeType**, which indicates whether a fault is being created, removed, or updated, and the **FaultId**. An event also contains all the properties of the affected fault.

PROPERTY	EXAMPLE
ChangeType	0
FaultId	{12345-12345-12345-12345-12345}
FaultType	Microsoft.Health.FaultType.Volume.Capacity
Reason	"The volume is running out of available space."

PROPERTY	EXAMPLE
PerceivedSeverity	5
FaultingObjectDescription	Contoso XYZ9000 S.N. 123456789
FaultingObjectLocation	Rack A06, RU 25, Slot 11
RecommendedActions	{"Expand the volume.", "Migrate workloads to other volumes."}

ChangeType ChangeType = { 0, 1, 2 } = { "Create", "Remove", "Update" }.

Coverage

In Windows Server 2016, the Health Service provides the following fault coverage:

PhysicalDisk (8)

FaultType: Microsoft.Health.FaultType.PhysicalDisk.FailedMedia

- Severity: Warning
- Reason: *"The physical disk has failed."*
- RecommendedAction: *"Replace the physical disk."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.LostCommunication

- Severity: Warning
- Reason: *"Connectivity has been lost to the physical disk."*
- RecommendedAction: *"Check that the physical disk is working and properly connected."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.Unresponsive

- Severity: Warning
- Reason: *"The physical disk is exhibiting recurring unresponsiveness."*
- RecommendedAction: *"Replace the physical disk."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.PredictiveFailure

- Severity: Warning
- Reason: *"A failure of the physical disk is predicted to occur soon."*
- RecommendedAction: *"Replace the physical disk."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.UnsupportedHardware

- Severity: Warning
- Reason: *"The physical disk is quarantined because it is not supported by your solution vendor."*
- RecommendedAction: *"Replace the physical disk with supported hardware."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.UnsupportedFirmware

- Severity: Warning
- Reason: *"The physical disk is in quarantine because its firmware version is not supported by your solution vendor."*
- RecommendedAction: *"Update the firmware on the physical disk to the target version."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.UnrecognizedMetadata

- Severity: Warning
- Reason: *"The physical disk has unrecognized meta data."*
- RecommendedAction: *"This disk may contain data from an unknown storage pool. First make sure there is no useful data on this disk, then reset the disk."*

FaultType: Microsoft.Health.FaultType.PhysicalDisk.FailedFirmwareUpdate

- Severity: Warning
- Reason: *"Failed attempt to update firmware on the physical disk."*
- RecommendedAction: *"Try using a different firmware binary."*

Virtual Disk (2)

FaultType: Microsoft.Health.FaultType.VirtualDisks.NeedsRepair

- Severity: Informational
- Reason: *"Some data on this volume is not fully resilient. It remains accessible."*
- RecommendedAction: *"Restoring resiliency of the data."*

FaultType: Microsoft.Health.FaultType.VirtualDisks.Detached

- Severity: Critical
- Reason: *"The volume is inaccessible. Some data may be lost."*
- RecommendedAction: *"Check the physical and/or network connectivity of all storage devices. You may need to restore from backup."*

Pool Capacity (1)

FaultType: Microsoft.Health.FaultType.StoragePool.InsufficientReserveCapacityFault

- Severity: Warning
- Reason: *"The storage pool does not have the minimum recommended reserve capacity. This may limit your ability to restore data resiliency in the event of drive failure(s)."*
- RecommendedAction: *"Add additional capacity to the storage pool, or free up capacity. The minimum recommended reserve varies by deployment, but is approximately 2 drives' worth of capacity."*

Volume Capacity (2)[1]

FaultType: Microsoft.Health.FaultType.Volume.Capacity

- Severity: Warning
- Reason: *"The volume is running out of available space."*
- RecommendedAction: *"Expand the volume or migrate workloads to other volumes."*

FaultType: Microsoft.Health.FaultType.Volume.Capacity

- Severity: Critical
- Reason: *"The volume is running out of available space."*
- RecommendedAction: *"Expand the volume or migrate workloads to other volumes."*

Server (3)

FaultType: Microsoft.Health.FaultType.Server.Down

- Severity: Critical
- Reason: *"The server cannot be reached."*
- RecommendedAction: *"Start or replace server."*

FaultType: Microsoft.Health.FaultType.Server.Isolated

- Severity: Critical
- Reason: *"The server is isolated from the cluster due to connectivity issues."*
- RecommendedAction: *"If isolation persists, check the network(s) or migrate workloads to other nodes."*

FaultType: Microsoft.Health.FaultType.Server.Quarantined

- Severity: Critical
- Reason: *"The server is quarantined by the cluster due to recurring failures."*
- RecommendedAction: *"Replace the server or fix the network."*

Cluster (1)

FaultType: Microsoft.Health.FaultType.ClusterQuorumWitness.Error

- Severity: Critical
- Reason: *"The cluster is one server failure away from going down."*
- RecommendedAction: *"Check the witness resource, and restart as needed. Start or replace failed servers."*

Network Adapter/Interface (4)

FaultType: Microsoft.Health.FaultType.NetworkAdapter.Disconnected

- Severity: Warning
- Reason: *"The network interface has become disconnected."*
- RecommendedAction: *"Reconnect the network cable."*

FaultType: Microsoft.Health.FaultType.NetworkInterface.Missing

- Severity: Warning
- Reason: *"The server {server} has missing network adapter(s) connected to cluster network {cluster network}."*
- RecommendedAction: *"Connect the server to the missing cluster network."*

FaultType: Microsoft.Health.FaultType.NetworkAdapter.Hardware

- Severity: Warning
- Reason: *"The network interface has had a hardware failure."*
- RecommendedAction: *"Replace the network interface adapter."*

FaultType: Microsoft.Health.FaultType.NetworkAdapter.Disabled

- Severity: Warning
- Reason: *"The network interface {network interface} is not enabled and is not being used."*
- RecommendedAction: *"Enable the network interface."*

Enclosure (6)

FaultType: Microsoft.Health.FaultType.StorageEnclosure.LostCommunication

- Severity: Warning
- Reason: *"Communication has been lost to the storage enclosure."*
- RecommendedAction: *"Start or replace the storage enclosure."*

FaultType: Microsoft.Health.FaultType.StorageEnclosure.FanError

- Severity: Warning
- Reason: *"The fan at position {position} of the storage enclosure has failed."*
- RecommendedAction: *"Replace the fan in the storage enclosure."*

FaultType: Microsoft.Health.FaultType.StorageEnclosure.CurrentSensorError

- Severity: Warning
- Reason: *"The current sensor at position {position} of the storage enclosure has failed."*
- RecommendedAction: *"Replace a current sensor in the storage enclosure."*

FaultType: Microsoft.Health.FaultType.StorageEnclosure.VoltageSensorError

- Severity: Warning
- Reason: *"The voltage sensor at position {position} of the storage enclosure has failed."*
- RecommendedAction: *"Replace a voltage sensor in the storage enclosure."*

FaultType: Microsoft.Health.FaultType.StorageEnclosure.IoControllerError

- Severity: Warning
- Reason: *"The IO controller at position {position} of the storage enclosure has failed."*
- RecommendedAction: *"Replace an IO controller in the storage enclosure."*

FaultType: Microsoft.Health.FaultType.StorageEnclosure.TemperatureSensorError

- Severity: Warning
- Reason: *"The temperature sensor at position {position} of the storage enclosure has failed."*

- RecommendedAction: *"Replace a temperature sensor in the storage enclosure."*

Firmware Rollout (3)

FaultType: Microsoft.Health.FaultType.FaultDomain.FailedMaintenanceMode

- Severity: Warning
- Reason: *"Currently unable to make progress while performing firmware roll out."*
- RecommendedAction: *"Verify all storage spaces are healthy, and that no fault domain is currently in maintenance mode."*

FaultType: Microsoft.Health.FaultType.FaultDomain.FirmwareVerifyVersionFaile

- Severity: Warning
- Reason: *"Firmware roll out was canceled due to unreadable or unexpected firmware version information after applying a firmware update."*
- RecommendedAction: *"Restart firmware roll out once the firmware issue has been resolved."*

FaultType: Microsoft.Health.FaultType.FaultDomain.TooManyFailedUpdates

- Severity: Warning
- Reason: *"Firmware roll out was canceled due to too many physical disks failing a firmware update attempt."*
- RecommendedAction: *"Restart firmware roll out once the firmware issue has been resolved."*

Storage QoS (3)[2]

FaultType: Microsoft.Health.FaultType.StorQos.InsufficientThroughput

- Severity: Warning
- Reason: *"Storage throughput is insufficient to satisfy reserves."*
- RecommendedAction: *"Reconfigure Storage QoS policies."*

FaultType: Microsoft.Health.FaultType.StorQos.LostCommunication

- Severity: Warning
- Reason: *"The Storage QoS policy manager has lost communication with the volume."*
- RecommendedAction: *"Please reboot nodes {nodes}"*

FaultType: Microsoft.Health.FaultType.StorQos.MisconfiguredFlow

- Severity: Warning
- Reason: *"One or more storage consumers (usually Virtual Machines) are using a non-existent policy with id {id}."*
- RecommendedAction: *"Recreate any missing Storage QoS policies."*

[1] Indicates the volume has reached 80% full (minor severity) or 90% full (major severity). [2] Indicates some .vhd(s) on the volume have not met their Minimum IOPS for over 10% (minor), 30% (major), or 50% (critical) of rolling 24-hour window.

> **NOTE**
> The health of storage enclosure components such as fans, power supplies, and sensors is derived from SCSI Enclosure Services (SES). If your vendor does not provide this information, the Health Service cannot display it.

Additional References

- Health Service in Windows Server 2016

Failover Cluster domain migration

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic provides an overview for moving Windows Server failover clusters from one domain to another.

Why migrate between domains

There are several scenarios where migrating a cluster from one doamin to another is necessary.

- CompanyA merges with CompanyB and must move all clusters into CompanyA domain
- Clusters are built in the main datacenter and shipped out to remote locations
- Cluster was built as a workgroup cluster and now needs to be part of a domain
- Cluster was built as a domain cluster and now needs to be part of a workgroup
- Cluster is being moved to one area of the company to another and is a different subdomain

Microsoft doesn't provide support to administrators who try to move resources from one domain to another if the underlying application operation is unsupported. For example, Microsoft doesn't provide support to administrators who try to move a Microsoft Exchange server from one domain to another.

> **WARNING**
>
> We recommend that you perform a full backup of all shared storage in the cluster before you move the cluster.

Windows Server 2016 and earlier

In Windows Server 2016 and earlier, the Cluster service didn't have the capability of moving from one domain to another. This was due to the increased dependence on Active Directory Domain Services and the virtual names created.

Options

In order to do such a move, there are two options.

The first option involves destroying the cluster and rebuilding it in the new domain.

Previously, changing domains were destructive

As the animation shows, this option is destructive with the steps being:

1. Destroy the Cluster.
2. Change the domain membership of the nodes into the new domain.
3. Recreate the Cluster as new in the updated domain. This would entail having to recreate all the resources.

The second option is less destructive but requires additional hardware as a new cluster would need to be built in the new domain. Once the cluster is in the new domain, run the Cluster Migration Wizard to migrate the resources. Note that this doesn't migrate data - you'll need to use another tool to migrate data, such as Storage Migration Service(once cluster support is added).

Migration of resources is an option

As the animation shows, this option is not destructive but does require either different hardware or a node from the existing cluster than has been removed.

1. Create a new clusterin the new domain while still having the old cluster available.
2. Use the Cluster Migration Wizard to migrate all the resources to the new cluster. Reminder, this does not copy data, so will need to be done separately.

3. Decommission or destroy the old cluster.

In both options, the new cluster would need to have all cluster-aware applications installed, drivers all up-to-date, and possibly testing to ensure all will run properly. This is a time consuming process if data also needs to be moved.

Windows Server 2019

In Windows Server 2019, we introduced cross cluster domain migration capabilities. So now, the scenarios listed above can easily be done and the need of rebuilding is no longer needed.

Moving a cluster from one domain is a straight-forward process. To accomplish this, there are two new PowerShell commandlets.

New-ClusterNameAccount – creates a Cluster Name Account in Active Directory **Remove-ClusterNameAccount** – removes the Cluster Name Accounts from Active Directory

The process to accomplish this is to change the cluster from one domain to a workgroup and back to the new domain. The need to destroy a cluster, rebuild a cluster, install applications, etc is not a requirement. For example, it would look like this:

Cross Domain Cluster Migration

Migrating a cluster to a new domain

In the following steps, a cluster is being moved from the Contoso.com domain to the new Fabrikam.com domain. The cluster name is *CLUSCLUS* and with a file server role called *FS-CLUSCLUS*.

1. Create a local Administrator account with the same name and password on all servers in the cluster. This may be needed to log in while the servers are moving between domains.

2. Sign in to the first server with a domain user or administrator account that has Active Directory permissions to the Cluster Name Object (CNO), Virtual Computer Objects (VCO), has access to the Cluster, and open PowerShell.

3. Ensure all Cluster Network Name resources are in an Offline state and run the below command. This command will remove the Active Directory objects that the cluster may have.

```
Remove-ClusterNameAccount -Cluster CLUSCLUS -DeleteComputerObjects
```

4. Use Active Directory Users and Computers to ensure the CNO and VCO computer objects associated with all clustered names have been removed.

> **NOTE**
> It's a good idea to stop the Cluster service on all servers in the cluster and set the service startup type to Manual so that the Cluster service doesn't start when the servers are restarting while changing domains.

```
Stop-Service -Name ClusSvc

Set-Service -Name ClusSvc -StartupType Manual
```

5. Change the servers' domain membership to a workgroup, restart the servers, join the servers to the new domain, and restart again.

6. Once the servers are in the new domain, sign in to a server with a domain user or administrator account that has Active Directory permissions to create objects, has access to the Cluster, and open PowerShell. Start the Cluster Service, and set it back to Automatic.

```
Start-Service -Name ClusSvc

Set-Service -Name ClusSvc -StartupType Automatic
```

7. Bring the Cluster Name and all other cluster Network Name resources to an Online state.

```
Start-ClusterResource -Name "Cluster Name"

Start-ClusterResource -Name FS-CLUSCLUS
```

8. Change the cluster to be a part of the new domain with associated active directory objects. To do this, the command is below and the network name resources must be in an online state. What this command will do is recreate the name objects in Active Directory.

```
New-ClusterNameAccount -Name CLUSTERNAME -Domain NEWDOMAINNAME.com -UpgradeVCOs
```

NOTE: If you do not have any additional groups with network names (i.e. a Hyper-V Cluster with only virtual machines), the -UpgradeVCOs parameter switch is not needed.

9. Use Active Directory Users and Computers to check the new domain and ensure the associated computer objects were created. If they have, then bring the remaining resources in the groups online.

```
Start-ClusterGroup -Name "Cluster Group"

Start-ClusterGroup -Name FS-CLUSCLUS
```

Known issues

If you are using the new USB witness feature, you will be unable to add the cluster to the new domain. The reasoning is that the file share witness type must utilize Kerberos for authentication. Change the witness to none

before adding the cluster to the domain. Once it is completed, recreate the USB witness. The error you will see is:

```
New-ClusternameAccount : Cluster name account cannot be created.  This cluster contains a file share witness
with invalid permissions for a cluster of type AdministrativeAccesssPoint ActiveDirectoryAndDns. To proceed,
delete the file share witness.  After this you can create the cluster name account and recreate the file
share witness.  The new file share witness will be automatically created with valid permissions.
```

Troubleshooting a Failover Cluster using Windows Error Reporting

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server, Azure Stack HCI, versions 21H2 and 20H2

Windows Error Reporting (WER) is a flexible event-based feedback infrastructure designed to help advanced administrators or Tier 3 support gather information about the hardware and software problems that Windows can detect, report the information to Microsoft, and provide users with any available solutions. This reference provides descriptions and syntax for all WindowsErrorReporting cmdlets.

The information on troubleshooting presented below will be helpful for troubleshooting advanced issues that have been escalated and that may require data to be sent to Microsoft for triaging.

Enabling event channels

When Windows Server is installed, many event channels are enabled by default. But sometimes when diagnosing an issue, we want to be able to enable some of these event channels since it will help in triaging and diagnosing system issues.

You could enable additional event channels on each server node in your cluster as needed; however, this approach presents two problems:

1. You have to remember to enable the same event channels on every new server node that you add to your cluster.
2. When diagnosing, it can be tedious to enable specific event channels, reproduce the error, and repeat this process until you root cause.

To avoid these issues, you can enable event channels on cluster startup. The list of enabled event channels on your cluster can be configured using the public property **EnabledEventLogs**. By default, the following event channels are enabled:

```
PS C:\Windows\system32> (get-cluster).EnabledEventLogs
```

Here's an example of the output:

```
Microsoft-Windows-Hyper-V-VmSwitch-Diagnostic,4,0xFFFFFFFD
Microsoft-Windows-SMBDirect/Debug,4
Microsoft-Windows-SMBServer/Analytic
Microsoft-Windows-Kernel-LiveDump/Analytic
```

The **EnabledEventLogs** property is a multistring, where each string is in the form: **channel-name, log-level, keyword-mask**. The **keyword-mask** can be a hexadecimal (prefix 0x), octal (prefix 0), or decimal number (no prefix) number. For instance, to add a new event channel to the list and to configure both **log-level** and **keyword-mask** you can run:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2,321"
```

If you want to set the **log-level** but keep the **keyword-mask** at its default value, you can use either of the following commands:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2,"
```

If you want to keep the **log-level** at its default value, but set the **keyword-mask** you can run the following command:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,,0xf1"
```

If you want to keep both the **log-level** and the **keyword-mask** at their default values, you can run any of the following commands:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,,"
```

These event channels will be enabled on every cluster node when the cluster service starts or whenever the **EnabledEventLogs** property is changed.

Gathering Logs

After you have enabled event channels, you can use the **DumpLogQuery** to gather logs. The public resource type property **DumpLogQuery** is a mutistring value. Each string is an XPATH query as described here.

When troubleshooting, if you need to collect additional event channels, you can a modify the **DumpLogQuery** property by adding additional queries or modifying the list.

To do this, first test your XPATH query using the get-WinEvent PowerShell cmdlet:

```
get-WinEvent -FilterXML "<QueryList><Query><Select Path='Microsoft-Windows-GroupPolicy/Operational'>*
[System[TimeCreated[timediff(@SystemTime) &gt;= 600000]]]</Select></Query></QueryList>"
```

Next, append your query to the **DumpLogQuery** property of the resource:

```
(Get-ClusterResourceType -Name "Physical Disk".DumpLogQuery += "<QueryList><Query><Select Path='Microsoft-
Windows-GroupPolicy/Operational'>*[System[TimeCreated[timediff(@SystemTime) &gt;= 600000]]]</Select></Query>
</QueryList>"
```

And if you want to get a list of queries to use, run:

```
(Get-ClusterResourceType -Name "Physical Disk").DumpLogQuery
```

Gathering Windows Error Reporting reports

Windows Error Reporting Reports are stored in **%ProgramData%\Microsoft\Windows\WER**

Inside the **WER** folder, the **ReportsQueue** folder contains reports that are waiting to be uploaded to Watson.

```
PS C:\Windows\system32> dir c:\ProgramData\Microsoft\Windows\WER\ReportQueue
```

Here's an example of the output:

```
Volume in drive C is INSTALLTO
Volume Serial Number is 4031-E397

Directory of C:\ProgramData\Microsoft\Windows\WER\ReportQueue

<date>  <time>    <DIR>          .
<date>  <time>    <DIR>          ..
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_02d10a3f
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_0588dd06
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_10d55ef5
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_13258c8c
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_13a8c4ac
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_13dcf4d3
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_1721a0b0
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_1839758a
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_1d4131cb
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_23551d79
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_2468ad4c
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_255d4d61
<date>  <time>    <DIR>          Critical_Physical
Disk_1cbd8ffecbc8a1a0e7819e4262e3ece2909a157a_00000000_cab_08289734
<date>  <time>    <DIR>          Critical_Physical
Disk_64acaf7e4590828ae8a3ac3c8b31da9a789586d4_00000000_cab_1d94712e
<date>  <time>    <DIR>          Critical_Physical
Disk_ae39f5243a104f21ac5b04a39efeac4c126754_00000000_003359cb
<date>  <time>    <DIR>          Critical_Physical
Disk_ae39f5243a104f21ac5b04a39efeac4c126754_00000000_cab_1b293b17
<date>  <time>    <DIR>          Critical_Physical
Disk_b46b8883d892cfa8a26263afca228b17df8133d_00000000_cab_08abc39c
<date>  <time>    <DIR>          Kernel_166_1234dacd2d1a219a3696b6e64a736408fc785cc_00000000_cab_19c8a127
               0 File(s)              0 bytes
              20 Dir(s)  23,291,658,240 bytes free
```

Inside the **WER** folder, the **ReportsArchive** folder contains reports that have already been uploaded to Watson. Data in these reports is deleted, but the **Report.wer** file persists.

```
PS C:\Windows\system32> dir C:\ProgramData\Microsoft\Windows\WER\ReportArchive
```

Here's an example of the output:

```
Volume in drive C is INSTALLTO
Volume Serial Number is 4031-E397

Directory of c:\ProgramData\Microsoft\Windows\WER\ReportArchive

<date>  <time>    <DIR>          .
<date>  <time>    <DIR>          ..
<date>  <time>    <DIR>
Critical_powershell.exe_7dd54f49935ce48b2dd99d1c64df29a5cfb73db_00000000_cab_096cc802
               0 File(s)              0 bytes
               3 Dir(s)  23,291,658,240 bytes free
```

Windows Error Reporting provides many settings to customize the problem reporting experience. For further information, please refer to the Windows Error Reporting documentation.

Troubleshooting using Windows Error Reporting reports

Physical disk failed to come online

To diagnose this issue, navigate to the WER report folder:

```
PS C:\Windows\system32> dir
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_PhysicalDisk_b46b8883d892cfa8a26263afca228b17df8
133d_00000000_cab_08abc39c
```

Here's an example of the output:

```
Volume in drive C is INSTALLTO
Volume Serial Number is 4031-E397

<date>  <time>    <DIR>          .
<date>  <time>    <DIR>          ..
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_1.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_10.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_11.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_12.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_13.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_14.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_15.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_16.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_17.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_18.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_19.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_2.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_20.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_21.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_22.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_23.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_24.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_25.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_26.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_27.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_28.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_29.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_3.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_30.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_31.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_32.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_33.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_34.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_35.evtx
<date>  <time>         2,166,784 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_36.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_37.evtx
<date>  <time>            33,194 Report.wer
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_38.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_39.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_4.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_40.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_41.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_5.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_6.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_7.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_8.evtx
<date>  <time>            69,632 CLUSWER_RHS_ERROR_8d06c544-47a4-4396-96ec-af644f45c70a_9.evtx
<date>  <time>             7,382 WERC263.tmp.WERInternalMetadata.xml
<date>  <time>            59,202 WERC36D.tmp.csv
<date>  <time>            13,340 WERC38D.tmp.txt
```

Next, start triaging from the **Report.wer** file — this will tell you what failed.

```
EventType=Failover_clustering_resource_error
<skip>
Sig[0].Name=ResourceType
Sig[0].Value=Physical Disk
Sig[1].Name=CallType
Sig[1].Value=ONLINERESOURCE
Sig[2].Name=RHSCallResult
Sig[2].Value=5018
Sig[3].Name=ApplicationCallResult
Sig[3].Value=999
Sig[4].Name=DumpPolicy
Sig[4].Value=5225058577
DynamicSig[1].Name=OS Version
DynamicSig[1].Value=10.0.17051.2.0.0.400.8
DynamicSig[2].Name=Locale ID
DynamicSig[2].Value=1033
DynamicSig[27].Name=ResourceName
DynamicSig[27].Value=Cluster Disk 10
DynamicSig[28].Name=ReportId
DynamicSig[28].Value=8d06c544-47a4-4396-96ec-af644f45c70a
DynamicSig[29].Name=FailureTime
DynamicSig[29].Value=2017//12//12-22:38:05.485
```

Since the resource failed to come online, no dumps were collected, but the Windows Error Reporting report did collect logs. If you open all **.evtx** files using Microsoft Message Analyzer, you will see all of the information that was collected using the following queries through the system channel, application channel, failover cluster diagnostic channels, and a few other generic channels.

```
PS C:\Windows\system32> (Get-ClusterResourceType -Name "Physical Disk").DumpLogQuery
```

Here's an example of the output:

```
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Kernel-PnP/Configuration">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-ReFS/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Ntfs/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Ntfs/WHC">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Storport/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Storport/Health">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Storport/Admin">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-ClassPnP/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-ClassPnP/Admin">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-ScmBus/Certification">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 86400000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-ScmBus/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-PmemDisk/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-NvdimmN/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-INvdimm/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-PersistentMemory-VirtualNvdimm/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Disk/Admin">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Disk/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-ScmDisk0101/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Partition/Diagnostic">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Volume/Diagnostic">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-VolumeSnapshot-Driver/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-FailoverClustering-Clusport/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-StorageSpaces-Driver/Diagnostic">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-StorageManagement/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 86400000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-StorageSpaces-Driver/Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Storage-Tiering/Admin">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Hyper-V-VmSwitch-Operational">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
<QueryList><Query Id="0"><Select Path="Microsoft-Windows-Hyper-V-VmSwitch-Diagnostic">*
[System[TimeCreated[timediff(@SystemTime) &lt;= 600000]]]</Select></Query></QueryList>
```

Message Analyzer enables you to capture, display, and analyze protocol messaging traffic. It also lets you trace and assess system events and other messages from Windows components. You can download Microsoft Message Analyzer from here. When you load the logs into Message Analyzer, you will see the following providers and messages from the log channels.

MessageNu	ProcessId	Threac	Leve	ActivityId	LevelDisplayNa	Timestamp
Channel (258): Application						
Channel (2979): Microsoft-Windows-FailoverClustering/Diagnostic						
Channel (1329): Microsoft-Windows-FailoverClustering/DiagnosticVerbose						
Channel (370): Microsoft-Windows-FailoverClustering/Operational						
Channel (20): Microsoft-Windows-FailoverClustering-CsvFs/Operational						
Channel (108): Microsoft-Windows-FailoverClustering-NetFt/Operational						
Channel (25): Microsoft-Windows-Kernel-LiveDump/Analytic						
Channel (6): Microsoft-Windows-Kernel-PnP/Configuration						
Channel (4): Microsoft-Windows-Ntfs/Operational						
Channel (8): Microsoft-Windows-Storage-ClassPnP/Operational						
Channel (4): Microsoft-Windows-StorageManagement/Operational						
Channel (12): Microsoft-Windows-Storage-Storport/Operational						
Channel (9): Microsoft-Windows-VolumeSnapshot-Driver/Operational						
Channel (832): System						

You can also group by providers to get the following view:

```
ProviderName (1):
ProviderName (2): BROWSER
ProviderName (3): Desktop Window Manager
ProviderName (3): DFSR
ProviderName (44): ESENT
ProviderName (9): EventLog
ProviderName (11): iScsiPrt
ProviderName (2): LsaSrv
ProviderName (4): Microsoft-Windows-DfsSvc
ProviderName (12): Microsoft-Windows-Dhcp-Client
ProviderName (10): Microsoft-Windows-DHCPv6-Client
ProviderName (2): Microsoft-Windows-Directory-Services-SAM
ProviderName (14): Microsoft-Windows-DNS-Client
ProviderName (1): Microsoft-Windows-Eventlog
ProviderName (2): Microsoft-Windows-EventSystem
ProviderName (4685): Microsoft-Windows-FailoverClustering
ProviderName (20): Microsoft-Windows-FailoverClustering-CsvFs-Diagnostic
ProviderName (108): Microsoft-Windows-FailoverClustering-NetFt
ProviderName (32): Microsoft-Windows-FilterManager
ProviderName (36): Microsoft-Windows-Hyper-V-Netvsc
ProviderName (12): Microsoft-Windows-Kernel-Boot
ProviderName (148): Microsoft-Windows-Kernel-General
ProviderName (24): Microsoft-Windows-Kernel-LiveDump
ProviderName (6): Microsoft-Windows-Kernel-PnP
ProviderName (4): Microsoft-Windows-Kernel-Power
ProviderName (4): Microsoft-Windows-Kernel-Processor-Power
ProviderName (1): Microsoft-Windows-LoadPerf
ProviderName (4): Microsoft-Windows-MSDTC
ProviderName (2): Microsoft-Windows-MSDTC 2
ProviderName (4): Microsoft-Windows-MSMQ
ProviderName (29): Microsoft-Windows-Ntfs
ProviderName (3): Microsoft-Windows-Perflib
ProviderName (40): Microsoft-Windows-Security-SPP
ProviderName (4): Microsoft-Windows-StorageManagement-WSP-Spaces
ProviderName (8): Microsoft-Windows-StorDiag
ProviderName (12): Microsoft-Windows-StorPort
ProviderName (12): Microsoft-Windows-Time-Service
ProviderName (7): Microsoft-Windows-User Profiles Service
ProviderName (9): Microsoft-Windows-VolumeSnapshot-Driver
ProviderName (9): Microsoft-Windows-WindowsUpdateClient
ProviderName (2): Microsoft-Windows-Wininit
ProviderName (4): Microsoft-Windows-Winlogon
ProviderName (3): Microsoft-Windows-WinRM
ProviderName (4): Microsoft-Windows-WMI
ProviderName (2): MSiSCSI
ProviderName (2): MSiSNS
ProviderName (1): NETLOGON
ProviderName (1): SceCli
ProviderName (441): Service Control Manager
ProviderName (104): SideBySide
ProviderName (2): User32
ProviderName (8): VSS
ProviderName (2): Windows Error Reporting
ProviderName (19): Wins
ProviderName (26): WTT
```

To identify why the disk failed, navigate to the events under **FailoverClustering/Diagnostic** and **FailoverClustering/DiagnosticVerbose**. Then run the following query: **EventLog.EventData["LogString"] contains "Cluster Disk 10"**. This will give you give you the following output:

Physical disk timed out

To diagnose this issue, navigate to the WER report folder. The folder contains log files and dump files for **RHS**, **clussvc.exe**, and of the process that hosts the "**smphost**" service, as shown below:

```
PS C:\Windows\system32> dir
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_PhysicalDisk_64acaf7e4590828ae8a3ac3c8b31da9a789
586d4_00000000_cab_1d94712e
```

Here's an example of the output:

```
Volume in drive C is INSTALLTO
Volume Serial Number is 4031-E397

<date>  <time>    <DIR>          .
<date>  <time>    <DIR>          ..
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_1.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_10.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_11.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_12.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_13.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_14.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_15.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_16.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_17.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_18.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_19.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_2.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_20.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_21.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_22.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_23.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_24.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_25.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_26.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_27.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_28.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_29.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_3.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_30.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_31.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_32.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_33.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_34.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_35.evtx
<date>  <time>         2,166,784 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_36.evtx
<date>  <time>         1,118,208 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_37.evtx
<date>  <time>        28,340,500 memory.hdmp
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_38.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_39.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_4.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_40.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_41.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_5.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_6.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_7.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_8.evtx
<date>  <time>            69,632 CLUSWER_RHS_HANG_75e60318-50c9-41e4-94d9-fb0f589cd224_9.evtx
<date>  <time>         4,466,943 minidump.0f14.mdmp
<date>  <time>         1,735,776 minidump.2200.mdmp
<date>  <time>            33,890 Report.wer
<date>  <time>            49,267 WER69FA.tmp.mdmp
<date>  <time>             5,706 WER70A2.tmp.WERInternalMetadata.xml
<date>  <time>            63,206 WER70E0.tmp.csv
<date>  <time>            13,340 WER7100.tmp.txt
```

Next, start triaging from the **Report.wer** file — this will tell you what call or resource is hanging.

```
EventType=Failover_clustering_resource_timeout_2
<skip>
Sig[0].Name=ResourceType
Sig[0].Value=Physical Disk
Sig[1].Name=CallType
Sig[1].Value=ONLINERESOURCE
Sig[2].Name=DumpPolicy
Sig[2].Value=5225058577
Sig[3].Name=ControlCode
Sig[3].Value=18
DynamicSig[1].Name=OS Version
DynamicSig[1].Value=10.0.17051.2.0.0.400.8
DynamicSig[2].Name=Locale ID
DynamicSig[2].Value=1033
DynamicSig[26].Name=ResourceName
DynamicSig[26].Value=Cluster Disk 10
DynamicSig[27].Name=ReportId
DynamicSig[27].Value=75e60318-50c9-41e4-94d9-fb0f589cd224
DynamicSig[29].Name=HangThreadId
DynamicSig[29].Value=10008
```

The list of services and processes that we collect in a dump is controlled by the following property: **PS C:\Windows\system32> (Get-ClusterResourceType -Name "Physical Disk").DumpServicesSmphost**

To identify why the hang happened, open the dump files. Then run the following query: **EventLog.EventData["LogString"] contains "Cluster Disk 10"** This will give you give you the following output:

Remove Apply Library History EventLog.EventData["LogString"] contains "Cluster Disk 10"

Right click on any column header and select 'Group' to create a grouping.

MessageNu	ProcessId	Threac	Lev	ActivityId	LevelDisplayNa	Timestamp	Ma	Chan	Provider	EventI	Vers	Opc	Su	Ev	EventData["LogString"]
1820	3860	5584	4	nothing	Informatio…	2017-12-12T22:41:57.7579775	E…	Mic…	Micro…	2049	0	In…	U…	m…	[RCM] Res Cluster Disk 10: OnlineCallIssued -> OnlinePending(StateUnknown)
177	3860	5584	4	nothing	Informatio…	2017-12-12T22:41:57.7580195	E…	Mic…	Micro…	5399	0	In…	U…	m…	[RCM] TransitionToState(Cluster Disk 10) OnlineCallIssued-->OnlinePending.
1821	3860	5584	4	nothing	Informatio…	2017-12-12T22:41:57.7580206	E…	Mic…	Micro…	2049	0	In…	U…	m…	[RCM] TransitionToState(Cluster Disk 10) OnlineCallIssued-->OnlinePending.
182	3860	4476	5	nothing	Verbose	2017-12-12T22:41:57.7746874	E…	Mic…	Micro…	5408	0	In…	U…	m…	[RCM] rcm::RcmResource::Control: (Cluster Disk 10, GET_ID)
1826	3860	4476	5	nothing	Verbose	2017-12-12T22:41:57.7746887	E…	Mic…	Micro…	2052	0	In…	U…	m…	[RCM] rcm::RcmResource::Control: (Cluster Disk 10, GET_ID)
239	7576	10008	2	75e60318…	Error	2017-12-12T22:42:06.0653880	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 1.
1883	7576	10008	2	75e60318…	Error	2017-12-12T22:42:06.0653900	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 1.
297	7576	10008	2	75e60318…	Error	2017-12-12T22:42:13.0160722	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 2.
1941	7576	10008	2	75e60318…	Error	2017-12-12T22:42:13.0160749	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 2.
335	7576	10008	2	75e60318…	Error	2017-12-12T22:42:23.0169812	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 3.
1979	7576	10008	2	75e60318…	Error	2017-12-12T22:42:23.0169839	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 3.
416	7576	10008	2	75e60318…	Error	2017-12-12T22:42:33.1598682	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 4.
2060	7576	10008	2	75e60318…	Error	2017-12-12T22:42:33.1598709	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 4.
466	7576	10008	2	75e60318…	Error	2017-12-12T22:42:43.4320410	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 5.
2110	7576	10008	2	75e60318…	Error	2017-12-12T22:42:43.4320437	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 5.
523	7576	10008	2	75e60318…	Error	2017-12-12T22:42:53.4365993	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 6.
2167	7576	10008	2	75e60318…	Error	2017-12-12T22:42:53.4366018	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 6.
635	7576	10008	2	75e60318…	Error	2017-12-12T22:43:03.4352304	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 7.
2285	7576	10008	2	75e60318…	Error	2017-12-12T22:43:03.4352328	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 7.
685	7576	10008	2	75e60318…	Error	2017-12-12T22:43:13.4357504	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 8.
2335	7576	10008	2	75e60318…	Error	2017-12-12T22:43:13.4357531	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 8.
729	7576	10008	2	75e60318…	Error	2017-12-12T22:43:23.4437011	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 9.
2379	7576	10008	2	75e60318…	Error	2017-12-12T22:43:23.4437037	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 9.
785	7576	10008	2	75e60318…	Error	2017-12-12T22:43:33.4421265	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 10.
2435	7576	10008	2	75e60318…	Error	2017-12-12T22:43:33.4421290	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 10.
824	7576	10008	2	75e60318…	Error	2017-12-12T22:43:43.4412809	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 11.
2474	7576	10008	2	75e60318…	Error	2017-12-12T22:43:43.4412837	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 11.
881	7576	10008	2	75e60318…	Error	2017-12-12T22:43:53.4410888	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 12.
2531	7576	10008	2	75e60318…	Error	2017-12-12T22:43:53.4410911	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 12.
928	7576	10008	2	75e60318…	Error	2017-12-12T22:44:03.4439773	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 13.
2578	7576	10008	2	75e60318…	Error	2017-12-12T22:44:03.4439798	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 13.
972	7576	10008	2	75e60318…	Error	2017-12-12T22:44:13.4446826	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 14.
2622	7576	10008	2	75e60318…	Error	2017-12-12T22:44:13.4446852	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 14.
1022	7576	10008	2	75e60318…	Error	2017-12-12T22:44:23.4461055	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 15.
2672	7576	10008	2	75e60318…	Error	2017-12-12T22:44:23.4461079	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 15.
1083	7576	10008	2	75e60318…	Error	2017-12-12T22:44:33.4469668	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 16.
2733	7576	10008	2	75e60318…	Error	2017-12-12T22:44:33.4469695	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 16.
1122	7576	10008	2	75e60318…	Error	2017-12-12T22:44:43.4474174	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 17.
2772	7576	10008	2	75e60318…	Error	2017-12-12T22:44:43.4474201	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 17.
1174	7576	10008	2	75e60318…	Error	2017-12-12T22:44:53.4478159	E…	Mic…	Micro…	5401	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 18.
2824	7576	10008	2	75e60318…	Error	2017-12-12T22:44:53.4478178	E…	Mic…	Micro…	2051	0	In…	U…	m…	[RES] Physical Disk <Cluster Disk 10>: OnlineThread: Simulating hang. Sleeping for 10 seconds. Iteration 18.
1176	7576	7644	3	5b123ed7…	Warning	2017-12-12T22:44:54.1274438	E…	Mic…	Micro…	5400	0	In…	U…	m…	[RHS - Timeout] Resource 'Cluster Disk 10' has not responded to the call ONLINERESOURCE:18. The timeout to respo…
2826	7576	7644	3	5b123ed7…	Warning	2017-12-12T22:44:54.1274454	E…	Mic…	Micro…	2050	0	In…	U…	m…	[RHS - Timeout] Resource 'Cluster Disk 10' has not responded to the call ONLINERESOURCE:18. The timeout to respo…
1186	7576	7644	3	5b123ed7…	Warning	2017-12-12T22:46:14.3576085	E…	Mic…	Micro…	5400	0	In…	U…	m…	[RHS-Timeout] Health Monitoring Failure: Resource Cluster Disk 10 is not functioning as expected. Cancelling cur…
2836	7576	7644	3	5b123ed7…	Warning	2017-12-12T22:46:14.3576103	E…	Mic…	Micro…	2050	0	In…	U…	m…	[RHS-Timeout] Health Monitoring Failure: Resource Cluster Disk 10 is not functioning as expected. Cancelling cur…
1187	7576	7644	5	5b123ed7…	Verbose	2017-12-12T22:46:14.3576415	E…	Mic…	Micro…	5408	0	In…	U…	m…	[RHS] SetOnlineOrOfflineCall: Stopping pending state timer for Resource Cluster Disk 10 CurrentState: OnlinePend…
2837	7576	7644	5	5b123ed7…	Verbose	2017-12-12T22:46:14.3576427	E…	Mic…	Micro…	2052	0	In…	U…	m…	[RHS] SetOnlineOrOfflineCall: Stopping pending state timer for Resource Cluster Disk 10 CurrentState: OnlinePend…
1188	7576	7644	5	5b123ed7…	Verbose	2017-12-12T22:46:14.3576913	E…	Mic…	Micro…	5408	0	In…	U…	m…	[RHS] OnlineResCall::OnDeadlock(Cluster Disk 10)
2838	7576	7644	5	5b123ed7…	Verbose	2017-12-12T22:46:14.3576924	E…	Mic…	Micro…	2052	0	In…	U…	m…	[RHS] OnlineResCall::OnDeadlock(Cluster Disk 10)
1190	3860	6224	3	nothing	Warning	2017-12-12T22:46:14.3591303	E…	Mic…	Micro…	5400	0	In…	U…	m…	[RCM] HandleMonitorReply: FAILURENOTIFICATION for 'Cluster Disk 10', gen(2) result 5018/0.
2840	3860	6224	3	nothing	Warning	2017-12-12T22:46:14.3591321	E…	Mic…	Micro…	2050	0	In…	U…	m…	[RCM] HandleMonitorReply: FAILURENOTIFICATION for 'Cluster Disk 10', gen(2) result 5018/0.

We can cross-examine this with the thread from the **memory.hdmp** file:

```
# 21  Id: 1d98.2718 Suspend: 0 Teb: 0000000b`f1f7b000 Unfrozen
# Child-SP          RetAddr           Call Site
00 0000000b`f3c7ec38 00007ff8`455d25ca ntdll!ZwDelayExecution+0x14
01 0000000b`f3c7ec40 00007ff8`2ef19710 KERNELBASE!SleepEx+0x9a
02 0000000b`f3c7ece0 00007ff8`3bdf7fbf clusres!ResHardDiskOnlineOrTurnOffMMThread+0x2b0
03 0000000b`f3c7f960 00007ff8`391eed34 resutils!ClusWorkerStart+0x5f
04 0000000b`f3c7f9d0 00000000`00000000 vfbasics+0xed34
```

Troubleshooting cluster issue with Event ID 1135

12/9/2022 • 12 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

Try our Virtual Agent - It can help you quickly identify and fix common Active Directory replication issues.

This article helps you diagnose and resolve Event ID 1135, which may be logged during the startup of the Cluster service in Failover Clustering environment.

Start Page

Event ID 1135 indicates that one or more Cluster nodes were removed from the active failover cluster membership. It may be accompanied by the following symptoms:

- Cluster Failover\nodes being removed from active Failover Cluster membership: Having a problem with nodes being removed from active Failover Cluster membership
- Event ID 1069 Event ID 1069 — Clustered Service or Application Availability
- Event ID 1177 for Quorum loss Event ID 1177 — Quorum and Connectivity Needed for Quorum
- Event ID 1006 for Cluster service halted: Event ID 1006 — Cluster Service Startup

A validation and the network tests would be recommended as one of the initial troubleshooting steps to ensure there are no configuration issues that might be a cause for problems.

Check if installed the recommended hot fixes

The Cluster service is the essential software component that controls all aspects of failover cluster operation and manages the cluster configuration database. If you see the event ID 1135, Microsoft recommends you to install the fixes mentioned in the below KB articles and reboot all the nodes of the cluster, then observe if issue reoccurs.

- Hotfix for Windows Server 2012 R2
- Hotfix for Windows Server 2012
- Hotfix for Windows Server 2008 R2

Check if the cluster service running on all the nodes

Follow the following command according to your Windows operation system to validate that cluster service is continuously running and available.

For Windows Server 2008 R2 cluster

From an elevated cmd prompt, run: `cluster.exe node /stat`

For Windows Server 2012 and Windows Server 2012 R2 cluster

Run the following PowerShell command: `Get-ClusterResource`

Is the cluster service continuously running and available on all the nodes?

Several scenarios of Event ID 1135

We want you to take a closer look on at the System Event logs on all the nodes of your cluster. Review the Event ID 1135 that you are seeing on the nodes and copy all the instances of this event. This will make it convenient for you to look at them and review.

```
Event ID 1135
Cluster node ' **NODE A** ' was removed from the active failover cluster membership. The Cluster service on
this node may have stopped.
This could also be due to the node having lost communication with other active nodes in the failover
cluster.
Run the Validate a Configuration wizard to check your network configuration.
If the condition persists, check for hardware or software errors related to the network adapters on this
node.
Also check for failures in any other network components to which the node is connected such as hubs,
switches, or bridges.
```

There are three typical scenarios:

Scenario A

You are looking at all the Events and all the nodes in the cluster are indicating that NODE A had lost communication.

It could be possible that when you are seeing the system logs on NODE A, it has events for all the remaining nodes in the cluster.

Solution

This quite suggests that at the time of issue, either due to network congestion or otherwise the communication to the NODE A was lost.

You should review and validate the Network configuration and communication issues. Remember to look for issues pertaining to Node A.

Scenario B

You are looking at the Events on the nodes and let us say that your cluster is dispersed across two sites. NODE A, NODE B, and NODE C at Site 1 and NODE D & NODE E at Site 2.

On Nodes A,B, and C, you see that the events that are logged are for connectivity to Nodes D & E. Similarly, when you see the events on Nodes D & E, the events suggest that we lost communication with A, B, and C.

Solution

If you see similar activity, it is indicative that there was a communication failure, over the link that connects these sites. We would recommend that you review the connection across the sites, if this is over a WAN connection, we would suggest that you verify with your ISP about the connectivity.

Scenario C

You are looking at the Events on the nodes and you see that the names of the nodes do not tally out with any particular pattern. Let us say that your cluster is dispersed across two sites. NODE A, NODE B and NODE C at Site 1 and NODE D & NODE E at Site 2.

- On Node A: You see events for Nodes B, D, E.
- On Node B: You see events for Nodes C, D, E.
- On Node C: You see events for Nodes A, B, E.
- On Node D: You see events for Nodes A, C, E.
- On Node E: You see events for Nodes B, C, D.
- Or any other combinations.

Solution

Such events are possible when the network channels between the nodes are choked and the cluster communication messages are not reaching in a timely manner, making the cluster to feel that the communication between the nodes is lost resulting in the removal of nodes from the cluster membership.

Review Cluster Networks

We would recommend that you review your Cluster Networks by checking the following three options one by one to continue this troubleshooting guide.

Check for Antivirus Exclusion

Exclude the following file system locations from virus scanning on a server that is running Cluster Services:

- The path of the FileShare Witness
- The *%Systemroot%\Cluster* folder

Configure the real-time scanning component within your antivirus software to exclude the following directories and files:

- Default virtual machine configuration directory (C:\ProgramData\Microsoft\Windows\Hyper-V)
- Custom virtual machine configuration directories
- Default virtual hard disk drive directory (C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks)
- Custom virtual hard disk drive directories
- Custom replication data directories, if you are using Hyper-V Replica
- Snapshot directories
- mms.exe

  > **NOTE**
  > This file may have to be configured as a process exclusion within the antivirus software.

- Vmwp.exe

  > **NOTE**
  > This file may have to be configured as a process exclusion within the antivirus software.

Additionally, when you use Live Migration together with Cluster Shared Volumes, exclude the CSV path *C:\Clusterstorage* and all its subdirectories. If you are troubleshooting failover issues or general problems with Cluster services and antivirus software is installed, temporarily uninstall the antivirus software or check with the manufacturer of the software to determine whether the antivirus software works with Cluster services. Just disabling the antivirus software is insufficient in most cases. Even if you disable the antivirus software, the filter driver is still loaded when you restart the computer.

Check for Network Port Configuration in Firewall

The Cluster service controls server cluster operations and manages the cluster database. A cluster is a collection of independent computers that act as a single computer. Managers, programmers, and users see the cluster as a single system. The software distributes data among the nodes of the cluster. If a node fails, other nodes provide the services and data that were formerly provided by the missing node. When a node is added or repaired, the cluster software migrates some data to that node.

System service name: **ClusSvc**

APPLICATION	PROTOCOL	PORTS
Cluster Service	UDP	3343
Cluster Service	TCP	3343 (This port is required during a node join operation.)
RPC	TCP	135

APPLICATION	PROTOCOL	PORTS
Cluster Admin	UDP	137
Kerberos	UDP/TCP	464*
SMB	TCP	445
Randomly allocated high UDP ports**	UDP	Random port number between 1024 and 65535 Random port number between 49152 and 65535***

> **NOTE**
> Additionally, for successful validation on Windows Failover Clusters on Windows Server 2008 and above, allow inbound and outbound traffic for ICMP4, ICMP6.

- For more information, see Creating a Windows Server 2012 Failover Cluster Fails with Error 0xc000005e.
- For more information about how to customize these ports, see Service overview and network port requirements for Windows in the "References" section.

This is the range in Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows Server 2008, and Windows Vista.

Besides, run the following command to check for Network Port Configuration in Firewall. For example: This command helps determine port 3343 available\open used for Failover Cluster:

```
netsh advfirewall firewall show rule name="Failover Clusters (UDP-In)" verbose
```

Run the Cluster Validation report for any errors or warnings

The cluster validation tool runs a suite of tests to verify that your hardware and settings are compatible with failover clustering.

Follow these instructions:

1. Run the Cluster Validation report for any errors or warnings. For more information, see Understanding Cluster Validation Tests: Network

2. Verify for warnings and errors for Networks. For more information, see Understanding Cluster Validation Tests: Network.

Check the List Network Binding Order

This test lists the order in which networks are bound to the adapters on each node.

The Adapters and Bindings tab lists the connections in the order in which the connections are accessed by network services. The order of these connections reflects the order in which generic TCP/IP calls/packets are sent on to the wire.

Follow the below steps to change the binding order of network adapters:

1. Click **Start**, click **Run**, type `ncpa.cpl`, and then click **OK**. You can see the available connections in the **LAN and High-Speed Internet** section of the **Network Connections** window.

2. On the **Advanced** menu, click **Advanced Settings**, and then click the **Adapters and Bindings** tab.
3. In the **Connections** area, select the connection that you want to move higher in the list. Use the arrow buttons to move the connection. As a general rule, the card that talks to the network (domain connectivity, routing to other networks, etc. should be the first bound (top of the list) card.

Cluster nodes are multi-homed systems. Network priority affects DNS Client for outbound network connectivity. Network adapters used for client communication should be at the top in the binding order. Non-routed networks can be placed at lower priority. In Windows Server 2012 and Windows Server2012 R2, the Cluster Network Driver (NETFT.SYS) adapter is automatically placed at the bottom in the binding order list.

Check the Validate Network Communication

Latency on your network could also cause this to happen. The packets may not be lost between the nodes, but they may not get to the nodes fast enough before the timeout period expires.

This test validates that tested servers can communicate with acceptable latency on all networks.

For example: Under Validate Network Communication, you may see the following messages for network latency issues:

```
Succeeded in pinging network interface node003.contoso.com IP Address 192.168.0.2 from network interface
node004.contoso.com IP Address 192.168.0.3 with maximum delay 500 after 1 attempt(s).
Either address 10.0.0.96 is not reachable from 192.168.0.2 or **the ping latency is greater than the maximum
allowed 2000 ms**
This may be expected, since network interfaces node003.contoso.com - Heartbeat Network and
node004.contoso.com - Production Network are on different cluster networks
Either address 192.168.0.2 is not reachable from 10.0.0.96 or **the ping latency is greater than the maximum
allowed 2000 ms**
This may be expected, since network interfaces node004.contoso.com - Production Network and
node003.contoso.com - Heartbeat Network for MSCS are on different cluster networks
```

For multi-site cluster, you may increase the time-out values. For more information, see Configure Heartbeat and DNS Settings in a Multi-Site Failover Cluster.

Check with ISP for any WAN connectivity issues.

Check if you encounter any of the following issues.

Network packets lost between nodes

1. Check Packet loss using Performance

   If the packet is lost on the wire somewhere between the nodes, then the heartbeats will fail. We can easily find out if this is a problem by using Performance Monitor to look at the "Network Interface\Packets Received Discarded" counter. Once you have added this counter, look at the Average, Minimum, and Maximum numbers and if they are any value higher than zero, then the receive buffer needs to be adjusted up for the adapter.

If you are experiencing network packet lost on VMware virtualization platform, see the "Cluster installed in the VMware virtualization platform" section.

2. Upgrade the NIC drivers

   This issue can occurs due to outdated NIC drivers\Integration Components (IC)\VmTools or faulty NIC adapters. If there are network packets lost between nodes on Physical machines, please have your network adapter driver updates. Old or out-of-date network card drivers and/or firmware. At times, a simple misconfiguration of the network card or switch can also cause loss of heartbeats.

Cluster installed in the VMware virtualization platform

Verify VMware adapter issues in case of VMware environment.

This issue may occur if the packets are dropped during high traffic bursts. Ensure that there is no traffic filtering occurring (for example, with a mail filter). After eliminating this possibility, gradually increase the number of buffers in the guest operating system and verify.

To reduce burst traffic drops, follow these steps:

1. Open Run box by using Windows Key + R.
2. Type `devmgmt.msc` and press **Enter**.
3. Expand **Network adapters**
4. Right-click **vmxnet3 and click Properties.**
5. Click the **Advanced** tab.
6. Click **Small Rx Buffers** and increase the value. The default value is 512 and the maximum is 8192.
7. Click **Rx Ring #1** Size and increase the value. The default value is 1024 and the maximum is 4096.

Check the following URLs to verify VMware adapter issues in case of VMware environment:

- Nodes being removed from Failover Cluster membership on VMware ESX?.
- Large packet loss at the guest operating system level on the VMXNET3 vNIC in ESXi

Notice any Network congestion

Network congestion can also cause network connectivity issues.

Verify your network is configured as per MS and vendor recommendations, see Configuring Windows Failover

Cluster Networks.

Check the network configuration

If it still does not work, please check if you have seen partitioned network in cluster GUI or you have NIC teaming enabled on the heartbeat NIC.

If you see partitioned network in cluster GUI, see "Partitioned" Cluster Networks to troubleshoot the issue.

If you have NIC teaming enabled on the heartbeat NIC, check Teaming software functionality as per teaming vendor's recommendation.

Upgrade the NIC drivers

This issue can occurs due to outdated NIC drivers or faulty NIC adapters.

If there are network packets lost between nodes on Physical machines, have your network adapter driver updates. Old or out-of-date network card drivers and/or firmware.

At times, a simple misconfiguration of the network card or switch can also cause loss of heartbeats.

Check the network configuration

If it still does not work, check whether you have seen partitioned network in cluster GUI or you have NIC teaming enabled on the heartbeat NIC.

Having a problem with nodes being removed from active Failover Cluster membership

12/9/2022 • 5 minutes to read • Edit Online

This article introduces how to resolve the problems in which nodes are removed from active failover cluster membership randomly.

Symptoms

When the issue occurs, you are seeing events like this logged in your System Event Log:

This event will be logged on all nodes in the Cluster except for the node that was removed. The reason for this event is because one of the nodes in the Cluster marked that node as down. It then notifies all of the other nodes of the event. When the nodes are notified, they discontinue and tear down their heartbeat connections to the downed node.

What caused the node to be marked down

All nodes in a Windows 2008 or 2008 R2 Failover Cluster talk to each other over the networks that are set to Allow cluster network communication on this network. The nodes will send out heartbeat packets across these networks to all of the other nodes. These packets are supposed to be received by the other nodes and then a response is sent back. Each node in the Cluster has its own heartbeats that it is going to monitor to ensure the network is up and the other nodes are up. The example below should help clarify this:

If any one of these packets is not returned, then the specific heartbeat is considered failed. For example, W2K8-R2-NODE2 sends a request and receives a response from W2K8-R2-NODE1 to a heartbeat packet so it determines the network and the node is up. If W2K8-R2-NODE1 sends a request to W2K8-R2-NODE2 and W2K8-R2-NODE1 does not get the response, it is considered a lost heartbeat and W2K8-R2-NODE1 keeps track of it. This missed response can have W2K8-R2-NODE1 show the network as down until another heartbeat request is received.

By default, Cluster nodes have a limit of five failures in 5 seconds before the connection is marked down. So if W2K8-R2-NODE1 does not receive the response five times in the time period, it considers that particular route to W2K8-R2-NODE2 to be down. If other routes are still considered to be up, W2K8-R2-NODE2 will remain as an active member.

If all routes are marked down for W2K8-R2-NODE2, it is removed from active Failover Cluster membership and the Event 1135 that you see in the first section is logged. On W2K8-R2-NODE2, the Cluster Service is terminated and then restarted so it can try to rejoin the Cluster.

For more information on how we handle specific routes going down with three or more nodes, see "Partitioned" Cluster Networks blog that was written by Jeff Hughes.

Now that we know how the heartbeat process works, what are some of the known causes for the process to fail

1. Actual network hardware failures. If the packet is lost on the wire somewhere between the nodes, then the heartbeats will fail. A network trace from both nodes involved will reveal this.

2. The profile for your network connections could possibly be bouncing from Domain to Public and back to Domain again. During the transition of these changes, network I/O can be blocked. You can check to see if this is the case by looking at the Network Profile Operational log. You can find this log by opening the Event Viewer and navigating to: Applications and Services Logs\Microsoft\Windows\NetworkProfile\Operational. Look at the events in this log on the node that was mentioned in the Event ID: 1135 and see if the profile was changing at this time. If so, check out the KB article The network location profile changes from "Domain" to "Public" in Windows 7 or in Windows Server 2008 R2.

3. You have IPv6 enabled on the servers, but have the following two rules disabled for Inbound and Outbound in the Windows Firewall:

   - Core Networking - Neighbor Discovery Advertisement
   - Core Networking - Neighbor Discovery Solicitation

4. Anti-virus software could be interfering with this process also. If you suspect this, test by disabling or uninstalling the software. Do this at your own risk because you will be unprotected from viruses at this point.

5. Latency on your network could also cause this to happen. The packets may not be lost between the nodes, but they may not get to the nodes fast enough before the timeout period expires.

6. IPv6 is the default protocol that Failover Clustering will use for its heartbeats. The heartbeat itself is a UDP unicast network packet that communicates over Port 3343. If there are switches, firewalls, or routers not configured properly to allow this traffic through, you can experience issues like this.

7. IPsec security policy refreshes can also cause this problem. The specific issue is that during an IPSec group policy update all IPsec Security Associations (SAs) are torn down by Windows Firewall with Advanced Security (WFAS). While this is happening, all network connectivity is blocked. When renegotiating the Security Associations if there are delays in performing authentication with Active Directory, these delays (where all network communication is blocked) will also block cluster heartbeats

from getting through and cause cluster health monitoring to detect nodes as down if they do not respond within the 5-second threshold.

8. Old or out-of-date network card drivers and/or firmware. At times, a simple misconfiguration of the network card or switch can also cause loss of heartbeats.

9. Modern network cards and virtual network cards may be experiencing packet loss. This can be tracked by opening Performance Monitor and adding the counter "Network Interface\Packets Received Discarded". This counter is cumulative and only increases until the server is rebooted. Seeing a large number of packets dropped here could be a sign that the receive buffers on the network card are set too low or that the server is performing slowly and cannot handle the inbound traffic. Each network card manufacturer chooses whether to expose these settings in the properties of the network card, therefore you need to refer to the manufacturer's website to learn how to increase these values and the recommended values should be used. If you are running on VMware, the following blog talks about this in a little more detail including how to tell if this is the issue as well as points you to the VMWare article on the settings to change.

   Nodes being removed from Failover Cluster membership on VMWare ESX

These are the most common reasons that these events are logged, but there could be other reasons also. The point of this blog was to give you some insight into the process and also give ideas of what to look for. Some will raise the following values to their maximum values to try to get this problem to stop.

PARAMETER	DEFAULT	RANGE
SameSubnetDelay	1000 milliseconds	250-2000 milliseconds
CrossSubnetDelay	1000 milliseconds	250-4000 milliseconds
SameSubnetThreshold	5	3-10
CrossSubnetThreshold	5	3-10

Increasing these values to their maximum may make the event and node removal go away, it just masks the problem. It doesn't fix anything. The best thing to do is found out the root cause of the heartbeat failures and get it fixed. The only real need for increasing these values is in a multi-site scenario where nodes reside in different locations and network latency cannot be overcome.

Nodes being removed from Failover Cluster membership on VMWare ESX

12/9/2022 • 2 minutes to read • Edit Online

This article addresses the issue of finding nodes removed from active failover cluster membership when the nodes are hosted on VMWare ESX.

Symptom

When the issue occurs, you will see in the System Event Log of the Event Viewer:

Resolution

One specific problem is with the VMXNET3 adapters dropping inbound network packets because the inbound buffer is set too low to handle large amounts of traffic. We can easily find out if this is a problem by using Performance Monitor to look at the “Network Interface\Packets Received Discarded” counter.

Once you have added this counter, look at the Average, Minimum, and Maximum numbers and if they are any value higher than zero, then the receive buffer needs to be adjusted up for the adapter. This problem is documented in VMWare's Knowledge Base: Large packet loss at the guest OS level on the VMXNET3 vNIC in ESXi 5.x / 4.x.

IaaS with SQL Server - Tuning Failover Cluster Network Thresholds

12/9/2022 • 3 minutes to read • Edit Online

This article introduces solutions for adjusting the threshold of failover cluster networks.

Symptom

When running Windows Failover Cluster nodes in IaaS with a SQL Server Always On availability group, changing the cluster setting to a more relaxed monitoring state is recommended. Cluster settings out of the box are restrictive and could cause unneeded outages. The default settings are designed for highly tuned on premises networks and do not take into account the possibility of induced latency caused by a multi-tenant environment such as Windows Azure (IaaS).

Windows Server Failover Clustering is constantly monitoring the network connections and health of the nodes in a Windows Cluster. If a node is not reachable over the network, then recovery action is taken to recover and bring applications and services online on another node in the cluster. Latency in communication between cluster nodes can lead to the following error:

```
Error 1135 (system event log)
```

Cluster node **Node1** was removed from the active failover cluster membership. The Cluster service on this node may have stopped. This could also be due to the node having lost communication with other active nodes in the failover cluster. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapters on this node. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Cluster.log Example:

```
0000ab34.00004e64::2014/06/10-07:54:34.099 DBG   [NETFTAPI] Signaled NetftRemoteUnreachable event, local
address 10.xx.x.xxx:3343 remote address 10.x.xx.xx:3343
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] got event: Remote endpoint 10.xx.xx.xxx:~3343~
unreachable from 10.xx.x.xx:~3343~
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] Marking Route from 10.xxx.xxx.xxxx:~3343~ to
10.xxx.xx.xxxx:~3343~ as down
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [NDP] Checking to see if all routes for route (virtual)
local fexx::xxx:5dxx:xxxx:3xxx:~0~ to remote xxx::cxxx:xxxd:xxx:dxxx:~0~ are down
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [NDP] All routes for route (virtual) local
fxxx::xxxx:5xxx:xxxx:3xxx:~0~ to remote fexx::xxxx:xxxx:xxxx:xxxx:~0~ are down
0000ab34.00007328::2014/06/10-07:54:34.099 INFO  [CORE] Node 8: executing node 12 failed handlers on a
dedicated thread
0000ab34.00007328::2014/06/10-07:54:34.099 INFO  [NODE] Node 8: Cleaning up connections for n12.
0000ab34.00007328::2014/06/10-07:54:34.099 INFO  [Nodename] Clearing 0 unsent and 15 unacknowledged
messages.
0000ab34.00007328::2014/06/10-07:54:34.099 INFO  [NODE] Node 8: n12 node object is closing its connections
0000ab34.00008b68::2014/06/10-07:54:34.099 INFO  [DCM] HandleNetftRemoteRouteChange
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] Route history 1: Old: 05.936, Message: Response, Route
sequence: 150415, Received sequence: 150415, Heartbeats counter/threshold: 5/5, Error: Success, NtStatus: 0
Timestamp: 2014/06/10-07:54:28.000, Ticks since last sending: 4
0000ab34.00007328::2014/06/10-07:54:34.099 INFO  [NODE] Node 8: closing n12 node object channels
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] Route history 2: Old: 06.434, Message: Request, Route
sequence: 150414, Received sequence: 150402, Heartbeats counter/threshold: 5/5, Error: Success, NtStatus: 0
Timestamp: 2014/06/10-07:54:27.665, Ticks since last sending: 36
0000ab34.0000a8ac::2014/06/10-07:54:34.099 INFO  [DCM] HandleRequest: dcm/netftRouteChange
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] Route history 3: Old: 06.934, Message: Response, Route
sequence: 150414, Received sequence: 150414, Heartbeats counter/threshold: 5/5, Error: Success, NtStatus: 0
Timestamp: 2014/06/10-07:54:27.165, Ticks since last sending: 4
0000ab34.00004b38::2014/06/10-07:54:34.099 INFO  [IM] Route history 4: Old: 07.434, Message: Request, Route
sequence: 150413, Received sequence: 150401, Heartbeats counter/threshold: 5/5, Error: Success, NtStatus: 0
Timestamp: 2014/06/10-07:54:26.664, Ticks since last sending: 36
```

```
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <realLocal>10.xxx.xx.xxx:~3343~</realLocal>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <realRemote>10.xxx.xx.xxx:~3343~</realRemote>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <virtualLocal>fexx::xxxx:xxxx:xxxx:xxxx:~0~
</virtualLocal>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <virtualRemote>fexx::xxxx:xxxx:xxxx:xxxx:~0~
</virtualRemote>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <Delay>1000</Delay>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <Threshold>5</Threshold>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <Priority>140481</Priority>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO    <Attributes>2147483649</Attributes>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO  </struct mscs::FaultTolerantRoute>
0000ab34.00007328::2014/06/10-07:54:34.100 INFO   removed
```

```
0000ab34.0000a7c0::2014/06/10-07:54:38.433 ERR   [QUORUM] Node 8: Lost quorum (3 4 5 6 7 8)
0000ab34.0000a7c0::2014/06/10-07:54:38.433 ERR   [QUORUM] Node 8: goingAway: 0, core.IsServiceShutdown: 0
0000ab34.0000a7c0::2014/06/10-07:54:38.433 ERR   lost quorum (status = 5925)
```

Cause

There are two settings that are used to configure the connectivity health of the cluster.

Delay – This defines the frequency at which cluster heartbeats are sent between nodes. The delay is the number of seconds before the next heartbeat is sent. Within the same cluster, there can be different delays between nodes on the same subnet and between nodes, which are on different subnets.

Threshold – This defines the number of heartbeats, which are missed before the cluster takes recovery action. The threshold is a number of heartbeats. Within the same cluster, there can be different thresholds between nodes on the same subnet and between nodes that are on different subnets.

By default Windows Server 2016 sets the **SameSubnetThreshold** to 10 and **SameSubnetDelay** to 1000 ms. For example, if connectivity monitoring fails for 10 seconds, the failover Threshold is reached resulting in the unreachable that node being removed from cluster membership. This results in the resources being moved to another available node on the cluster. Cluster errors will be reported, including cluster error 1135 (above) is reported.

Resolution

To resolve this issue, relax the Cluster network configuration settings. See Heartbeat and threshold.

References

For more information on tuning Windows Cluster network configuration settings, see Tuning Failover Cluster Network Thresholds.

For information on using cluster.exe to tune Windows Cluster network configuration settings, see How to Configure Cluster Networks for a Failover Cluster.

Failover Clustering system log events

12/9/2022 • 66 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Azure Stack HCI, versions 21H2 and 20H2

This topic lists the Failover Clustering events from the Windows Server System log (viewable in Event Viewer). These events all share the event source of **FailoverClustering** and can be helpful when troubleshooting a cluster.

Critical events

Event 1000: UNEXPECTED_FATAL_ERROR

Cluster service suffered an unexpected fatal error at line %1 of source module %2. The error code was %3.

Event 1001: ASSERTION_FAILURE

Cluster service failed a validity check on line %1 of source module %2. '%3'

Event 1006: NM_EVENT_MEMBERSHIP_HALT

Cluster service was halted due to incomplete connectivity with other cluster nodes.

Event 1057: DM_DATABASE_CORRUPT_OR_MISSING

The cluster database could not be loaded. The file may be missing or corrupt. Automatic repair might be attempted.

Event 1070: NM_EVENT_BEGIN_JOIN_FAILED

The node failed to join failover cluster '%1' due to error code '%2'.

Event 1073: CS_EVENT_INCONSISTENCY_HALT

The Cluster service was halted to prevent an inconsistency within the failover cluster. The error code was '%1'.

Event 1080: CS_DISKWRITE_FAILURE

The Cluster service failed to update the cluster database (error code '%1'). Possible causes are insufficient disk space or file system corruption.

Event 1090: CS_EVENT_REG_OPERATION_FAILED

The Cluster service cannot be started. An attempt to read configuration data from the Windows registry failed with error '%1'. Please use the Failover Cluster Management snap-in to ensure that this machine is a member of a cluster. If you intend to add this machine to an existing cluster use the Add Node Wizard. Alternatively, if this machine has been configured as a member of a cluster, it will be necessary to restore the missing configuration data that is necessary for the Cluster Service to identify that it is a member of a cluster. Perform a System State Restore of this machine in order to restore the configuration data.

Event 1092: NM_EVENT_MM_FORM_FAILED

Failed to form cluster '%1' with error code '%2'. Failover cluster will not be available.

Event 1093: NM_EVENT_NODE_NOT_MEMBER

The Cluster service cannot identify node '%1' as a member of failover cluster '%2'. If the computer name for this node was recently changed, consider reverting to the previous name. Alternatively, add the node to the failover cluster and if necessary, reinstall clustered applications.

Event 1105: CS_EVENT_RPC_INIT_FAILED

The Cluster service failed to start because it was unable to register interface(s) with the RPC service. The error code was '%1'.

Event 1135: EVENT_NODE_DOWN

Cluster node '%1' was removed from the active failover cluster membership. The Cluster service on this node may have stopped. This could also be due to the node having lost communication with other active nodes in the failover cluster. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapters on this node. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1146: RCM_EVENT_RESMON_DIED

The cluster Resource Hosting Subsystem (RHS) process was terminated and will be restarted. This is typically associated with cluster health detection and recovery of a resource. Refer to the System event log to determine which resource and resource DLL is causing the issue.

Event 1177: MM_EVENT_ARBITRATION_FAILED

The Cluster service is shutting down because quorum was lost. This could be due to the loss of network connectivity between some or all nodes in the cluster, or a failover of the witness disk.

Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1181: NETRES_RESOURCE_START_ERROR

Cluster resource '%1' cannot be brought online because the associated service failed to start. The service return code is '%2'. Please check for additional events associated with the service and ensure the service starts correctly.

Event 1247: CLUSTER_EVENT_INVALID_SERVICE_SID_TYPE

The Security Identifier (SID) type for the cluster service is configured as '%1' but the expected SID type is 'Unrestricted'. The cluster service is automatically modifying its SID type configuration with the Service Control Manager (SCM) and will restart in order for this change to take effect.

Event 1248: CLUSTER_EVENT_SERVICE_SID_MISSING

The Security Identifier (SID) '%1' associated with the cluster service is not present in the process token. The cluster service will automatically correct this problem and restart.

Event 1282: SM_EVENT_HANDSHAKE_TIMEOUT

Security Handshake between local and remote endpoints '%2' did not complete in '%1' seconds, node terminating the connection

Event 1542: SERVICE_PRERESTORE_FAILED

The restore request for the cluster configuration data has failed. This restore failed during the 'pre-restore' stage usually indicating that some nodes comprising the cluster are not currently operational. Ensure that the cluster service is running successfully on all nodes comprising this cluster.

Event 1543: SERVICE_POSTRESTORE_FAILED

The restore operation of the cluster configuration data has failed. This restore failed during the 'post-restore' stage usually indicating that some nodes comprising the cluster are not currently operational. It is recommended that you replace the current cluster configuration data file (ClusDB) with '%1'.

Event 1546: SERVICE_FORM_VERSION_INCOMPATIBLE

Node '%1' failed to form a failover cluster. This was due to one or more nodes executing incompatible versions of the cluster service software. If node '%1' or a different node in the cluster has been recently upgraded, please

re-verify that all nodes are executing compatible versions of the cluster service software.

Event 1547: SERVICE_CONNECT_VERSION_INCOMPATIBLE

Node '%1' attempted to join a failover cluster but failed due to incompatibility between versions of the cluster service software. If node '%1' or a different node in the cluster has been recently upgraded, please verify that the changed cluster deployment with different versions of the cluster service software is supported.

Event 1553: SERVICE_NO_NETWORK_CONNECTIVITY

This cluster node has no network connectivity. It cannot participate in the cluster until connectivity is restored. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1554: SERVICE_NETWORK_CONNECTIVITY_LOST

This cluster node has lost all network connectivity. It cannot participate in the cluster until connectivity is restored. The cluster service on this node will be terminated.

Event 1556: SERVICE_UNHANDLED_EXCEPTION_IN_WORKER_THREAD

The cluster service encountered an unexpected problem and will be shut down. The error code was '%2'.

Event 1561: SERVICE_NONSTORAGE_WITNESS_BETTER_TAG

Cluster service failed to start because this node detected that it does not have the latest copy of cluster configuration data. Changes to the cluster occurred while this node was not in membership and as a result was not able to receive configuration data updates.

Guidance

Attempt to start the cluster service on all nodes in the cluster so that nodes with the latest copy of the cluster configuration data can first form the cluster. This node will then be able join the cluster and will automatically obtain the updated cluster configuration data. If there are no nodes available with the latest copy of the cluster configuration data, run the 'Start-ClusterNode -FQ' Windows PowerShell cmdlet. Using the ForceQuorum (FQ) parameter will start the cluster service and mark this node's copy of the cluster configuration data to be authoritative. Forcing quorum on a node with an outdated copy of the cluster database may result in cluster configuration changes that occurred while the node was not participating in the cluster to be lost.

Event 1564: RES_FSW_ARBITRATEFAILURE

File share witness resource '%1' failed to arbitrate for the file share '%2'. Please ensure that file share '%2' exists and is accessible by the cluster.

Event 1570: SERVICE_CONNECT_AUTHENTICATION_FAILURE

Node '%1' failed to establish a communication session while joining the cluster. This was due to an authentication failure. Please verify that the nodes are running compatible versions of the cluster service software.

Event 1571: SERVICE_CONNECT_AUTHORIZAION_FAILURE

Node '%1' failed to establish a communication session while joining the cluster. This was due to an authorization failure. Please verify that the nodes are running compatible versions of the cluster service software.

Event 1572: SERVICE_NETFT_ROUTE_INITIAL_FAILURE

Node '%1' failed to join the cluster because it could not send and receive failure detection network messages with other cluster nodes. Please run the Validate a Configuration wizard to ensure network settings. Also verify the Windows Firewall 'Failover Clusters' rules.

Event 1574: DM_DATABASE_UNLOAD_FAILED

The failover cluster database could not be unloaded. If restarting the cluster service does not fix the problem, please restart the machine.

Event 1575: DM_DATABASE_CORRUPT_OR_MISSING_FIXQUORUM

An attempt to forcibly start the cluster service has failed because the cluster configuration data on this node is either missing or corrupt. Please first start the cluster service on another node that has an intact and valid copy of the cluster configuration data. Then, reattempt the start operation on this node (which will attempt to obtain updated valid configuration information automatically). If no other node is available, please use WBAdmin.msc to perform a System State Restore of this node in order to restore the configuration data.

Event 1593: DM_COULD_NOT_DISCARD_CHANGES

The failover cluster database could not be unloaded and any potentially incorrect changes in memory could not be discarded. The cluster service will attempt to repair the database by retrieving it from another cluster node. If the cluster service does not come online, restart the cluster service on this node. If restarting the cluster service does not fix the problem, please restart the machine. If the cluster service fails to come online after a reboot, please restore the cluster database from the last backup. The current database was copied to '%1'. If no backups are available, please copy '%1' to '%2' and attempt to start the cluster service. If the cluster service then comes online on this node, some cluster configuration changes may be lost and the cluster may not function properly. Run the Validate a Configuration wizard to check your cluster configuration and verify that the hosted Services and Applications are online and functioning correctly.

Event 1672: EVENT_NODE_QUARANTINED

Cluster node '%1' has been quarantined. The node experienced '%2' consecutive failures within a short amount of time and has been removed from the cluster to avoid further disruptions. The node will be quarantined until '%3' and then the node will automatically attempt to re-join the cluster.

Refer to the System and Application event logs to determine the issues on this node. When the issue is resolved, quarantine can be manually cleared to allow the node to rejoin with the 'Start-ClusterNode –ClearQuarantine' Windows PowerShell cmdlet.

Node Name : %1

Number of consecutive cluster membership loses: %2

Time quarantine will be automatically cleared: %3

Error events

Event 1024: CP_REG_CKPT_RESTORE_FAILED

The registry checkpoint for cluster resource '%1' could not be restored to registry key HKEY_LOCAL_MACHINE\%2. The resource may not function correctly. Make sure that no other processes have open handles to registry keys in this registry subtree.

Event 1034: RES_DISK_MISSING

Cluster physical disk resource '%1' cannot be brought online because the associated disk could not be found. The expected signature of the disk was '%2'. If the disk was replaced or restored, in the Failover Cluster Manager snap-in, you can use the Repair function (in the properties sheet for the disk) to repair the new or restored disk. If the disk will not be replaced, delete the associated disk resource.

Event 1035: RES_DISK_MOUNT_FAILED

While disk resource '%1' was being brought online, access to one or more volumes failed with error '%2'. Run the Validate a Configuration wizard to check your storage configuration. Optionally you may want to run Chkdsk to verify the integrity of all volumes on this disk.

Event 1037: RES_DISK_FILESYSTEM_FAILED

The file system for one or more partitions on the disk for resource '%1' may be corrupt. Run the Validate a Configuration wizard to check your storage configuration. Optionally, you may want to run Chkdsk to verify the integrity of all volumes on this disk.

Event 1038: RES_DISK_RESERVATION_LOST

Ownership of cluster disk '%1' has been unexpectedly lost by this node. Run the Validate a Configuration wizard to check your storage configuration.

Event 1039: RES_GENAPP_CREATE_FAILED

Generic application '%1' could not be brought online (with error '%2') during an attempt to create the process. Possible causes include: the application may not be present on this node, the path name may have been specified incorrectly, the binary name may have been specified incorrectly.

Event 1040: RES_GENSVC_OPEN_FAILED

Generic service '%1' could not be brought online (with error '%2') during an attempt to open the service. Possible causes include: the service is either not installed or the specified service name is invalid.

Event 1041: RES_GENSVC_START_FAILED

Generic service '%1' could not be brought online (with error '%2') during an attempt to start the service. Possible cause: the specified service parameters might be invalid.

Event 1042: RES_GENSVC_FAILED_AFTER_START

Generic service '%1' failed with error '%2'. Please examine the application event log.

Event 1044: RES_IPADDR_NBT_INTERFACE_CREATE_FAILED

Encountered a failure when attempting to create a new NetBIOS interface while bringing resource '%1' online (error code '%2'). The maximum number of NetBIOS names may have been exceeded.

Event 1046: RES_IPADDR_INVALID_SUBNET

Cluster IP address resource '%1' cannot be brought online because the subnet mask value is invalid. Please check your IP address resource properties.

Event 1047: RES_IPADDR_INVALID_ADDRESS

Cluster IP address resource '%1' cannot be brought online because the address value is invalid. Please check your IP address resource properties.

Event 1048: RES_IPADDR_INVALID_ADAPTER

Cluster IP address resource '%1' failed to come online. Configuration data for the network adapter corresponding to cluster network interface '%2' could not be determined (error code was '%3'). Please check that the IP address resource is configured with the correct address and network properties.

Event 1049: RES_IPADDR_IN_USE

Cluster IP address resource '%1' cannot be brought online because a duplicate IP address '%2' was detected on the network. Please ensure all IP addresses are unique.

Event 1050: RES_NETNAME_DUPLICATE

Cluster network name resource '%1' cannot be brought online because name '%2' matches this cluster node name. Ensure that network names are unique.

Event 1051: RES_NETNAME_NO_IP_ADDRESS

Cluster network name resource '%1' cannot be brought online. Ensure that the network adapters for dependent IP address resources have access to at least one DNS server. Alternatively, enable NetBIOS for dependent IP addresses.

Event 1052: RES_NETNAME_CANT_ADD_NAME_STATUS

Cluster Network Name resource '%1' cannot be brought online because the name could not be added to the system. The associated error code is stored in the data section.

Event 1053: RES_SMB_CANT_CREATE_SHARE

Cluster File Share '%1' cannot be brought online because the share could not be created.

Event 1054: RES_SMB_SHARE_NOT_FOUND

Health check for file share resource '%1' failed. Retrieving information for share '%2' (scoped to network name %3) returned error code '%4'. Ensure the share exists and is accessible.

Event 1055: RES_SMB_SHARE_FAILED

Health check for file share resource '%1' failed. Retrieving information for share '%2' (scoped to network name %3) indicated that the share does not exist (error code '%4'). Please ensure the share exists and is accessible.

Event 1069: RCM_RESOURCE_FAILURE

Cluster resource '%1' in clustered role '%2' failed.

Event 1069: RCM_RESOURCE_FAILURE_WITH_TYPENAME

Cluster resource '%1' of type '%3' in clustered role '%2' failed.

Based on the failure policies for the resource and role, the cluster service may try to bring the resource online on this node or move the group to another node of the cluster and then restart it. Check the resource and group state using Failover Cluster Manager or the Get-ClusterResource Windows PowerShell cmdlet.

Event 1069: RCM_RESOURCE_FAILURE_WITH_CAUSE

Cluster resource '%1' of type '%3' in clustered role '%2' failed. The error code was '%5' ('%4').

Based on the failure policies for the resource and role, the cluster service may try to bring the resource online on this node or move the group to another node of the cluster and then restart it. Check the resource and group state using Failover Cluster Manager or the Get-ClusterResource Windows PowerShell cmdlet.

Event 1069: RCM_RESOURCE_FAILURE_WITH_ERROR_CODE

Cluster resource '%1' of type '%3' in clustered role '%2' failed. The error code was '%4'.

Based on the failure policies for the resource and role, the cluster service may try to bring the resource online on this node or move the group to another node of the cluster and then restart it. Check the resource and group state using Failover Cluster Manager or the Get-ClusterResource Windows PowerShell cmdlet.

Event 1069: RCM_RESOURCE_FAILURE_DUE_TO_VETO

Cluster resource '%1' of type '%3' in clustered role '%2' failed due to an attempt to block a required state change in that cluster resource.

Event 1077: RES_IPADDR_IPV4_ADDRESS_INTERFACE_FAILED

Health check for IP interface '%1' (address '%2') failed (status is '%3'). Run the Validate a Configuration wizard to ensure that the network adapter is functioning properly.

Event 1078: RES_IPADDR_WINS_ADDRESS_FAILED

Cluster IP address resource '%1' cannot be brought online because WINS registration failed on interface '%2' with error '%3'. Ensure that a valid, accessible WINS server has been specified.

Event 1121: CP_CRYPTO_CKPT_RESTORE_FAILED

Encrypted settings for cluster resource '%1' could not be successfully applied to the container name '%2' on this node.

Event 1127: TM_EVENT_CLUSTER_NETINTERFACE_FAILED

Cluster network interface '%1' for cluster node '%2' on network '%3' failed. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1129: TM_EVENT_CLUSTER_NETWORK_PARTITIONED

Cluster network '%1' is partitioned. Some attached failover cluster nodes cannot communicate with each other over the network. The failover cluster was not able to determine the location of the failure. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1130: TM_EVENT_CLUSTER_NETWORK_DOWN

Cluster network '%1' is down. None of the available nodes can communicate using this network. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1137: RCM_DRAIN_MOVE_FAILED

Move of cluster role '%1' for drain could not be completed. The operation failed with error code %2.

Event 1138: RES_SMB_CANT_CREATE_DFS_ROOT

Cluster file share resource '%1' cannot be brought online. Creation of DFS namespace root failed with error '%3'. This may be due to failure to start the 'DFS Namespace' service or failure to create the DFS-N root for share '%2'.

Event 1141: RES_SMB_CANT_INIT_DFS_SVC

Cluster file share resource '%1' cannot be brought online. Resynchronization of DFS root target '%2' failed with error '%3'.

Event 1142: RES_SMB_CANT_ONLINE_DFS_ROOT

Cluster file share resource '%1' for DFS Namespace cannot be brought online due to error '%2'.

Event 1182: NETRES_RESOURCE_STOP_ERROR

Cluster resource '%1' cannot be brought online because the associated service failed an attempted restart. The error code is '%2'. The service required a restart in order to update parameters. However, the service failed before it could be stopped and restarted. Please check for additional events associated with the service and ensure the service is functioning correctly.

Event 1183: RES_DISK_INVALID_MP_SOURCE_NOT_CLUSTERED

Cluster disk resource '%1' contains an invalid mount point. Both the source and target disks associated with the mount point must be clustered disks, and must be members of the same group.
Mount point '%2' for volume '%3' references an invalid source disk. Please ensure that the source disk is also a clustered disk and in the same group as the target disk (hosting the mount point).

Event 1191: RES_NETNAME_DELETE_COMPUTER_ACCOUNT_FAILED_STATUS

Cluster network name resource '%1' failed to delete its associated computer object in domain '%2'. The error code was '%3'.
Please have a domain administrator manually delete the computer object from the Active Directory domain.

Event 1192: RES_NETNAME_DELETE_COMPUTER_ACCOUNT_FAILED

Cluster network name resource '%1' failed to delete its associated computer object in domain '%2' for the following reason:
%3.

Please have a domain administrator manually delete the computer object from the Active Directory domain.

Event 1193: RES_NETNAME_ADD_COMPUTER_ACCOUNT_FAILED_STATUS

Cluster network name resource '%1' failed to create its associated computer object in domain '%2' for the

following reason: %3.

The associated error code is: %5

Please work with your domain administrator to ensure that:

- The cluster identity '%4' can create computer objects. By default all computer objects are created in the 'Computers' container; consult the domain administrator if this location has been changed.
- The quota for computer objects has not been reached.
- If there is an existing computer object, verify the Cluster Identity '%4' has 'Full Control' permission to that computer object using the Active Directory Users and Computers tool.

Event 1194: RES_NETNAME_ADD_COMPUTER_ACCOUNT_FAILED

Cluster network name resource '%1' failed to create its associated computer object in domain '%2' during: %3.

The text for the associated error code is: %4

Please work with your domain administrator to ensure that:

- The cluster identity '%5' has Create Computer Objects permissions. By default all computer objects are created in the same container as the cluster identity '%5'.
- The quota for computer objects has not been reached.
- If there is an existing computer object, verify the Cluster Identity '%5' has 'Full Control' permission to that computer object using the Active Directory Users and Computers tool.

Event 1195: RES_NETNAME_DNS_REGISTRATION_FAILED_STATUS

Cluster network name resource '%1' failed registration of one or more associated DNS name(s). The error code was '%2'. Ensure that the network adapters associated with dependent IP address resources are configured with access to at least one DNS server.

Event 1196: RES_NETNAME_DNS_REGISTRATION_FAILED

Cluster network name resource '%1' failed registration of one or more associated DNS name(s) for the following reason:
%2.

Ensure that the network adapters associated with dependent IP address resources are configured with at least one accessible DNS server.

Event 1205: RCM_EVENT_GROUP_FAILED_ONLINE_OFFLINE

The Cluster service failed to bring clustered role '%1' completely online or offline. One or more resources may be in a failed state. This may impact the availability of the clustered role.

Event 1206: RES_NETNAME_UPDATE_COMPUTER_ACCOUNT_FAILED_STATUS

The computer object associated with the cluster network name resource '%1' could not be updated in domain '%2'. The error code was '%3'. The cluster identity '%4' may lack permissions required to update the object. Please work with your domain administrator to ensure that the cluster identity can update computer objects in the domain.

Event 1207: RES_NETNAME_UPDATE_COMPUTER_ACCOUNT_FAILED

The computer object associated with the cluster network name resource '%1' could not be updated in domain '%2' during the
%3 operation.

The text for the associated error code is: %4

The cluster identity '%5' may lack permissions required to update the object. Please work with your domain administrator to ensure that the cluster identity can update computer objects in the domain.

Event 1208: RES_DISK_INVALID_MP_TARGET_NOT_CLUSTERED

Cluster disk resource '%1' contains an invalid mount point. Both the source and target disks associated with the mount point must be clustered disks, and must be members of the same group.
Mount point '%2' for volume '%3' references an invalid target disk. Please ensure that the target disk is also a clustered disk and in the same group as the source disk (hosting the mount point).

Event 1211: RES_NETNAME_NO_WRITEABLE_DC_STATUS

Cluster network name resource '%1' cannot be brought online. Attempt to locate a writeable domain controller (in domain %2) in order to create or update a computer object associated with the resource failed. The error code was '%3'. Ensure that a writeable domain controller is accessible to this node within the configured domain. Also ensure that the DNS server is running in order to resolve the name of the domain controller.

Event 1212: RES_NETNAME_NO_WRITEABLE_DC

Cluster network name resource '%1' cannot be brought online. Attempt to locate a writeable domain controller (in domain %2) in order to create or update a computer object associated with the resource failed for the following reason:
%3.

The error code was '%4'. Ensure that a writeable domain controller is accessible to this node within the configured domain. Also ensure that the DNS server is running in order to resolve the name of the domain controller.

Event 1213: RES_NETNAME_RENAME_RESTORE_FAILED

Cluster network name resource '%1' could not completely rename the associated computer object on domain controller '%2'. Attempting to rename the computer object from new name '%3' back to its original name '%4' has also failed. The error code was '%5'. This may affect client connectivity until the network name and its associated computer object name are consistent. Contact your domain administrator to manually rename the computer object.

Event 1214: RES_NETNAME_CANT_ADD_NAME2

Cluster Network Name resource cannot be registered with Netbios.

Network Name: '%3'
Reason for failure: %2
Resource name:'%1'

Run nbtstat for the network name to ensure that the name is not already registered with Netbios.

Event 1215: RES_NETNAME_NOT_REGISTERED_WITH_RDR

Cluster network name resource '%1' failed a health check. Network name '%2' is no longer registered on this node. The error code was '%3'. Check for hardware or software errors related to the network adapter. Also, you can run the Validate a Configuration wizard to check your network configuration.

Event 1218: RES_NETNAME_ONLINE_RENAME_RECOVERY_MISSING_ACCOUNT

Cluster network name resource '%1' failed to perform a name change operation (attempting to change original name '%3' to name '%4'). The computer object could not be found on the domain controller '%2' (where it was created). An attempt will be made to recreate the computer object the next time the resource is brought online. Additionally, please work with your domain administrator to ensure that the computer object exists in the domain.

Event 1219: RES_NETNAME_ONLINE_RENAME_DC_NOT_FOUND

Cluster network name resource '%1' failed to perform a name change operation. The domain controller '%2' where computer object '%3' was being renamed, could not be contacted. The error code was '%4'. Ensure a writeable domain controller is accessible and check for any connectivity issue.

Event 1220: RES_NETNAME_ONLINE_RENAME_RECOVERY_FAILED

The computer account for resource '%1' failed to be renamed from %2 to %3 using Domain Controller %4. The associated error code is stored in the data section.

The computer account for this resource was in the process of being renamed and did not complete. This was detected during the online process for this resource. In order to recover, the computer account must be renamed to the current value of the Name property, i.e., the name presented on the network.

The Domain Controller where the renamed was attempted might not be available; if this is the case, wait for the Domain Controller to be available again. The Domain Controller could be denying access to the account; after resolving access, try to bring the name online again.

If this is not possible, disable and re-enable Kerberos Authentication and an attempt will be made to find the computer account on a different DC. You need to change the Name property to %2 in order to use the existing computer account.

Event 1223: RES_IPADDR_INVALID_NETWORK_ROLE

Cluster IP address resource '%1' cannot be brought online because the cluster network '%2' is not configured to allow client access. Please use the Failover Cluster Manager snap-in to check the configured properties of the cluster network.

Event 1226: RES_NETNAME_TCB_NOT_HELD

Network Name resource '%1' (with associated network name '%2') has Kerberos Authentication support enabled. Failed to add required credentials to the LSA - the associated error code '%3' indicates insufficient privileges normally required for this operation. The required privilege is 'Trusted Computing Base' and must be locally enabled on each node comprising the cluster.

Event 1227: RES_NETNAME_LSA_ERROR

Network Name resource '%1' (with associated network name '%2') has Kerberos Authentication support enabled. Failed to add required credentials to the LSA - the associated error code is '%3'.

Event 1228: RES_NETNAME_CLONE_FAILURE

Cluster network name resource '%1' encountered an error enabling the network name on this node. The reason for the failure was:
'%2'.

The error code was '%3'.

You may take the network name resource offline and online again to retry.

Event 1229: RES_NETNAME_NO_IPS_FOR_DNS

Cluster network name resource '%1' was unable to identify any IP addresses to register with a DNS server. Ensure that there is one or more networks that are enabled for cluster use with the 'Allow clients to connect through this network' setting, and that each node has a valid IP address configured for the networks.

Event 1230: RCM_DEADLOCK_OR_CRASH_DETECTED

A component on the server did not respond in a timely fashion. This caused the cluster resource '%1' (resource type '%2', DLL '%3') to exceed its time-out threshold. As part of cluster health detection, recovery actions will be

taken. The cluster will try to automatically recover by terminating and restarting the Resource Hosting Subsystem (RHS) process that is running this resource. Verify that the underlying infrastructure (such as storage, networking, or services) that are associated with the resource are functioning correctly.

Event 1230: RCM_RESOURCE_CONTROL_DEADLOCK_DETECTED

A component on the server did not respond in a timely fashion. This caused the cluster resource '%1' (resource type '%2', DLL '%3') to exceed its time-out threshold while processing control code '%4;'. As part of cluster health detection, recovery actions will be taken. The cluster will try to automatically recover by terminating and restarting the Resource Hosting Subsystem (RHS) process that is running this resource. Verify that the underlying infrastructure (such as storage, networking, or services) that are associated with the resource are functioning correctly.

Event 1231: RES_NETNAME_LOGON_FAILURE

Cluster network name resource '%1' encountered an error logging on to the domain. The reason for the failure was:
'%2'.

The error code was '%3'.

Ensure that a domain controller is accessible to this node within the configured domain.

Event 1232: RES_GENSCRIPT_TIMEOUT

Entry point '%2' in cluster generic script resource '%1' did not complete execution in a timely manner. This could be due to an infinite loop or other issues possibly resulting in an infinite wait. Alternatively, the specified pending timeout value may be too short for this resource. Please review the '%2' script entry point to ensure all possible infinite waits in the script code have been corrected. Then, consider increasing the pending timeout value if deemed necessary.

Event 1233: RES_GENSCRIPT_HANGMODE

Cluster generic script resource '%1': request to perform the '%2' operation will not be processed. This is due to a previously failed attempt to execute the '%3' entry point in a timely fashion. Please review the script code for this entry point to ensure there does not exist any infinite loop or other issues possibly resulting in an infinite wait. Then, consider increasing the resource pending timeout value if deemed necessary.

Event 1234: CLUSTER_EVENT_ACCOUNT_MISSING_PRIVS

The Cluster service has detected that its service account is missing one or more of the required privileges. The missing privilege list is: '%1' and is not currently granted to the service account. Use the 'sc.exe qprivs clussvc' to verify the privileges of the Cluster service (ClusSvc). Additionally check for any security policies or group policies in Active Directory Domain Services that may have altered the default privileges. Type the following command to grant the Cluster service the necessary privileges to function correctly:

```
sc.exe privs
clussvc
SeBackupPrivilege/SeRestorePrivilege/SeIncreaseQuotaPrivilege/SeIncreaseBasePriorityPrivilege/SeTcbPrivilege
/SeDebugPrivilege/SeSecurityPrivilege/SeAuditPrivilege/SeImpersonatePrivilege/SeChangeNotifyPrivilege/SeIncr
easeWorkingSetPrivilege/SeManageVolumePrivilege/SeCreateSymbolicLinkPrivilege/SeLoadDriverPrivilege
```

Event 1242: RES_IPADDR_LEASE_EXPIRED

Lease of IP address '%2' associated with cluster IP address resource '%1' has expired or is about to expire, and currently cannot be renewed. Ensure that the associated DHCP server is accessible and properly configured to renew the lease on this IP address.

Event 1245: RES_IPADDR_LEASE_RENEWAL_FAILED

Cluster IP address resource '%1' failed to renew the lease for IP address '%2'. Ensure that the DHCP server is

accessible and properly configured to renew the lease on this IP address.

Event 1250: RCM_RESOURCE_EMBEDDED_FAILURE

Cluster resource '%1' in clustered role '%2' has received a critical state notification. For a virtual machine this indicates that an application or service inside the virtual machine is in an unhealthy state. Verify the functionality of the service or application being monitored within the virtual machine.

Event 1254: RCM_GROUP_TERMINAL_FAILURE

Clustered role '%1' has exceeded its failover threshold. It has exhausted the configured number of failover attempts within the failover period of time allotted to it and will be left in a failed state. No additional attempts will be made to bring the role online or fail it over to another node in the cluster. Please check the events associated with the failure. After the issues causing the failure are resolved the role can be brought online manually or the cluster may attempt to bring it online again after the restart delay period.

Event 1255: RCM_RESOURCE_NETWORK_FAILURE

Cluster resource '%1' in clustered role '%2' has received a critical state notification. For a virtual machine this indicates that a critical network of the virtual machine is in an unhealthy state. Verify the network connectivity of the virtual machine and the virtual networks that the virtual machine is configured to use.

Event 1256: RES_NETNAME_DNS_REGISTRATION_FAILED_DYNAMIC_DNS_ZONE

Cluster network name resource failed registration of one or more associated DNS names(s) because the corresponding DNS Zone does not accept dynamic updates.

Cluster Network name: '%1'
DNS Zone: '%2'

Guidance

Ensure that the DNS is configured as a Dynamic DNS zone. If the DNS server does not accept dynamic updates uncheck the 'Register this connection's' addresses in DNS' in the properties of the network adapter.

Event 1257: RES_NETNAME_DNS_REGISTRATION_FAILED_SECURE_DNS_ZONE

Cluster network name resource failed registration of one or more associated DNS names(s) because the access to update the secure DNS Zone was denied.

Cluster Network name: '%1'
DNS Zone: '%2'

Ensure that cluster name object (CNO) is granted permissions to the Secure DNS Zone.

Event 1258: RES_NETNAME_DNS_REGISTRATION_FAILED_TIMEOUT

Cluster network name resource failed registration of one or more associated DNS name(s) because the a DNS server could not be reached.

Cluster Network name: '%1'
DNS Zone: '%2'
DNS Server: '%3'

Ensure that the network adapters associated with dependent IP address resources are configured with at least one accessible DNS server.

Event 1259: RES_NETNAME_DNS_REGISTRATION_FAILED_CLEANUP

Cluster network name resource failed registration of one or more associated DNS name(s) because the cluster service failed clean up the existing records corresponding to the network name.

Cluster Network name: '%1'
DNS Zone: '%2'

Ensure that cluster name object (CNO) is granted permissions to the Secure DNS Zone.

Event 1260: RES_NETNAME_DNS_REGISTRATION_MODIFY_FAILED

Cluster network name resource failed to modify the DNS registration.

Cluster Network name: '%1'
Error code: '%2'

Guidance

Ensure that the network adapters associated with dependent IP address resources are configured with access to at least one DNS server.

Event 1261: RES_NETNAME_DNS_REGISTRATION_MODIFY_FAILED_STATUS

Cluster network name resource failed to modify the DNS registration.

Cluster Network name: '%1'
Reason: '%2'

Guidance

Ensure that the network adapters associated with dependent IP address resources are configured with access to at least one DNS server.

Event 1262: RES_NETNAME_DNS_REGISTRATION_PUBLISH_PTR_FAILED

Cluster network name resource failed to publish the PTR record in the DNS reverse lookup zone.

Cluster Network name: '%1'
Error Code: '%2'

Guidance

Ensure that the network adapters associated with dependent IP address resources are configured with access to at least one DNS server and that the DNS reverse lookup zone exists.

Event 1264: RES_NETNAME_DNS_REGISTRATION_PUBLISH_PTR_FAILED_STATUS

Cluster network name resource failed to publish the PTR record in the DNS reverse lookup zone.

Cluster Network name: '%1'
Reason: '%2'

Guidance

Ensure that the network adapters associated with dependent IP address resources are configured with access to at least one DNS server and that the DNS reverse lookup zone exists.

Event 1265: RES_TYPE_CONTROL_TIMED_OUT

Cluster resource type '%1' timed out while processing the control code %2. The cluster will try to automatically recover by terminating and restarting the Resource Hosting Subsystem (RHS) process that was processing the call.

Event 1289: NETFT_ADAPTER_NOT_FOUND

The Cluster Service was unable to access network adapter '%1'. Verify that other network adapters are functioning properly and check the device manager for errors associated with adapter '%1'. If the configuration for adapter '%1' has been changed, it may become necessary to reinstall the failover clustering feature on this computer.

Event 1360: RES_IPADDR_INVALID_NETWORK

Cluster IP address resource '%1' failed to come online. Ensure the network property '%2' matches a cluster network name or the address property '%3' matches one of the subnets on a cluster network. If this is an IPv6 Address type, please verify that the cluster network matching this resource has at least one IPv6 prefix that is not link-local or tunnel.

Event 1361: RES_IPADDR_MISSING_DEPENDANT

IPv6 Tunnel address resource '%1' failed to come online because it does not depend on an IP Address (IPv4) resource. Dependency on at least one IP Address (IPv4) resource is required.

Event 1362: RES_IPADDR_MISSING_DATA

Cluster IP address resource '%1' failed to come online because the '%2' property could not be read. Please ensure that the resource is correctly configured.

Event 1363: RES_IPADDR_NO_ISATAP_SUPPORT

IPv6 tunnel address resource '%1' failed to come online. Cluster network '%2' associated with dependent IP address (IPv4) resource '%3' does not support ISATAP tunneling. Please ensure that the cluster network supports ISATAP tunneling.

Event 1540: SERVICE_BACKUP_NOQUORUM

The backup operation for the cluster configuration data has been aborted because quorum for the cluster has not yet been achieved. Please retry this backup operation after the cluster achieves quorum.

Event 1554: SERVICE_RESTORE_INVALIDUSER

The restore operation for the cluster configuration data has failed. This was due to insufficient privileges associated with the user account performing the restore. Please ensure that the user account has local administrator privileges.

Event 1557: SERVICE_WITNESS_ATTACH_FAILED

Cluster service failed to update the cluster configuration data on the witness resource. Please ensure that the witness resource is online and accessible.

Event 1559: RES_WITNESS_NEW_NODE_CONFLICT

File share '%1' associated with the file share witness resource is currently hosted by server '%2'. This server '%2' has just been added as a new node within the failover cluster. Hosting of the file share witness by any node comprising the same cluster is not recommended. Please choose a file share witness that is not hosted by any node within the same cluster and modify settings of the file share witness resource accordingly.

Event 1560: RES_SMB_SHARE_CONFLICT

Cluster file share resource '%1' has detected shared folder conflicts. As a result, some of these shared folders may not be accessible. To rectify this situation, ensure multiple shared folders do not have the same share name.

Event 1563: RES_FSW_ONLINEFAILURE

File share witness resource '%1' failed to come online. Please ensure that file share '%2' exists and is accessible by the cluster.

Event 1566: RES_NETNAME_TIMEDOUT

Cluster network name resource '%1' cannot be brought online. The network name resource was terminated by the resource host subsystem because it did not complete an operation in an acceptable time. The operation timed out while performing:
'%2'

Event 1567: SERVICE_FAILED_TO_CHANGE_LOG_SIZE

Cluster service failed to change the trace log size. Please verify the ClusterLogSize setting with the 'Get-Cluster |

Format-List *' PowerShell cmdlet. Also, use the Performance Monitor snap-in to verify the event trace session settings for FailoverClustering.

Event 1567: RES_VIPADDR_ADDRESS_INTERFACE_FAILED

Health check for IP interface '%1'(address '%2') failed (status is '%3'). Check for hardware or software errors related to the physical or virtual network adapters.

Event 1568: RES_CLOUD_WITNESS_CANT_COMMUNICATE_TO_AZURE

Cloud witness resource could not reach Microsoft Azure storage services.

Cluster resource: %1
Cluster node: %2

Guidance

This could be due to network communication between the cluster node and the Microsoft Azure service being blocked. Verify the node's internet connectivity to Microsoft Azure. Connect to the Microsoft Azure portal and verify that the storage account exists.

Event 1569: SERVICE_USING_RESTRICTED_NETWORK

Network '%1' which has been disabled for failover cluster use, was found to be the only currently possible network that node '%2' can use to communicate with other nodes in the cluster. This may impact the node's ability to participate in the cluster. Please verify network connectivity of node '%2' and enable at least one network for cluster communication. Run the Validate a Configuration wizard to check your network configuration.

Event 1569: RES_CLOUD_WITNESS_TOKEN_EXPIRED

Cloud witness resource failed to authenticate with Microsoft Azure storage services. An access denied error was returned while attempting to contact the Microsoft Azure storage account.

Cluster resource: %1

Guidance

The storage account's access key may no longer be valid. Use the Configure Cluster Quorum Wizard in the Failover Cluster Manager or the Set-ClusterQuorum Windows PowerShell cmdlet, to configure the Cloud witness resource with the updated storage account access key.

Event 1573: SERVICE_FORM_WITNESS_FAILED

Node '%1' failed to form a cluster. This was because the witness was not accessible. Please ensure that the witness resource is online and available.

Event 1580: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_FAILED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4' in a secure DNS zone. This was due to an existing record with this name and the cluster identity does not have the sufficient privileges to update that record. The error code was '%3'. Please contact your DNS server administrator to verify the cluster identity has permissions on DNS record '%2'.

Event 1580: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_FAILED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4' in a secure DNS zone. This was due to an existing record with this name and the cluster identity does not have the sufficient privileges to update that record. The error code was '%3'. Please contact your DNS server administrator to verify the cluster identity has permissions on DNS record '%2'.

Event 1585: RES_FILESERVER_FSCHECK_SRVSVC_STOPPED

Cluster file server resource '%1' failed a health check. This was due to the Server service not being started. Please use Server Manager to confirm the state of the Server service on this cluster node.

Event 1586: RES_FILESERVER_FSCHECK_SCOPED_NAME_NOT_REGISTERED

Cluster file server resource '%1' failed a health check. This was because some of its shared folders were inaccessible. Verify that the folders are accessible from clients. Additionally, confirm the state of the Server service on this cluster node using Server Manager and look for other events related to the Server service on this cluster node. It may be necessary to restart the network name resource '%2' in this clustered role.

Event 1587: RES_FILESERVER_FSCHECK_FAILED

Cluster file server resource '%1' failed a health check. This was because some of its shared folders were inaccessible. Verify that the folders are accessible from clients. Additionally, confirm the state of the Server service on this cluster node using Server Manager and look for other events related to the Server service on this cluster node.

Event 1588: RES_FILESERVER_SHARE_CANT_ADD

Cluster file server resource '%1' cannot be brought online. The resource failed to create file share '%2' associated with network name '%3'. The error code was '%4'. Verify that the folders exist and are accessible. Additionally, confirm the state of the Server service on this cluster node using Server Manager and look for other related events on this cluster node. It may be necessary to restart the network name resource '%3' in this clustered role.

Event 1600: CLUSAPI_CREATE_CANNOT_SET_AD_DACL

Cluster service failed to set the permissions on the cluster computer object '%1'. Please contact your network administrator to check the cluster security descriptor of the computer object in Active Directory, verify that the DACL is not too big, and remove any unnecessary extra ACE(s) on the object if necessary.

Event 1603: RES_FILESERVER_CLONE_FAILED

File Server could not start because expected dependency on 'Network Name' resource was not found or it was not configured properly. Error=0x%2.

Event 1606: RES_DISK_CNO_CHECK_FAILED

Cluster disk resource '%1' contains a BitLocker-protected volume, '%2', but for this volume, the Active Directory cluster name account (also called the cluster name object or CNO) is not a BitLocker protector for the volume. This is required for BitLocker-protected volumes. To correct this, first remove the disk from the cluster. Next, use the Manage-bde.exe command-line tool to add the cluster name as an ADAccountOrGroup protector, using the format domain\ClusterName$ for the cluster name. Then add the disk back to the cluster. For more information, see the documentation for Manage-bde.exe

Event 1607: RES_DISK_CNO_UNLOCK_FAILED

Cluster disk resource '%1' was unable to unlock the BitLocker-protected volume '%2'. The cluster name object (CNO) is not set to be a valid BitLocker protector for this volume. To correct this, remove the disk from the cluster. Then use the Manage-bde.exe command-line tool to add the cluster name as an ADAccountOrGroup protector, using the format domain\ClusterName$, and add the disk back to the cluster. For more information, see the documentation for Manage-bde.exe.

Event 1608: RES_FILESERVER_LEADER_FAILED

File Server could not start because expected dependency on 'Network Name' resource was not found or it was not configured properly. Error=0x%2.

Event 1609: RES_SODA_FILESERVER_LEADER_FAILED

Scale Out File Server could not start because expected dependency on 'Distributed Network Name' resource was not found or it was not configured properly. Error=0x%2.

Event 1632: CLUSAPI_CREATE_MISMATCHED_OU

The creation of the cluster failed. Unable to create the cluster name object '%1' in active directory organizational unit '%2'. The object already exists in organizational unit '%3'. Verify that the specified distinguished name path

and the cluster name object are correct. If the distinguished name path is not specified, the existing computer object '%1' will be used.

Event 1652: SERVICE_TCP_CONNECTION_FAILURE

Cluster node '%1' failed to join the cluster. A TCP connection could not be established to node(s) '%2'. Verify network connectivity and configuration of any network firewalls.

Event 1652: SERVICE_UDP_CONNECTION_FAILURE

Cluster node '%1' failed to join the cluster. A UDP connection could not be established to node(s) '%2'. Verify network connectivity and configuration of any network firewalls.

Event 1652: SERVICE_VIRTUAL_TCP_CONNECTION_FAILURE

Cluster node '%1' failed to join the cluster. A TCP connection using the Microsoft Failover Cluster Virtual Adapter could not be established to node(s) '%2'. Verify network connectivity and configuration of any network firewalls.

Event 1653: SERVICE_NO_CONNECTIVITY

Cluster node '%1' failed to join the cluster because it could not communicate over the network with any other node in the cluster. Verify network connectivity and configuration of any network firewalls.

Event 1654: RES_VIPADDR_INVALID_ADAPTERNAME

Cluster Disjoint IP address resource '%1' failed to come online. Configuration data for the network adapter corresponding to network adapter '%2' could not be determined (error code was '%3'). Check that the IP address resource is configured with the correct address and network properties.

Event 1655: RES_VIPADDR_INVALID_VSID

Cluster Disjoint IP address resource '%1' failed to come online. Configuration data for the network adapter corresponding to Virtual Subnet Id '%2' and Routing Domain Id '%3' could not be determined (error code was '%4'). Check that the IP address resource is configured with the correct address and network properties.

Event 1656: RES_VIPADDR_ADDRESS_CREATE_FAILED

Failed to add the IP Address '%2' for Disjoint IP address resource '%1' (error code was '%3'). Check for hardware or software errors related to the physical or virtual network adapters.

Event 1664: CLUSTER_UPGRADE_INCOMPLETE

Upgrading the functional level of the cluster failed. Check that all nodes of the cluster are currently running and are the same version of Windows Server, then run the Update-ClusterFunctionalLevel Windows PowerShell cmdlet again.

Event 1676: EVENT_LOCAL_NODE_QUARANTINED

Local cluster node has been quarantined by '%1'. The node will be quarantined until '%2' and then the node will automatically attempt to re-join the cluster.

Refer to the System and Application event logs to determine the issues on this node. When the issue is resolved, quarantine can be manually cleared to allow the node to rejoin with the 'Start-ClusterNode –ClearQuarantine' Windows PowerShell cmdlet.

QuarantineType : Quarantined by %1
Time quarantine will be automatically cleared: %2

Event 1677: EVENT_NODE_DRAIN_FAILED

Node drain failed on Cluster node %1.

Reference the node's System and Application event logs and cluster logs to investigate the cause of the drain failure. When the problem is resolved, you can retry the drain operation.

Event 1683: RES_NETNAME_COMPUTER_ACCOUNT_NO_DC

The cluster service was unable to reach any available domain controller on the domain. This may impact functionality that is dependent on Cluster network name authentication.

DC Server: %1

Guidance

Verify that domain controllers are accessible on the network to the cluster nodes.

Event 1684: RES_NETNAME_COMPUTER_OBJECT_VCO_NOT_FOUND

Cluster network name resource failed to find the associated computer object in Active Directory. This may impact functionality that is dependent on Cluster network name authentication.

Network Name: %1
Organizational Unit: %2

Guidance

Restore the computer object for the network name from the Active Directory recycle bin. Alternately, offline the cluster network name resource and run the Repair action to recreate the computer object in Active Directory.

Event 1685: RES_NETNAME_COMPUTER_OBJECT_CNO_NOT_FOUND

Cluster network name resource failed to find the associated computer object in Active Directory. This may impact functionality that is dependent on Cluster network name authentication.

Network Name: %1
Organizational Unit: %2

Guidance

Restore the computer object for the network name from the Active Directory recycle bin.

Event 1686: RES_NETNAME_COMPUTER_OBJECT_VCO_DISABLED

Cluster network name resource found the associated computer object in Active Directory to be disabled. This may impact functionality that is dependent on Cluster network name authentication.

Network Name: %1
Organizational Unit: %2

Guidance

Enable the computer object for the network name in Active Directory.

Event 1687: RES_NETNAME_COMPUTER_OBJECT_CNO_DISABLED

Cluster network name resource found the associated computer object in Active Directory to be disabled. This may impact functionality that is dependent on Cluster network name authentication.

Network Name: %1
Organizational Unit: %2

Guidance

Enable the computer object for the network name in Active Directory. Alternately, offline the cluster network name resource and run the Repair action to enable the computer object in Active Directory.

Event 1688: RES_NETNAME_COMPUTER_OBJECT_FAILED

Cluster network name resource detected that the associated computer object in Active Directory was disabled and failed in its attempt to enable it. This may impact functionality that is dependent on Cluster network name authentication.

Network Name: %1
Organizational Unit: %2

Guidance

Enable the computer object for the network name in Active Directory.

Event 4608: NODECLEANUP_GET_CLUSTERED_DISKS_FAILED

Cluster service failed to retrieve the list of clustered disks while destroying the cluster. The error code was '%1'. If these disks are not accessible, execute the 'Clear-ClusterDiskReservation' PowerShell cmdlet.

Event 4611: NODECLEANUP_RELEASE_CLUSTERED_DISKS_FROM_PARTMGR_FAILED

Clustered disk with ID '%2' was not released by the Partition Manager while destroying the cluster. The error code was '%1'. Restarting the machine will ensure the disk is released by the Partition Manager.

Event 4613: NODECLEANUP_CLEAR_CLUSDISK_DATABASE_FAILED

The cluster service failed to properly cleanup a clustered disk with ID '%2' while destroying the cluster. The error code was '%1'. You may unable to access this disk until cleanup has been successfully completed. For manual cleanup, delete the 'AttachedDisks' value of the 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ClusDisk\Parameters' key in the Windows registry.

Event 4615: NODECLEANUP_DISABLE_CLUSTER_SERVICE_FAILED

The cluster service has been stopped and set as disabled as part of cluster node cleanup.

Event 4616: NODECLEANUP_DISABLE_CLUSTER_SERVICE_TIMEOUT

Termination of the cluster service during cluster node cleanup has not completed within the expected time period. Please restart this machine to ensure the cluster service is no longer running.

Event 4618: NODECLEANUP_RESET_CLUSTER_REGISTRY_ENTRIES_FAILED

Resetting cluster service registry entries during cluster node cleanup failed. The error code was '%1'. You may be unable to create or join a cluster with this machine until cleanup has been successfully completed. For manual cleanup, execute the 'Clear-ClusterNode' PowerShell cmdlet on this machine.

Event 4620: NODECLEANUP_UNLOAD_CLUSTER_HIVE_FAILED

Unloading the cluster service registry hive during cluster node cleanup failed. The error code was '%1'. You may be unable to create or join a cluster with this machine until cleanup has been successfully completed. For manual cleanup, execute the 'Clear-ClusterNode' PowerShell cmdlet on this machine.

Event 4622: NODECLEANUP_ERRORS

The Cluster service encountered an error during node cleanup. You may be unable to create or join a cluster with this machine until cleanup has been successfully completed. Use the 'Clear-ClusterNode' PowerShell cmdlet on this node.

Event 4624: NODECLEANUP_RESET_NLBSFLAGS_FAILED

Resetting the IPSec security association timeout registry value failed during cluster node cleanup. The error code was '%1'. For manual cleanup, execute the 'Clear-ClusterNode' PowerShell cmdlet on this machine. Alternatively, you may reset the IPSec security association timeout by deleting the '%2' value and the '%3' value from HKEY_LOCAL_MACHINE in the Windows registry.

Event 4627: NODECLEANUP_DELETE_CLUSTER_TASKS_FAILED

Deletion of clustered tasks during node cleanup failed. The error code was '%1'. Use Windows Task Scheduler to delete any remaining clustered tasks.

Event 4629: NODECLEANUP_DELETE_LOCAL_ACCOUNT_FAILED

During node cleanup, the local user account that is managed by the cluster was not deleted. The error code was

'%1'. Open Local Users and Groups (lusrmgr.msc) to delete the account.

Event 4864: RES_VSSTASK_OPEN_FAILED

Volume shadow copy service task resource '%1' creation failed. The error code was '%2'.

Event 4865: RES_VSSTASK_TERMINATE_TASK_FAILED

Volume shadow copy service task resource '%1' failed. The error code was '%2'. This is because the associated task could not be stopped as part of an offline operation. You may need to stop it manually using the Task Scheduler snap-in.

Event 4866: RES_VSSTASK_DELETE_TASK_FAILED

Volume shadow copy service task resource '%1' failed. The error code was '%2'. This is because the associated task could not be deleted as part of an offline operation. You may need to delete it manually using the Task Scheduler snap-in.

Event 4867: RES_VSSTASK_ONLINE_FAILED

Volume shadow copy service task resource '%1' failed. The error code was '%2'. This is because the associated task could not be added as part of an online operation. Please use the Task Scheduler snap-in to ensure your tasks are properly configured.

Event 4868: UNABLE_TO_START_AUTOLOGGER

Cluster service failed to start the cluster log trace session. The error code was '%2'. The cluster will function properly, but supplemental logging information will be missing. Use the Performance Monitor snap-in to verify the event channel settings for '%1'.

Event 4869: NETFT_WATCHDOG_PROCESS_HUNG

User mode health monitoring has detected that the system is not being responsive. The Failover cluster virtual adapter has lost contact with the '%1' process with a process ID '%2', for '%3' seconds. Please use Performance Monitor to evaluate the health of the system and determine which process may be negatively impacting the system.

Event 4870: NETFT_WATCHDOG_PROCESS_TERMINATED

User mode health monitoring has detected that the system is not being responsive. The Failover cluster virtual adapter has lost contact with the '%1' process with a process ID '%2', for '%3' seconds. Recovery action will be taken.

Event 4871: NETFT_MINIPORT_INITIALIZATION_FAILURE

The cluster service failed to start. This was because the failover cluster virtual adapter failed to initialize the miniport adapter. The error code was '%1'. Verify that other network adapters are functioning properly and check the device manager for errors. If the configuration was changed, it may be necessary to reinstall the failover clustering feature on this computer.

Event 4872: NETFT_MISSING_DATALINK_ADDRESS

The failover cluster virtual adapter failed to generate a unique MAC address. Either it was unable to find a physical Ethernet adapter from which to generate a unique address or the generated address conflicts with another adapter on this machine. Please run the Validate a Configuration wizard to check your network configuration.

Event 5122: DCM_EVENT_ROOT_CREATION_FAILED

Cluster service failed to create the Cluster Shared Volumes root directory '%2'. The error message was '%1'.

Event 5142: DCM_VOLUME_NO_ACCESS

Cluster Shared Volume '%1' ('%2') is no longer accessible from this cluster node because of error '%3'. Please troubleshoot this node's connectivity to the storage device and network connectivity.

Event 5143: DCM_VETO_RESOURCE_MOVE_DUE_TO_CC

Move of the disk ('%2') is vetoed based on the current state of the Cache Manager on the node '%1' to prevent a potential deadlock. 'Cache Manager Dirty Pages Threshold' is %3, and 'Cache Manager Dirty Pages' is %4. Move is allowed if 'Cache Manager Dirty Pages' is less than 70% of 'Cache Manager Dirty Pages Threshold' or if 'Cache Manager Dirty Pages Threshold' minus 'Cache Manager Dirty Pages' is greater than 128000 pages (about 500MB if a page size is 4096 bytes). Cluster vetoed resource move to prevent potential deadlock due to Cache Manager throttling buffered writes while Cluster Shared Volumes on this disk are being paused.

Event 5144: DCM_SNAPSHOT_DIFF_AREA_FAILURE

While adding the disk ('%1') to Cluster Shared Volumes, setting explicit snapshot diff area association for volume ('%2') failed with error '%3'. The only supported software snapshot diff area association for Cluster Shared Volumes is to self.

Event 5145: DCM_SNAPSHOT_DIFF_AREA_DELETE_FAILURE

Cluster disk resource '%1' failed to delete a software snapshot. The diff area on volume '%3' could not be dissociated from volume '%2'. This may be caused by active snapshots. Cluster Shared Volumes requires that the software snapshot be located on the same disk.

Event 5146: DCM_VETO_RESOURCE_MOVE_DUE_TO_DISMOUNT

Move of the Cluster Shared Volume resource '%1' is vetoed because one of the volumes belonging to the resource is in dismounted state. Please retry the action after the dismount operation is completed.

Event 5147: DCM_VETO_RESOURCE_MOVE_DUE_TO_SNAPSHOT

Move of the Cluster Shared Volume resource '%1' is vetoed because one of the volumes belonging to the resource is in dismounted state. Please retry the action after the dismount operation is completed.

Event 5148: DCM_VETO_RESOURCE_MOVE_DUE_TO_IO_MODE_CHANGE

Move of the Cluster Shared Volume resource '%1' is vetoed because an IO mode change operation (Direct IO to Redirected IO or vice versa) is in progress on one of the volumes belonging to the resource. Please retry the action after the operation is completed.

Event 5150: DCM_SET_RESOURCE_IN_FAILED_STATE

Cluster physical disk resource '%1' failed. The Cluster Shared Volume was put in failed state with the following error: '%2'

Event 5200: CAM_CANNOT_CREATE_CNO_TOKEN

Cluster service failed to create a cluster identity token for Cluster Shared Volumes. The error code was '%1'. Ensure the domain controller is accessible and check for connectivity issues. Until connection to the domain controller is recovered, some operations on this node against the Cluster Shared Volumes might fail.

Event 5216: CSV_SW_SNAPSHOT_FAILED

Software snapshot creation on Cluster Shared Volume '%1' ('%2') failed with error %3. The resource must be online to support snapshot creation. Please check the state of the resource.

Event 5217: CSV_SW_SNAPSHOT_SET_FAILED

Software snapshot creation on Cluster Shared Volume(s) ('%1') with snapshot set id '%2' failed with error '%3'. Please check the state of the CSV resources and the system events of the resource owner nodes.

Event 5219: CSV_REGISTER_SNAPSHOT_PROV_WITH_VSS_FAILED

Cluster service failed to register the Cluster Shared Volumes snapshot provider with the Volume Shadow Service (VSS). This may be due to the VSS service shutting down or may be a problem with the VSS service having a problem that causes it to not accept incoming requests.
Error: %1

Event 5377: OPERATION_EXCEEDED_TIMEOUT

An internal Cluster service operation exceeded the defined threshold of '%2' seconds. The Cluster service has been terminated to recover. Service Control Manager will restart the Cluster service and the node will rejoin the cluster.

Event 5396: TWO_PARTITIONS_HAVE_QUORUM

The Cluster service on this node is shutting down because it has detected that there are other cluster nodes that have quorum. This occurs when the Cluster service detects another node that was started with the Force Quorum switch (/fq). The node which was started with the Force Quorum Switch will remain running. Use Failover Cluster Manager to verify that this node automatically joined the cluster when the cluster service restarted.

Event 5397: RLUA_ACCOUNT_FAILED

The cluster resource '%1' could not create or modify the replicated local user account '%2' on this node. Check the cluster logs for more information.

Event 5398: NM_EVENT_CLUSTER_FAILED_TO_FORM

Cluster failed to start. The latest copy of cluster configuration data was not available within the set of nodes attempting to start the cluster. Changes to the cluster occurred while the set of nodes were not in membership and as a result were not able to receive configuration data updates. .

Votes required to start cluster: %1
Votes available: %2
Nodes with votes: %3

Guidance

Attempt to start the cluster service on all nodes in the cluster so that nodes with the latest copy of the cluster configuration data can first form the cluster. The cluster will be able to start and the nodes will automatically obtain the updated cluster configuration data. If there are no nodes available with the latest copy of the cluster configuration data, run the 'Start-ClusterNode -FQ' Windows PowerShell cmdlet. Using the ForceQuorum (FQ) parameter will start the cluster service and mark this node's copy of the cluster configuration data to be authoritative. Forcing quorum on a node with an outdated copy of the cluster database may result in cluster configuration changes that occurred while the node was not participating in the cluster to be lost.

Warning events

Event 1011: NM_NODE_EVICTED

Cluster node %1 has been evicted from the failover cluster.

Event 1045: RES_IPADDR_IPV4_ADDRESS_CREATE_FAILED

No matching network interface found for resource '%1' IP address '%2' (return code was '%3'). If your cluster nodes span different subnets, this may be normal.

Event 1066: RES_DISK_CORRUPT_DISK

Cluster disk resource '%1' indicates corruption for volume '%2'. Chkdsk is being run to repair problems. The disk will be unavailable until Chkdsk completes. Chkdsk output will be logged to file '%3'.
Chkdsk may also write information to the Application Event Log.

Event 1068: RES_SMB_SHARE_CANT_ADD

Cluster file share resource '%1' cannot be brought online. Creation of file share '%2' (scoped to network name %3) failed due to error '%4'. This operation will be automatically retried.

Event 1071: RCM_RESOURCE_ONLINE_BLOCKED_BY_LOCKED_MODE

The operation attempted on cluster resource '%1' of type '%3' in clustered role '%2' could not be completed because the resource or one of its providers has locked status.

Event 1071: RCM_RESOURCE_OFFLINE_BLOCKED_BY_LOCKED_MODE

The operation attempted on cluster resource '%1' of type '%3' in clustered role '%2' could not be completed because the resource or one of its dependents has locked status.

Event 1094: SM_INVALID_SECURITY_LEVEL

The cluster common property SecurityLevel cannot be changed on this cluster. The cluster security level cannot be changed because the cluster is currently configured for no authentication mode.

Event 1119: RES_NETNAME_DNS_REGISTRATION_MISSING

Cluster network name resource '%1' failed to register DNS name '%2' over adapter '%4' for the following reason:

'%3'

Event 1125: TM_EVENT_CLUSTER_NETINTERFACE_UNREACHABLE

Cluster network interface '%1' for cluster node '%2' on network '%3' is unreachable by at least one other cluster node attached to the network. The failover cluster was not able to determine the location of the failure. Run the Validate a Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1149: RES_NETNAME_CANT_DELETE_DNS_RECORDS

The DNS Host (A) and Pointer (PTR) records associated with Cluster resource '%1' were not removed from the resource's associated DNS server. If necessary, they can be deleted manually. Contact your DNS administrator to assist with this effort.

Event 1150: RES_NETNAME_DNS_PTR_RECORD_DELETE_FAILED

The removal of the DNS Pointer (PTR) record '%2' for host '%3' which is associated with the cluster network name resource '%1' failed with error '%4'. If necessary, the record can be deleted manually. Contact your DNS administrator for assistance.

Event 1151: RES_NETNAME_DNS_A_RECORD_DELETE_FAILED

The removal of the DNS Host (A) record '%2' associated with the cluster network name resource '%1' failed with error '%3'. If necessary, the record can be deleted manually. Contact your DNS administrator for assistance.

Event 1155: RCM_EVENT_EXITED_QUEUING

The pending move for the role '%1' did not complete.

Event 1197: RES_NETNAME_DELETE_DISABLE_FAILED

Cluster network name resource '%1' failed to delete or disable its associated computer object '%2' during resource deletion. The error code was '%3'.
Please check if the site is Read-Only. Ensure that the cluster name object has the appropriate permissions on the '%2' object in Active Directory.

Event 1198: RES_NETNAME_DELETE_VCO_GUID_FAILED

Cluster network name resource '%1' failed to delete computer object with guid '%2'. The error code was '%3'. Please check if the site is Read-Only. Ensure that the cluster name object has the appropriate permissions on the '%2' object in Active Directory.

Event 1216: SERVICE_NETNAME_CHANGE_WARNING

A name change operation on the cluster core netname resource has failed. Attempting to revert the name change operation back to the original name has also failed. The error code was '%1'. You may not be able to remotely manage the cluster using the cluster name until this situation has been manually corrected.

Event 1221: RES_NETNAME_RENAME_OUT_OF_SYNCH_WITH_COMPOBJ

Cluster network name resource '%1' has a name '%2' which does not match the corresponding computer object name '%3'. It is likely that a previous name change of the computer object has not replicated to all domain controllers in the domain. You will be unable to rename the network name resource until the names become consistent. If the computer object has not been recently changed, please contact your domain administrator to rename the computer object and thereby make it consistent. Also, ensure that replication across domain controllers has been successfully completed.

Event 1222: RES_NETNAME_SET_PERMISSIONS_FAILED

The computer object associated with cluster network name resource '%1' could not be updated.

The text for the associated error code is: %2

The cluster identity '%3' may lack permissions required to update the object. Please work with your domain administrator to ensure that the cluster identity can update computer objects in the domain.

Event 1240: RES_IPADDR_OBTAIN_LEASE_FAILED

Cluster IP address resource '%1' failed to obtain a leased IP address.

Event 1243: RES_IPADDR_RELEASE_LEASE_FAILED

Cluster IP address resource '%1' failed to release the lease for IP address '%2'.

Event 1251: RCM_GROUP_PREEMPTED

Clustered role '%2' was taken offline. This role was preempted by the higher priority clustered role '%1'. The cluster service will attempt to bring clustered role '%2' online later when system resources are available.

Event 1544: SERVICE_VSS_ONABORT

The backup operation for the cluster configuration data has been canceled. The cluster Volume Shadow Copy Service (VSS) writer received an abort request.

Event 1548: SERVICE_CONNECT_VERSION_COMPATIBLE

Node '%1' established communication with node '%2' and detected that it is running a different, but compatible, version of the operating system. We recommend that all nodes run the same version of the operating system. After all nodes have been upgraded, run the Update-ClusterFunctionalLevel Windows PowerShell cmdlet to complete upgrading the cluster.

Event 1550: SERVICE_CONNECT_NOVERCHECK

Node '%1' established a communication session with node '%2' without performing a version compatibility check because version compatibility checking is disabled. Disabling version compatibility checking is not supported.

Event 1551: SERVICE_FORM_NOVERCHECK

Node '%1' formed a failover cluster without performing a version compatibility check because version compatibility checking is disabled. Disabling version compatibility checking is not supported.

Event 1555: SERVICE_NETFT_DISABLE_AUTOCONFIG_FAILED

Attempting to use IPv4 for '%1' network adapter failed. This was due to a failure to disable IPv4 auto-configuration and DHCP. This may be expected if the DHCP Client service is already disabled. IPv6 will be used if enabled, otherwise this node may not be able to participate in a failover cluster.

Event 1558: SERVICE_WITNESS_FAILOVER_ATTEMPT

The cluster service detected a problem with the witness resource. The witness resource will be failed over to another node within the cluster in an attempt to reestablish access to cluster configuration data.

Event 1562: RES_FSW_ALIVEFAILURE

File share witness resource '%1' failed a periodic health check on file share '%2'. Please ensure that file share

'%2' exists and is accessible by the cluster.

Event 1576: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_REFUSED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4' in a secure DNS zone. This was due to an existing record with this name and the cluster identity does not have the sufficient privileges to update that record. The error code was '%3'. Please contact your DNS server administrator to verify the cluster identity has permissions on DNS record '%2'.

Event 1576: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_REFUSED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4' in a secure DNS zone. This was due to an existing record with this name and the cluster identity does not have the sufficient privileges to update that record. The error code was '%3'. Please contact your DNS server administrator to verify the cluster identity has permissions on DNS record '%2'.

Event 1577: RES_NETNAME_DNS_SERVER_COULD_NOT_BE_CONTACTED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4'. The DNS server could not be contacted. The error code was '%3.' Ensure that a DNS server is accessible from this cluster node. The DNS registration will be retried later.

Event 1577: RES_NETNAME_DNS_SERVER_COULD_NOT_BE_CONTACTED

Cluster network name resource '%1' failed to register the name '%2' over adapter '%4'. The DNS server could not be contacted. The error code was '%3.' Ensure that a DNS server is accessible from this cluster node. The DNS registration will be retried later.

Event 1578: RES_NETNAME_DNS_TEST_FOR_DYNAMIC_UPDATE_FAILED

Cluster network name resource '%1' failed to register dynamic updates for name '%2' over adapter '%4'. The DNS server may not be configured to accept dynamic updates. The error code was '%3'. Please contact your DNS server administrator to verify that the DNS server is available and configured for dynamic updates.

Alternatively, you can disable dynamic DNS updates by unchecking the 'Register this connection's addresses in DNS' setting in the advanced TCP/IP settings for adapter '%4' under the DNS tab.

Event 1578: RES_NETNAME_DNS_TEST_FOR_DYNAMIC_UPDATE_FAILED

Cluster network name resource '%1' failed to register dynamic updates for name '%2' over adapter '%4'. The DNS server may not be configured to accept dynamic updates. The error code was '%3'. Please contact your DNS server administrator to verify that the DNS server is available and configured for dynamic updates.

Alternatively, you can disable dynamic DNS updates by unchecking the 'Register this connection's addresses in DNS' setting in the advanced TCP/IP settings for adapter '%4' under the DNS tab.

Event 1579: RES_NETNAME_DNS_RECORD_UPDATE_FAILED

Cluster network name resource '%1' failed to update the DNS record for name '%2' over adapter '%4'. The error code was '%3'. Ensure that a DNS server is accessible from this cluster node and contact your DNS server administrator to verify the cluster identity can update the DNS record '%2'.

Event 1579: RES_NETNAME_DNS_RECORD_UPDATE_FAILED

Cluster network name resource '%1' failed to update the DNS record for name '%2' over adapter '%4'. The error code was '%3'. Ensure that a DNS server is accessible from this cluster node and contact your DNS server administrator to verify the cluster identity can update the DNS record '%2'.

Event 1581: CLUSSVC_UNABLE_TO_MOVE_HIVE_TO_SAFE_FILE

The restore request for the cluster configuration data failed to make a copy of the existing cluster configuration data file (ClusDB). While attempting to preserve the existing configuration, the restore operation was unable to create a copy at location '%1'. This might be expected if the existing configuration data file was corrupt. The

restore operation has continued but attempts to revert to the existing cluster configuration may not be possible.

Event 1582: CLUSSVC_UNABLE_TO_MOVE_RESTORED_HIVE_TO_CURRENT

Cluster Service failed to move the restored cluster hive at '%1' to '%2'. This may prevent the restore operation from succeeding successfully. If the cluster configuration was not properly restored, please retry the restore action.

Event 1583: CLUSSVC_NETFT_DISABLE_CONNECTIONSECURITY_FAILED

Cluster service failed to disable Internet Protocol security (IPsec) on the Failover cluster virtual adapter '%1'. This could have a negative impact on cluster communication performance. If this problem persists, please verify your local and domain connection security policies applying to IPSec and the Windows Firewall. Additionally, please check for events related to the Base Filtering Engine service.

Event 1584: SHARED_VOLUME_NOT_READY_FOR_SNAPSHOT

A backup application initiated a VSS snapshot on Cluster Shared Volume '%1' ('%3') without properly preparing the volume for snapshot. This snapshot may be invalid and the backup may not be usable for restore operations. Please contact your backup application vendor to verify compatibility with Cluster Shared Volumes.

Event 1589: RES_NETNAME_DNS_RETURNING_IP_THAT_IS_NOT_PROVIDER

Cluster network name resource '%1' found one or more IP addresses associated with DNS name '%2' that are not dependent IP address resources. The additional addresses found were '%3'. This may affect client connectivity until the network name and its associated DNS records are consistent. Please contact your DNS server administrator to verify the records associated with name '%2'.

Event 1604: RES_DISK_CHKDSK_SPOTFIX_NEEDED

Cluster disk resource '%1' detected corruption for volume '%2'. Spotfix Chkdsk is required to repair problems.

Event 1605: RES_DISK_SPOTFIX_PERFORMED

Cluster disk resource '%1' completed running ChkDsk.exe /spotfix on volume '%2'. The return code was '%4'. Output from the ChkDsk has been logged to file '%3'.
Check the application event log for additional information from ChkDsk.

Event 1671: RES_DISK_ONLINE_SET_ATTRIBUTES_COMPLETED_FAILURE

Cluster physical disk resource cannot be brought online.

Physical Disk resource name: %1
Error Code: %2
Time Elapsed (seconds): %3

Guidance

Run the Validate a Configuration wizard to check your storage configuration. If the error code was ERROR_CLUSTER_SHUTDOWN then the Online Pending state was canceled by an administrator. If this is a replicated volume then this could be the result of a failure to set the disk attributes. Review the Storage Replication events for additional information.

Event 1673: CLUSTER_NODE_ENTERED_ISOLATED_STATE

Cluster node '%1' has entered the isolated state.

Event 1675: EVENT_JOINING_NODE_QUARANTINED

Cluster node '%1' has been quarantined by '%2' and cannot join the cluster. The node will be quarantined until '%3' and then the node will automatically attempt to re-join the cluster.

Refer to the System and Application event logs to determine the issues on this node. When the issue is resolved, quarantine can be manually cleared to allow the node to rejoin with the 'Start-ClusterNode –ClearQuarantine' Windows PowerShell cmdlet.

Node Name : %1
QuarantineType : Quarantine by %2
Time quarantine will be automatically cleared: %3

Event 1681: CLUSTER_GROUPS_UNMONITORED_ON_NODE

Virtual machines on node '%1' have entered an unmonitored state. The virtual machines health will be monitored again once the node returns from an isolated state or may failover if the node does not return. The virtual machine no longer being monitored are: %2.

Event 1689: EVENT_DISABLE_AND_STOP_OTHER_SERVICE

The cluster service detected a service which is not compatible with Failover Clustering. The service has been disabled to avoid possible problems with the Failover Cluster.

Service name: '%1'

Event 4625: NODECLEANUP_RESET_NLBSFLAGS_PRESERVED

Resetting the IPSec security association timeout registry value failed during cluster node cleanup. This is because the IPSec security association timeout was modified after this machine was configured to be a member of a cluster. For manual cleanup, execute the 'Clear-ClusterNode' PowerShell cmdlet on this machine. Alternatively, you may reset the IPSec security association timeout by deleting the '%1' value and the '%2' value from HKEY_LOCAL_MACHINE in the Windows registry.

Event 4873: NETFT_CLUSSVC_TERMINATE_BECAUSE_OF_WATCHDOG

The cluster service has detected that the failover cluster virtual adapter has stopped. This is expected when hot replace CPU is performed on this node. Cluster service will stop and should automatically restart after the operation is complete. Please check for additional events associated with the service and ensure that the cluster service has been restarted on this node.

Event 5120: DCM_VOLUME_AUTO_PAUSE_AFTER_FAILURE

Cluster Shared Volume '%1' ('%2') has entered a paused state because of '%3'. All I/O will temporarily be queued until a path to the volume is reestablished.

Event 5123: DCM_EVENT_ROOT_RENAME_SUCCESS

Cluster Shared Volumes root directory '%1' already exists. The directory '%1' was renamed to '%2'. Please verify that applications accessing data in this location have been updated as necessary.

Event 5124: DCM_UNSAFE_FILTERS_FOUND

Cluster Shared Volume '%1' ('%3') has identified one or more active filter drivers on this device stack that could interfere with CSV operations. I/O access will be redirected to the storage device over the network through another Cluster node. This may result in degraded performance. Please contact the filter driver vendor to verify interoperability with Cluster Shared Volumes.

Active filter drivers found:
%2

Event 5125: DCM_UNSAFE_VOLFILTER_FOUND

Cluster Shared Volume '%1' ('%3') has identified one or more active volume drivers on this device stack that could interfere with CSV operations. I/O access will be redirected to the storage device over the network through another Cluster node. This may result in degraded performance. Please contact the volume driver vendor to verify interoperability with Cluster Shared Volumes.

Active volume drivers found:
%2

Event 5126: DCM_EVENT_CANNOT_DISABLE_SHORT_NAMES

Physical disk resource '%1' does not allow disabling short name generation. This may cause application compatibility issues. Please use 'fsutil 8dot3name set 2' to allow disabling short name generation and then offline/online the resource.

Event 5128: DCM_EVENT_CANNOT_DISABLE_SHORT_NAMES

Physical disk resource '%1' does not allow disabling short name generation. This may cause application compatibility issues. Please use 'fsutil 8dot3name set 2' to allow disabling short name generation and then offline/online the resource.

Event 5133: DCM_CANNOT_RESTORE_DRIVE_LETTERS

Cluster Disk '%1' has been removed and placed back in the 'Available Storage' cluster group. During this process an attempt to restore the original drive letter(s) has taken longer than expected, possibly due to those drive letters being already in use.

Event 5134: DCM_CANNOT_SET_ACL_ON_ROOT

Cluster service failed to set the permissions (ACL) on the Cluster Shared Volumes root directory '%1'. The error was '%2'.

Event 5135: DCM_CANNOT_SET_ACL_ON_VOLUME_FOLDER

Cluster service failed to set the permissions on the Cluster Shared Volume directory '%1' ('%2'). The error was '%3'.

Event 5136: DCM_CSV_INTO_REDIRECTED_MODE

Cluster Shared Volume '%1' ('%2') redirected access was turned on. Access to the storage device will be redirected over the network from all cluster nodes that are accessing this volume. This may result in degraded performance. Turn off redirected access for this volume to resume normal operations.

Event 5149: DCM_CSV_BLOCK_CACHE_RESIZED

Cache size resized to '%1' based on populated memory, user setsize is too high.

Event 5156: DCM_VOLUME_AUTO_PAUSE_AFTER_SNAPSHOT_FAILURE

Cluster Shared Volume '%1' ('%2') has entered a paused state because of '%3'. This error is encountered when the volsnap snapshots underlying the CSV volume are deleted outside of a user request. Possible causes of the snapshots getting deleted are lack of space in the volume for the snapshots to grow, or IO failure while trying to update the snapshot data. All I/O will temporarily be queued until the snapshot state is synchronized with volsnap.

Event 5157: DCM_VOLUME_AUTO_PAUSE_AFTER_FAILURE_EXPECTED

Cluster Shared Volume '%1' ('%2') has entered a paused state because of '%3'. All I/O will temporarily be queued until a path to the volume is reestablished. This error is usually caused by an infrastructure failure. For example, losing connectivity to storage or the node owning the Cluster Shared Volume being removed from active cluster membership.

Event 5394: POOL_ONLINE_WARNINGS

The Cluster service encountered some storage errors while trying to bring storage pool online. Run cluster storage validation to troubleshoot the issue.

Event 5395: RCM_GROUP_AUTO_MOVE_STORAGE_POOL

Cluster is moving the group for storage pool '%1' because current node '%3' does not have optimal connectivity to the storage pool physical disks.

Informational events

Event 1592: CLUSSVC_TCP_RECONNECT_CONNECTION_REESTABLISHED

Cluster node '%1' lost communication with cluster node '%2'. Network communication was reestablished. This could be due to communication temporarily being blocked by a firewall or connection security policy update. If the problem persists and network communication are not reestablished, the cluster service on one or more nodes will stop. If that happens, run the Validate a Configuration wizard to check your network configuration. Additionally, check for hardware or software errors related to the network adapters on this node, and check for failures in any other network components to which the node is connected such as hubs, switches, or bridges.

Event 1594: CLUSTER_FUNCTIONAL_LEVEL_UPGRADE_COMPLETE

Cluster service successfully upgraded the cluster functional level.

Functional Level: %1
Upgrade Version: %2

Event 1635: RCM_RESOURCE_FAILURE_INFO_WITH_TYPENAME

Cluster resource '%1' of type '%3' in clustered role '%2' failed.

Event 1636: CLUSSVC_PASSWORD_CHANGED

The Cluster service has changed the password of account '%1' on node '%2'.

Event 1680: CLUSTER_NODE_EXITED_ISOLATED_STATE

Cluster node '%1' has exited the isolated state.

Event 1682: CLUSTER_GROUP_MOVED_NO_LONGER_UNMONITORED

Virtual machine '%2' which was unmonitored on the isolated node '%1' has been failed over to another node. The health of the virtual machine is once again being monitored.

Event 1682: CLUSTER_MULTIPLE_GROUPS_NO_LONGER_UNMONITORED

Node '%1' has rejoined the cluster and the following virtual machines running on that node are once again having their health state monitored: %2.

Event 4621: NODECLEANUP_SUCCESS

This node was successfully removed from the cluster.

Event 5121: DCM_VOLUME_NO_DIRECT_IO_DUE_TO_FAILURE

Cluster Shared Volume '%1' ('%2') is no longer directly accessible from this cluster node. I/O access will be redirected to the storage device over the network to the node that owns the volume. If this results in degraded performance, please troubleshoot this node's connectivity to the storage device and I/O will resume to a healthy state once connectivity to the storage device is reestablished.

Event 5218: CSV_OLD_SW_SNAPSHOT_DELETED

Cluster physical disk resource '%1' deleted a software snapshot. The software snapshot on Cluster Shared Volume '%2' was deleted because it was older than '%3' day(s). The snapshot ID was '%4' and it was created from node '%5' at '%6'. It is expected that snapshots are deleted by a backup application after a backup job is completed. This snapshot exceeded the time that is expected for a snapshot to exist. Verify with the backup application that backup jobs are completing successfully.

Additional References

- Detailed event info for Failover Clustering components in Windows Server 2008

Use BitLocker with Cluster Shared Volumes (CSV)

12/9/2022 • 14 minutes to read • Edit Online

Applies to: Windows Server 2022, Azure Stack HCI, version 20H2

BitLocker overview

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inadequately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer hasn't been tampered with while the system was offline.

On computers that don't have a TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the volume on a computer without TPM. Neither option provides the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker gives you the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device. This device could be a USB flash drive, that contains a startup key. These additional security measures provide multi-factor authentication and assurance that the computer won't start or resume from hibernation until the correct PIN or startup key is presented.

Cluster Shared Volumes overview

Cluster Shared Volumes (CSV) enable multiple nodes in a Windows Server failover cluster or Azure Stack HCI to simultaneously have read-write access to the same logical unit number (LUN), or disk, that is provisioned as an NTFS volume. The disk can be provisioned as Resilient File System (ReFS). However, the CSV drive will be in redirected mode which means write access will be sent to the coordinator node. With CSV, clustered roles can fail over quickly from one node to another without requiring a change in drive ownership, or dismounting and remounting a volume. CSV also help simplify the management of a potentially large number of LUNs in a failover cluster.

CSV provides a general-purpose, clustered file system that is layered above NTFS or ReFS. CSV applications include:

- Clustered virtual hard disk (VHD/VHDX) files for clustered Hyper-V virtual machines
- Scale out file shares to store application data for the Scale-Out File Server clustered role. Examples of the application data for this role include Hyper-V virtual machine files and Microsoft SQL Server data. ReFS is not supported for a Scale-Out File Server in Windows Server 2012 R2 and below. For more information about Scale-Out File Server, see Scale-Out File Server for Application Data.
- Microsoft SQL Server 2014 (or higher) Failover Cluster Instance (FCI) Microsoft SQL Server clustered workload in SQL Server 2012 and earlier versions of SQL Server don't support the use of CSV.
- Windows Server 2019 or higher Microsoft Distributed Transaction Control (MSDTC)

Use BitLocker with Cluster Shared Volumes

BitLocker on volumes within a cluster are managed based on how the cluster service "views" the volume to be

protected. The volume can be a physical disk resource such as a logical unit number (LUN) on a storage area network (SAN) or network attached storage (NAS).

Alternatively, the volume can be a Cluster Shared Volume (CSV) within the cluster. When using BitLocker with volumes designated for a cluster, the volume can be enabled with BitLocker before its addition to the cluster or when in the cluster. Put the resource into maintenance mode before enabling BitLocker.

Windows PowerShell or the Manage-BDE command-line interface is the preferred method to manage BitLocker on CSV volumes. This method is recommended over the BitLocker Control Panel item because CSV volumes are mount points. Mount points are an NTFS object that is used to provide an entry point to other volumes. Mount points don't require the use of a drive letter. Volumes that lack drive letters don't appear in the BitLocker Control Panel item.

BitLocker will unlock protected volumes without user intervention by attempting protectors in the following order:

1. Clear Key
2. Driver-based auto-unlock key
3. **ADAccountOrGroup** protector
    a. Service context protector
    b. User protector
4. Registry-based auto-unlock key

Failover Cluster requires the Active Directory-based protector option for cluster disk resource. Otherwise, CSV resources are not available in the Control Panel item.

An Active Directory Domain Services (AD DS) protector for protecting clustered volumes held within your AD DS infrastructure. The **ADAccountOrGroup** protector is a domain security identifier (SID)-based protector that can be bound to a user account, machine account, or group. When an unlock request is made for a protected volume, the BitLocker service interrupts the request and uses the BitLocker protect/unprotect APIs to unlock or deny the request.

New functionality

In previous versions of Windows Server and Azure Stack HCI, the only supported encryption protector is the SID-based protector where the account being used is Cluster Name Object (CNO) that is created in Active Directory as part of the Failover Clustering creation. This is a secure design because the protector is stored in Active Directory and protected by the CNO password. Also, it makes provisioning and unlocking volumes easy because every Failover Cluster node has access to the CNO account.

The downside is three-fold:

1. This method obviously does not work when a Failover Cluster is created without any access to an Active Directory controller in the datacenter.
2. Volume unlock, as part of failover, may take too long (and possibly time out) if the Active Directory controller is unresponsive or slow.
3. The online process of the drive will fail if an Active Directory controller is not available.

New functionality has been added that Failover Clustering will generate and maintain its own BitLocker Key protector for a volume. It will be encrypted and saved in the local cluster database. Since the cluster database is a replicated store backed by the system volume on every cluster node, the system volume on every cluster node should be BitLocker protected as well. Failover Clustering will not enforce it as some solutions may not want or

need to encrypt the system volume. If the system drive is not Bitlockered, Failover Cluster will flag this as a warning event during the online and unlock process. Failover Cluster validation will log a message if it detects that this is an Active Directory-less or workgroup setup and the system volume is not encrypted.

Installing BitLocker encryption

BitLocker is a feature that must be added to all nodes of the Cluster.

Adding BitLocker using Server Manager

1. Open **Server Manager** by selecting the Server Manager icon or running servermanager.exe.
2. Select **Manage** from the Server Manager Navigation bar and select **Add Roles and Features** to start the **Add Roles and Features Wizard**.
3. With the **Add Roles and Features Wizard** open, select **Next** at the **Before you begin** pane (if shown).
4. Select **Role-based or feature-based installation** on the **Installation type** pane of the **Add Roles and Features Wizard** pane and select **Next** to continue.
5. Select the **Select a server from the server pool** option in the **Server Selection** pane and confirm the server for the BitLocker feature install.
6. Select **Next** on the **Server Roles** pane of the **Add Roles and Features** wizard to proceed to the **Features** pane.
7. Select the check box next to **BitLocker Drive Encryption** within the **Features** pane of the **Add Roles and Features** wizard. The wizard will show the additional management features available for BitLocker. If you don't want to install these features, deselect the **Include management tools** option and select **Add Features**. Once optional features selection is complete, select **Next** to continue.

> **NOTE**
> The **Enhanced Storage** feature is a required feature for enabling BitLocker. This feature enables support for Encrypted Hard Drives on capable systems.

1. Select **Install** on the **Confirmation** pane of the **Add Roles and Features Wizard** to begin BitLocker feature installation. The BitLocker feature requires a restart to complete. Selecting the **Restart the destination server automatically if required** option in the **Confirmation** pane will force a restart of the computer after installation is complete.
2. If the **Restart the destination server automatically if required** check box is not selected, the **Results** pane of the **Add Roles and Features Wizard** will display the success or failure of the BitLocker feature installation. If required, a notification of additional action necessary to complete the feature installation, such as the restart of the computer, will be displayed in the results text.

Add BitLocker using PowerShell

Use the following command for each server:

```
Install-WindowsFeature -ComputerName "Node1" -Name "BitLocker" -IncludeAllSubFeature -IncludeManagementTools
```

To run the command on all cluster servers at the same time, use the following script, modifying the list of variables at the beginning to fit your environment:

Fill in these variables with your values.

```
$ServerList = "Node1", "Node2", "Node3", "Node4"
$FeatureList = "BitLocker"
```

This part runs the Install-WindowsFeature cmdlet on all servers in $ServerList, passing the list of features in $FeatureList.

```
Invoke-Command ($ServerList) {
    Install-WindowsFeature -Name $Using:Featurelist -IncludeAllSubFeature -IncludeManagementTools
}
```

Next, restart all the servers:

```
$ServerList = "Node1", "Node2", "Node3", "Node4" Restart-Computer -ComputerName $ServerList -
WSManAuthentication Kerberos
```

Multiple roles and features can be added at the same time. For example, to add BitLocker, Failover Clustering, and the File Server role, the $FeatureList would include all needed separated by a comma. For example:

```
$ServerList = "Node1", "Node2", "Node3", "Node4"
$FeatureList = "BitLocker", “Failover-Clustering”, “FS-FileServer”
```

Provision an encrypted volume

Provisioning a drive with BitLocker encryption can be done either when then drive is a part of the Failover Cluster or outside before adding it. To create the External Key Protector automatically, the drive must be a resource in the Failover Cluster before enabling BitLocker. If BitLocker is enabled before adding the drive to the Failover Cluster, additional manual steps to create the External Key Protector must be accomplished.

Provisioning encrypted volumes will require PowerShell commands run with administrative privileges. There are two options to encrypt the drives and have Failover Clustering be able to create and use its own BitLocker keys.

1. Internal recovery key
2. External recovery key file

Encrypt using a recovery key

Encrypting the drives using a recovery key will allow a BitLocker recovery key to be created and added into the Cluster database. As the drive is coming online, it only needs to consult the local cluster hive for the recovery key.

Move the disk resource to the node where BitLocker encryption will be enabled:

```
Get-ClusterSharedVolume -Name "Cluster Disk 1" | Move-ClusterSharedVolume Resource -Node Node1
```

Put the disk resource into Maintenance Mode:

```
Get-ClusterSharedVolume -Name "Cluster Disk 1" | Suspend-ClusterResource
```

A dialog box will pop up that says:

```
Suspend-ClusterResource

Are you sure that you want to turn on maintenance for Cluster Shared Volume ‘Cluster Disk 1’? Turning on
maintenance will stop all clustered roles that use this volume and will interrupt client access.
```

To continue, press **Yes**.

To enable BitLocker encryption, run:

```
Enable-BitLocker -MountPoint "C:\\ClusterStorage\\Volume1" -RecoveryPasswordProtector
```

Once entering the command, a warning will show that provides a numeric recovery password. Save the password in a secure location as it will also be needed in an upcoming step. The warning will look similar to this:

```


WARNING: ACTIONS REQUIRED:

    1. Save this numerical recovery password in a secure location away from your computer:

        271733-258533-688985-480293-713394-034012-061963-682044

    To prevent data loss, save this password immediately. This password helps ensure that you can unlock the
encrypted volume.


```

To get the BitLocker protector information for the volume, the following command can be run:

```
(Get-BitlockerVolume -MountPoint "C:\\ClusterStorage\\Volume1").KeyProtector
```

This will display both the key protector ID and the recovery password string.

```
KeyProtectorId : {26935AC3-8B17-482D-BA3F-D373C7954D29}
AutoUnlockProtector :
KeyProtectorType : RecoveryPassword
KeyFileName :
RecoveryPassword : 271733-258533-688985-480293-713394-034012-061963-682044
KeyCertificateType :
Thumbprint :
```

The key protector ID and recovery password will be needed and saved into a new physical disk private property called **BitLockerProtectorInfo**. This new property will be used when the resource comes out of Maintenance Mode. The format of the protector will be a string where the protector ID and the password are separated by a ":".

```
Get-ClusterSharedVolume "Cluster Disk 1" | Set-ClusterParameter -Name BitLockerProtectorInfo -Value "
{26935AC3-8B17-482D-BA3F-D373C7954D29}:271733-258533-688985-480293-713394-034012-061963-682044" -Create
```

To verify that the **BitlockerProtectorInfo** key and value are set, run the command:

```
Get-ClusterSharedVolume "Cluster Disk 1" | Get-ClusterParameter BitLockerProtectorInfo
```

Now that the information is present, the disk can be brought out of maintenance mode once the encryption process is completed.

```
Get-ClusterSharedVolume -Name "Cluster Disk 1" | Resume-ClusterResource
```

If the resource fails to come online, it could be a storage issue, an incorrect recovery password, or some issue. Verify the **BitlockerProtectorInfo** key has the proper information. If it does not, the commands previously given should be run again. If the problem is not with this key, we recommended getting with the proper group within your organization or the storage vendor to resolve the issue.

If the resource comes online, the information is correct. During the process of coming out of maintenance mode, the **BitlockerProtectorInfo** key is removed and encrypted under the resource in the cluster database.

Encrypting using External Recovery Key file

Encrypting the drives using a recovery key file will allow a BitLocker recovery key to be created and accessed from a location that all nodes have access to, such as a file server. As the drive is coming online, the owning node will connect to the recovery key.

Move the disk resource to the node where BitLocker encryption will be enabled:

```
Get-ClusterSharedVolume -Name "Cluster Disk 2" | Move-ClusterSharedVolume Resource -Node Node2
```

Put the disk resource into Maintenance Mode:

```
Get-ClusterSharedVolume -Name "Cluster Disk 2" | Suspend-ClusterResource
```

A dialog box will pop up

```
Suspend-ClusterResource

Are you sure that you want to turn on maintenance for Cluster Shared Volume ‘Cluster Disk 2’? Turning on
maintenance will stop all clustered roles that use this volume and will interrupt client access.
```

To continue, press **Yes**.

To enable BitLocker encryption and create the key protector file locally, run the following command. Creating the file locally first and then move it to a location accessible to all nodes is recommended.

```
Enable-BitLocker -MountPoint "C:\ClusterStorage\Volume2" -RecoveryKeyProtector -RecoveryKeyPath
C:\Windows\Cluster
```

To get the BitLocker protector information for the volume, the following command can be run:

```
(Get-BitlockerVolume -MountPoint "C:\ClusterStorage\Volume2").KeyProtector
```

This will display both the key protector ID and the key filename it creates.

```
KeyProtectorId : {F03EB4C1-073C-4E41-B43E-B9298B6B27EC}
AutoUnlockProtector :
KeyProtectorType : ExternalKey
KeyFileName : F03EB4C1-073C-4E41-B43E-B9298B6B27EC.BEK
RecoveryPassword :
KeyCertificateType :
Thumbprint :
```

When going to the folder that was specified creating it in, you will not see it at first glance. The reasoning is that

it will be created as a hidden file. For example:

```
C:\Windows\Cluster\>dir f03

Directory of C:\\Windows\\Cluster

File Not Found

C:\Windows\Cluster\>dir /a f03

Directory of C:\Windows\Cluster

<Date> <Time> 148 F03EB4C1-073C-4E41-B43E-B9298B6B27EC.BEK

C:\Windows\Cluster\>attrib f03

A SHR C:\Windows\Cluster\F03EB4C1-073C-4E41-B43E-B9298B6B27EC.BEK
```

Since this is created on a local path, it must be copied over to a network path so that all nodes will have access to it using the **Copy-Item** command.

```
Copy-Item -Path C:\Windows\Cluster\F03EB4C1-073C-4E41-B43E-B9298B6B27EC.BEK -Destination \\Server\Share\Dir
```

Since the drive will be using a file and is located on a network share, bring the drive out of maintenance mode specifying the path to the file. Once the drive has completed with encryption, the command to resume it would be:

```
Resume-ClusterPhysicalDiskResource -Name "Cluster Disk 2" -RecoveryKeyPath \\Server\Share\Dir\F03EB4C1-073C-
4E41-B43E-B9298B6B27EC.BEK
```

Once the drive has been provisioned, the *.BEK file can be removed from share and is no longer needed.

New PowerShell cmdlets

With this new feature, two new cmdlets have been created to bring the resource online or resuming the resource manually using the recovery key or the recovery key file.

Start-ClusterPhysicalDiskResource

Example 1

```
    Start-ClusterPhysicalDiskResource -Name "My Disk" -RecoveryPassword "password-string"
```

Example 2

```
    Start-ClusterPhysicalDiskResource -Name "My Disk" -RecoveryKeyPath "path-to-external-key-file"
```

Resume-ClusterPhysicalDiskResource

Example 1

```
    Resume-ClusterPhysicalDiskResource -Name "My Disk" -RecoveryPassword "password-string"
```

Example 2

```
Resume-ClusterPhysicalDiskResource -Name "My Disk" -RecoveryKeyPath "path-to-external-key-file"
```

New events

There are several new events that have been added that are in the Microsoft-Windows-FailoverClustering/Operational event channel.

When it is successful in creating the key protector or key protector file, the event shown would be similar to:

```
Source: Microsoft-Windows-FailoverClustering Event ID: 1810 Task Category: Physical Disk Resource Level:
Information Description: Cluster Physical Disk Resource added a protector to a BitLocker encrypted volume.
```

If there is a failure in creating the key protector or key protector file, the event shown would be similar to:

```
Source: Microsoft-Windows-FailoverClustering Event ID: 1811 Task Category: Physical Disk Resource Level:
Information Description: Cluster Physical Disk Resource failed to create an external key protector for the
volume
```

As mentioned previously, since the cluster database is a replicated store backed by the system volume on every cluster node, it is recommended the system volume on every cluster node should also be BitLocker protected. Failover Clustering will not enforce it as some solutions may not want or need to encrypt the system volume. If the system drive is not secured by BitLocker, Failover Cluster will flag this as an event during the unlock/online process. The event shown would be similar to:

```
Source: Microsoft-Windows-FailoverClustering Event ID: 1824 Task Category: Physical Disk Resource Level:
Warning Description: Cluster Physical Disk Resource contains a BitLocker protected volume, but the system
volume is not BitLocker protected. For data protection, it is recommended that the system volume be BitLocker
protected as well. ResourceName: Cluster Disk 1
```

Failover Cluster validation will log a message if it detects that this is an Active Directory-less or workgroup setup and the system volume is not encrypted.

Change history for Failover Clustering topics

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic lists new and updated topics in the Failover Clustering documentation for Windows Server.

> If you're looking for update history for Windows Server 2016, see Windows 10 and Windows Server 2016 update history.

January 2020

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster events	New

March 2019

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster affinity	New

February 2019

NEW OR CHANGED TOPIC	DESCRIPTION
Upgrading a failover cluster on the same hardware	New
Deploy a two-node file server	New

January 2019

NEW OR CHANGED TOPIC	DESCRIPTION
Deploy a file share witness	New
Cluster-domain migration	New

November 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Configuring cluster accounts in Active Directory	Migrated from the Previous Versions library

October 2018

NEW OR CHANGED TOPIC	DESCRIPTION
What's new in clustering	Updates for Windows Server 2019

June 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster sets	New topic

May 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Configure and manage quorum	Migrated from the Previous Versions library.

April 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Troubleshooting a Failover Cluster using Windows Error Reporting	New topic.
Scale-Out File Server for application data	Migrated from the Previous Versions library.
Hardware requirements	Migrated from the Previous Versions library.
Use Cluster Shared Volumes (CSVs)	Migrated from the Previous Versions library.
Create a failover cluster	Migrated from the Previous Versions library.
Prestage a cluster in AD DS	Migrated from the Previous Versions library.
Deploy a Cloud Witness for a Failover Cluster	Migrated from the Previous Versions library.

June 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster-Aware Updating advanced options	Added info about using run profile paths that include spaces.

April 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster-Aware Updating overview	New topic.
Cluster-Aware Updating requirements and best practices	New topic.

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster-Aware Updating advanced options	New topic.
Cluster-Aware Updating FAQ	New topic.
Cluster-Aware Updating plug-ins	New topic.
Deploy a cloud witness for a Failover Cluster	Clarified the type of storage account that's required (you can't use Azure Premium Storage or Blob storage accounts).

March 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Deploy a cloud witness for a Failover Cluster	Updated screenshots to match changes to Microsoft Azure.

February 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Cluster operating system rolling upgrade	Removed an unnecessary Caution note and added a link.